Threater Enforce Cumulative Release Notes

This document provides cumulative release notes for our Threater Enforce software.

If you have any questions about the content of these release notes, please contact our Customer Success team at **support@threater.com** or by calling +**1-855-765-4925**.

***IMPORTANT NOTE*: as previously communicated multiple times, customers running a build earlier than Build 153 must perform a from-scratch local USB reinstall in order to install the newest software. If you need help with instructions to perform a local USB reinstall, please contact our Customer Success team.**

For customers who are able, we strongly recommend that customers leverage the fully automated software update capability from within our SaaS platform. For those customers who, for whatever reason, are attempting the update manually, you should first contact our Customer Success team.

Recent software releases now leverage industry-standard security updates from the standard publicly accessible Ubuntu security servers. As such, customers should ensure that both their software configuration (see our curated allowed lists in our SaaS platform, for example) and any firewall architecture being employed are both configured to allow the following Ubuntu security infrastructure IP addresses and domains. It is possible that the security community may change these in the future, but these are the current known static assignments. Most customers already leveraging Ubuntu linux in other existing corporate infrastructure will already have these assignments in place:

security.ubuntu.com, 91.189.91.81, 91.189.91.82, 91.189.91.83, 185.125.190.36, 185.125.190.39

changelogs.ubuntu.com, 91.189.91.48, 91.189.91.49, 185.125.190.17, 185.125.190.18

As of Build 130, for performance and scalability, where feasible we now leverage protected bucket services via AWS S3 for certain real-time threat intelligence updates. As such, some customers may need to ensure that the following three domains are reachable from our software's administration port in their firewall rules sets in order to ensure maximum performance. If these are not available, the system will use a less-reliable and less-performant legacy fallback approach:

ati-files-prod.s3.amazonaws.com, s3-w.us-east-1.amazonaws.com, s3-1-w.amazonaws.com

As of Build 229, we've rebranded to Threater, and as such, we have some URL changes. Please make sure that the following domains are reachable via your security infrastructure, such as your next generation firewall rules sets:

portal.threater.com, rms.threater.com

RELEASE NOTES

Release: **Build 247**

File Date: 14 June 2024

Purpose of the Release

This is a standard quarterly release. It contains an exciting new set of features - we're happy to report that we've finalized the migration of the remaining key configuration data from our Enforcer UI into our cloud management portal UI!

As always, we've done a ton of other work and fixed a few bugs as described below.

New and Improved

- **Migrate Enforce Configuration Elements to our Cloud Based Management Portal (#439)**
  - We've finalized a long-standing goal of moving the remainder of our Enforcer configuration from the local Enforcer UI and into our cloud based management portal. If all is as intended, then this means that after initial onboarding configuration (where obviously you have to do local initial network configurations), nearly everything can be managed from the cloud portal. There are of course a few items that can still be managed from the Enforcer UI as needed, to guard against inadvertent lockouts due to configuration errors and such. For the multitudes of our customers who have been asking us for quite some time (you know who you are - thank you!) to 'finish' the configuration migration to cloud control, we're finally there!
- **Bridging Pair Configuration on Non-Standard Hardware (#509)**
  - We had a customer attempt to install our software on non-standard hardware (yes, we support that - as long as the hardware meets our minimum specifications, you can deploy us practically anywhere). Specifically, they were employing a relatively new network chipset that required a slight internal software configuration tweak in order for it to work properly with our DPDK-driven processing engine. We had never seen this happen before, but after isolating the root-cause, we updated our software to ensure more robust DPDK initialization for similar hardware configurations that may appear in the future. This is especially relevant for our international customers that may wish to deploy our software on specific hardware configurations from their own procurement cycles, for any of a variety of reasons, such as supply-chain implications in certain parts of the world.
- **Support for DPDK 22.11.5 LTS (#510, #515, #516)**
  - We've updated our underlying DPDK infrastructure to keep pace with recent LTS changes and ensure that we pick up any residual security patches. We've also updated the core linux kernel in use. These changes are transparent to system operation.
- **Miscellaneous Internal Improvements (#500, #508)**
  - A variety of internal improvements were made for performance and operation, as well as paving the way for some exciting new features coming soon. Stay tuned!

Defect Fix Description(s)

- **Visibility into Stats Metadata Transfer Failures (#495)**
  - While troubleshooting a new customer installation, we ran across a firewall misconfiguration issue at the customer site with an odd symptom of only SOME

information being transferable to our portal. We tracked this down to some MTU issues on the customer-side that we were able to help the customer configure in their infrastructure, but we thought it would be a good idea to improve our Enforcer UI 'Welcome Page' health checks to include a visual indicator of whether this was happening or not for simplified triage. On that note, we now have a new entry 'Upstream Link to Portal' in our welcome page health check statistics, as well as supporting data elsewhere on the page for specific upstream metadata link details.

- **Logging Hysteresis Updates (#506, #512, #517)**
    - We did a ton of work on this in the prior release (build 240). But during internal testing shortly thereafter, we found a few spots where we had missed hysteresis for a few sets of errors for some of the internal filters, so we updated the error handling for those cases as well so as not to inadvertently spam the logs with normal/transient conditions.
- **Syslog Export Log Duplication (#513)**
    - During the course of internal testing, we discovered a condition where it would be conceivable for logs to be exported multiple times in specially crafted scenarios. We have not seen this in the wild, but we fixed this out of an abundance of caution as it was clearly an unhandled edge case in the software.
- **Domain Log Filtering by Direction (#514)**
    - A customer (you know who you are - thank you!) reported a problem with direction filtering of domain logs, where an internal error message was being generated. This is now fixed.

Release: Build 240

File Date: 6 Mar 2024

Purpose of the Release

This is a standard quarterly release - with many exciting features, highlighted by our new Unexpected Blocks feature set, all managed by the backend portal! This can result in significant time savings when making decisions about what to add to allow lists over time, especially when users report a situation where they can't get to a critical business site.

As always, we've also added a ton of other useful features and fixed a few bugs.

New and Improved

- **Threat Categories Now Included in Clipboard Copy from Internal Logs (#344)**
    - We improved the clipboard cut-and-paste features in our internal logs so that now the threat category information is included. We had a customer ask for this feature - you know who you are (thank you!) - and we thought it was a good idea too! Note that this only impacts the clipboard cut-and-paste; ALL information is always exported if you're using our awesome Syslog Export features (and if you're not, you really should be!)
- **ARM Support for AWS (#426)**
    - In addition to our standard 64-bit Intel architecture support that we've always had in

place, we now also support 64-bit ARM architectures in AWS! This can be a tremendous cost savings over time for customers leveraging the cloud, since ARM cores generally cost less than their Intel equivalents, while still meeting or exceeding performance characteristics. When targeting a new instance for deployment, you just have to use the proper architecture template data as described in our cloud deployment documentation and you'll be running in no time. After that, all software updates are intelligent and seamless and will automatically pull the proper architecture from our backend infrastructure when new updates are deployed. In all cases for both architecture variants, we use simple .deb packages. During internal testing, we successfully deployed and tested ARM support leveraging both the AWS c6g.large (a 2 core 4GB RAM instance leveraging the AWS Graviton2 ARM CPU) and c7g.large (a 2 core 4GB RAM instance leveraging the newer AWS Graviton3 ARM CPU) instance types, with excellent results in both cases. We'll be testing and extending our ARM support for other environments as well (both on-premise and other clouds where supported), so stay tuned!

- **HTTP Access Can Now Be Disabled (#455)**
    - Customers can now completely disable HTTP access, to enforce pure HTTPS access only (as opposed to redirect HTTP->HTTPS access). We had a customer request this (Thank you! You know who you are!) and we agreed it's a great feature request so we added it.
- **More Consistent NTP Support (#466, #490)**
    - One of the things that we've continued to do is migrate background system services to be more "Linux-like". The community has consistently migrated towards systemd-timesyncd and away from old-school ntpd, and we've now done the same. There's no significant impact to existing configurations, although you should be aware that if you've configured multiple NTP servers, the 'first' one will be used, and the others will be used only if the first is unreachable. This change is expected to result in significantly better time synchronization over time (no pun intended). As an aside, we know of at least one customer who ran into a few ntpd problems, and we're confident that this feature adjustment will address those too.
- **Support for Backend Portal Unexpected Blocks Feature (#498)**
    - We're extremely excited to release the first iteration of this feature, and we plan on extending this capability set even further over time. Once all of a given customer's Enforcers are running this software version or later, they will be able to initiate Unexpected Blocks analysis directly from the backend portal, which will seamlessly grab relevant data from the Enforcers for analysis by the user in the portal, with easy to understand data augmentations. This should greatly simplify the process of identifying unexpected blocks and streamlining the decision process surrounding whether or not you wish to allow those connections using available allow lists and policy configurations, with a few simple clicks, without ever having to log in to your Enforcer(s) directly. To be clear, this is not meant to be a panacea, but it is meant to greatly simplify the process associated with identifying and remediating potential unexpected blocks.
- **Miscellaneous Internal Improvements (#454, #486, #492, #493, #499)**
    - A variety of internal improvements were made for performance and operation, as well as paving the way for some exciting new features coming soon. Stay tuned!

Defect Fix Description(s)

- **Web App Reloads on Software Updates (#31)**
    - The web app UI is supposed to be able to properly reload on a new software update having occurred, but that wasn't happening in all environments. We think we have this fixed now. Previously the workaround was to simply refresh the browser if a stale UI was noticed after a software update finished.
- **More Intelligent Critical Warning Hysteresis (#38, #417, #488)**
    - Several customers (we feel your pain) have recently complained (and rightly so) that some of our error logs were causing them consternation, given they were flagged as alerting as critical errors. In fact, these were not critical errors, but instead normal, transient conditions. We have fixed this to use a proper hysteresis architecture to ensure that anything flagged as a critical/error alert is in fact that, and not a transient lower level informational consideration.
- **Automatic Package Updates ONLY on Enforce Software Updates (#501)**
    - During routine testing we noticed that certain internal system package updates were happening on an automatic schedule, which is not the intent of our application. We've fixed this, so that now such internal package updates ONLY occur when updating the software (via on-demand or scheduled activity from the portal). We haven't seen this cause any issues to-date, but it conceivably could have, since it could have resulted in short network blips during update sequences, or in the very worst case the possibility of a bricked system (although, again, we've never witnessed that occur). This is now addressed with this improvement, and such update activity can only now occur when updating our software stack through controllable means such as via portal invocation. Note that this in no way changes the ability for the end user to do local on-demand updates if they so desire, through features previously put in place in our local UI.
- **Internal Defect Remediation (#489, #496)**
    - A variety of internal defects were found and fixed. These internal defects are tracked here for completeness, but are not otherwise expected to be customer impacting.

Release: **Build 229**

File Date: 3 Nov 2023

Purpose of the Release

This is an exciting release for us, as it coincides with a corporate rebranding effort. In addition to updating the branding, we took the liberty of doing a lot of internal code cleanup to improve overall maintainability moving forward, and to improve our internal build times. As always, a few defects were addressed and a few minor improvements also made their way into this release.

With our rebrand, we have some URL changes. Please make sure that the following domains are reachable via your security infrastructure, such as your next generation firewall rules sets:

portal.threater.com, rms.threater.com

New and Improved

- **Automatic Middlebox Interface Assignments in AWS (#442)**
  - Previously our middlebox deployment option for AWS required a manual step where the user would key in the proper inside and outside middlebox IP assignments. This is no longer required, and the code is able to auto-determine them.
- **Rebranding (#457, #458, #480, #482, #484)**
  - We've rebranded! We're now Threater, and our enforcement software for on-premise, virtual, and cloud is now known as Enforce!
- **Support for DPDK 22.11.3 LTS (#456)**
  - We've updated our underlying DPDK infrastructure to keep pace with recent LTS changes and ensure that we pick up any residual security patches. These changes are transparent to system operation.
- **Bridge Pair Flip Capability in Software (#465)**
  - This new feature provides a simple way from software control to flip a bridge pair to swap the inside and outside port mappings. Generally it is preferred to flip the physical wires themselves (and then immediately retest for any necessary policy triage) for on-premise installations to avoid downstream confusion, but this new feature can be used in a pinch for remote reconfiguration in one atomic step.
- **Auto-detection for Lanner NCA-1510A Installations (#469)**
  - Our box build partners are now able to ship Lanner NCA-1510A set-top boxes with our software pre-installed, and our stock ISO installer will detect them and fully configure them in automated fashion. Previously, customers receiving NCA-1510A equipment had to manually configure the bridging pair during their initial configuration. With this release, that additional manual step is no longer required.
- **Removal of Defunct Navigation Items (#470)**
  - We've removed several defunct navigation items in the software pertaining to legacy Resource Groups and Service Groups, which were moved to our central cloud-based admin console earlier this year, where they are configured and managed as protected networks and ports.
- **Auto-detection for Dell R350 Installations (#472)**
  - Our box build partners are now able to ship the latest Dell R350 hardware (since Dell no longer manufactures R340 servers) with our stock ISO installer, which supports full auto-detection for supported hardware, to include 10G (downlinkable to 1G) Silicom bypass cards when installed. Previously, customers leveraging Dell R350 servers had to manually configure the bridging pair during their initial configuration. With this release, that additional manual step is no longer required.
- **Half-duplex NIC Improvements (#403)**
  - We now handle DPDK-related messaging for half-duplex environments in a more straightforward manner, to better assist customers identifying deployment anomalies when they've inadvertently used unsupported hardware.
- **Miscellaneous Internal Improvements (#117, #438, #447, #448, #459, #477, #478, #485)**
  - A variety of internal improvements were made for performance and operation, as well

as paving the way for some exciting new features coming soon. Stay tuned!

Defect Fix Description(s)

- **VirtualBox Issues for Minimal Installations (#438, #481)**
  - Although we haven't seen any users deploy directly on VirtualBox (that we know of), we do occasionally use VirtualBox internally for a variety of quick-turn testing. We found issues with bridge creation when using a minimal 2 core 4GB implementation in Virtualbox, and given nuances of the VirtualBox-supporting network drivers which are outside of our control, anyone deploying on VirtualBox will need to configure 4 core and 4GB RAM to ensure a working system.
- **Improve LSH Packet Handling (#461)**
  - When working with our Customer Success team on a configuration issue, one customer (you know who you are - thank you!) noticed an issue with a loose-state handling (LSH) scenario that resulted in an inbound allow that should have been blocked. Part of this was a misunderstanding of what LSH is and how it operates, and to address that, we've added some hover-over text describing LSH handling. Additionally, we re-architected portions of the engine to leverage proper protected networks configurations as they apply to LSH handling. To leverage some of the new features in play, we extended the row details expansion to also include policy and direction information where applicable, so that it can be visualized alongside LSH markers more easily. For those leveraging it, there is no change to the exported syslog information.
- **Resetting protected networks isn't clearing ASN assignments (#471)**
  - When working with our Customer Success team on a configuration issue, one customer (you know who you are - thank you!) noticed that the UI function to reset the protected network configuration from the instance UI was not functioning properly given some recent changes to the way ASNs are mapped to policies. This left the configuration in an abnormal state. We've fixed that in this release.
- **SQL Injection via Local UI ASN Log Filtering (#474)**
  - Internal testing discovered that SQL injection errors were possible when filtering logs by ASN in the UI. This is potentially a security hole, but it is deemed minor as it would take a local trusted user with existing administration privileges to even attempt to cause the problem in the first place. Regardless, we've fixed this in this release.
- **File Corruption on Power Outage (#475)**
  - Internal testing discovered that there was a (very slight) possibility of configuration file corruption on power outages (you ARE running with a UPS connected, right?!). We've rearchitected portions of the codebase to greatly reduce the potential for this to occur. Obviously, when it comes to powering, nothing is 100%, so our recommendation, as with any security control or network critical hardware, is to always ensure that equipment running our software leverages a robust UPS.
- **Errors Running on Google Cloud (#476, #483)**
  - Internal testing discovered some spin-up nuances and a few error messages showing up on Google Cloud deployments. We've adjusted these in this release to avoid customer confusion.
- **Internal System Update Impacting Detection of MAC Addresses on Cloud Systems (#487)**

    - This does not impact previous on-the-rails builds, but could impact systems that are updated out-of-band, so we decided to document this here. We discovered during internal testing of this release on major cloud providers that recent changes beyond our control to the Ubuntu LTS networking ecosystem could result in detection problems of our cloud-facing interfaces. We've fixed this to make sure that systems that are fully updated still function as expected when running in major cloud provider environments.
- **Internal Defect Remediation (#125, #453, #473, #479)**
    - A variety of internal defects were found and fixed. These internal defects are tracked here for completeness, but are not otherwise expected to be customer impacting.

Release: Build 219

File Date: 20 July 2023

Purpose of the Release

This is an out-of-cycle CRITICAL release. During routine, ongoing, internal testing, we saw one of our test systems exhibit strange behavior relating to an underlying critical software networking component. While debugging this, we saw this also happen on at least one customer system. **We have fixed this issue, and we urge all customers to update as soon as possible to ensure that the software will be able to function properly to protect your network, users, and data.** In addition to this critical defect, this release also addresses two other (minor) defects and adds a new feature enabling certain Broadcom NIC support.

New and Improved

- **Support for Certain High-End Broadcom NICs (#463)**
    - The Broadcom BCM5741X/BCM575XX NetXtreme-E® Family of Ethernet Network Controllers are now supported, by virtue of us having enabled the associated DPDK-supplied `bnxt` poll-mode drivers in this release. Note that we do not currently have the ability to test this network driver since we do not leverage any Broadcom adapters in our existing test infrastructure, so customers attempting to leverage the aforementioned Broadcom NICs via the newly enabled DPDK-supplied drivers should do so with that knowledge.

Defect Fix Description(s)

- **Software Locking Issue in Open-Source DPDK (#460)**
    - Data Plan Development Kit (DPDK) is a popular open source software package running on top of Linux and sponsored and used by many large corporations. We leverage DPDK to ensure the most performant, low-latency network environments to assist with the enforcement of our real-time intelligence at scale. Unfortunately, we have found the potential in this open source toolkit for what is called a 'software deadlock' condition. This keeps processes leveraging DPDK from running properly. We discovered this recently during ongoing internal testing of build 214, and we have had at least one

customer (you know who you are; thank you for assisting us!) exhibit the problem as well, while running build 200. Our analysis shows that the potential for this deadlock condition in DPDK goes back to at least build 189, with the potential to occur even before that, although some system timing modifications in build 189 appear to adjust the system timing enough such that this long-dormant DPDK bug reared its ugly head more often than it otherwise might have.
    - In any case, we have fixed this at the DPDK layers, and have patched our own build with this release. As good stewards of the open source community, we are also submitting the patches to the DPDK project so that other DPDK solutions out there can leverage it as well. Thankfully, when the deadlock condition occurs, the software still properly passes protected traffic, but the downside is it may not receive timely threat intelligence updates. Also, it may not be possible to login to the UI when in this state. Lastly, it also may not be possible to use the automated remote software update features from our centrally managed admin console.
    - **Although we have only run into this sparingly, in the interest of caution and in the strongest terms possible, we strongly urge ALL customers to update to this new build as soon as possible.** If the automated download fails the first time, we recommend manually rebooting the instance. If you are not able to access the UI, you can attempt a software reboot by logging into the serial port if available, or via SSH if you have it configured. Once logged in, use '`sudo reboot now`' (without the single quotes) to reboot the system. If these options are unavailable to you, as a last resort, you can use the power button to cycle power. It is highly likely that on reboot the condition will clear, and you should then be able to remotely update the software from our central admin console. In the unlikely scenario that the condition does not clear and you remain unable to initiate a remote software update after two such successive manual reboot attempts, our recommendation is to contact our Customer Success team so that we can assist with further remediation as needed.
- **DNS Response Logs Not Generated Properly (#462)**
    - During ongoing internal testing, we found that build 214 introduced a problem where the syslog-export target DNS Response Log category was not being properly generated. There is no impact to the UI, as those log types are only exported via syslog export. Customers expecting those logs to show up in the RFC-compliant syslog export will want to update their software to pick up this fix. No other export log type was impacted.
- **Threat List Source Name Attribution Missing From Syslog Export Logs (#464)**
    - During ongoing internal testing, we found that build 214 introduced a problem where the syslog-export logs were not properly attributing results to threat lists by name. Categories and thresholds were properly appearing, but threat list names were not, which impacted attribution for Webroot and Proofpoint (where applicable). This impacted only the syslog export message function and nothing else. We've fixed this in this release, so that the syslog export threat list attribution is now correct.

Release: **Build 214**

File Date: 30 June 2023

Purpose of the Release

This is a standard quarterly release. It incorporates several exciting new features and fixes a couple of (very) minor bugs. Given the newly incorporated features, in particular the per-policy configuration improvements and login via proxied SSO support, we do strongly recommend that customers update to this release as soon as possible.

New and Improved

- **Domain Lists, ASN Lists, and Threat Lists are Now Tied to Policies (#53, #54)**
    - Previously, domain lists, ASN lists and threat lists were all largely globally configured. This caused some customers some difficulties, where, for example, they wanted to selectively allow (or block) certain things (such as a specific ASN or specific domain list) only for certain policy groupings. Previously, they had no way of doing that. With this release, this is now trivial to accomplish. Once all instances tied to a particular customer are running this new release (or later), these features are opened up, and users can selectively enable/disable domain lists, ASN lists, and threat lists on a per-policy basis. By default, the global settings are propagated to all existing policy configurations, so there's "nothing" that needs to be done until and unless a customer wishes to adjust per-policy settings as needed. When creating new policies, the customer decides at that time what gets used across the board. We are really excited about this feature - the collection of these things culminates from no less than a dozen direct customer requests for a variety of similar features. For those of you who had asked for one or more of these - you know who you are, and we thank you for your input!
- **SSO Support (#424)**
    - We have always supported and allowed local login/user configuration. Now, with this release, we also enable the ability to login via SSO. This works via proxy to our SSO configuration on Admin Console. That is, once configured appropriately in Admin Console, you will be able to login to the local UI via proxied SSO. This means that you won't be forced to maintain separate user accounts on your local instances (unless, of course, you choose to do so). Nothing changes for the current login configuration, and the default local login credentials for new deployments remains unchanged as well. Put another way, the SSO support is a new feature addition and does not invalidate any way you may currently be using local credentials. You do, of course, have the ability to remove those local configurations if you'd like (ie, deleting local users), if using SSO is preferable. There are many great reasons to consider the use of SSO, not the least of which are the ability to require MFA even for local access, as well as to simplify the removal of login credentials when in-access employees are offboarded.
- **Support for Google Cloud Platform (#440)**
    - Most of our customers are aware that we support on-premise (via hardware meeting minimum specifications), virtual via VMware or KVM, protection of AWS infrastructure and protection of Azure infrastructure.
    - We are excited to report that we now additionally support Google Cloud Platform (GCP), extending our ability to protect your infrastructure wherever it is!

    - Just like other cloud-based deployments, there are some nuances to GCP which make it slightly more complicated than on-premise environments, so as always, if you have GCP infrastructure in need of protection, be sure to hand our comprehensive documentation to your GCP-certified IT team(s) for analysis first! As with all of the technical documentation, our customers are able to access it directly from our support portal(s). Note that unlike our other deployment options, our software installation on GCP requires relatively high-core instances (we currently recommend a e2-highcpu-8 machine type), due to nuances of networking support in GCP that are beyond our control.
- **Miscellaneous Internal Improvements (#428, #443, #444, #449)**
    - A variety of internal improvements were made for performance and operation, as well as paving the way for some exciting new features coming later in the year. Stay tuned!

Defect Fix Description(s)

- **Inbound and Outbound Naming Nomenclature (#451)**
    - We noticed when renaming protected networks internally that redundant inbound/outbound terminology could be inadvertently appended, causing naming cascade problems. Generally there were no user-facing implications, except conceivably for naming redundancy in certain syslog export configurations or potentially when perusing internal logs. In any case, we've fixed this in this release.
- **Internal Defect Remediation (#425)**
    - A variety of internal defects were found and fixed. These internal defects are tracked here for completeness, but are not otherwise expected to be customer impacting.

Release: **Build 200**

File Date: 24 May 2023

Purpose of the Release

This is an out-of-cycle release to address another software update issue that crept up due to some unanticipated and uncommunicated OS kernel package removals from Canonical, the corporation responsible for Ubuntu LTS security updates. Customers already running Build 195 or Build 198 do **NOT** need to update right away if they don't want to. Of course, as always, it doesn't hurt if you do update.

New and Improved

- **N/A**

Defect Fix Description(s)

- **A Second Canonical/Ubuntu Kernel Package Removal Event Causes Software Update to Fail (#452)**
    - It appears that Canonical, the company behind the Ubuntu linux distribution that we

leverage in the software, is routinely removing older kernel packages from their stock repositories, even when they are in LTS chains. We first saw evidence of this a few weeks ago, which culminated in us releasing Build 198 to address the lone incident at the time. We have now seen it again. The symptom would have been customers being unable to update the software. This release fixes this problem in a more standard way, versus the one-off mechanism that was employed in Build 198. Users who have recently attempted a software update that failed due to these issues can retry with this release, and the issue should be addressed. It is our intent that this is the 'last' one of these, but of course we will continue to monitor the situation to ensure that any future 'shenanigans' on the Ubuntu LTS side don't negatively impact timely underlying software updates.

Release: **Build 198**

File Date: 11 May 2023

Purpose of the Release

This is an out-of-cycle release to address two minor fixes. One in particular addresses a software update issue that crept up due to some unanticipated and uncommunicated OS kernel package removals from Canonical, the corporation responsible for Ubuntu security updates. Customers already running Build 195 do NOT need to update right away if they don't want to. Customers not yet on Build 195 who want to update their software may have run into issues when updating, and this release addresses that.

New and Improved

- **N/A**

Defect Fix Description(s)

- **2 Core / 4GB Deployments on Azure Could Hang Over Time (#445)**
  - During internal testing, we noticed two instances where a bare-bones 2 core/4GB instance running on Microsoft Azure would hang. This occurred due to memory exhaustion due to an internal system memory leak. The prior workaround was to reboot the instance. We've now fixed this.
- **Canonical/Ubuntu Kernel Package Removal Causes Software Update to Fail (#450)**
  - A recent decision by Canonical, the company behind the Ubuntu linux distribution that we leverage in the software, resulted in some critical OS kernel packages being removed from their repositories, which could cause a software update to fail (but the system would still remain functional running the older software). The symptom would have been customers being unable to update to the previously released build 195 software. The symptom would have started in early May 2023, when the associated OS kernel packages appear to have been removed by Canonical. This release fixes this problem, and software updates to the latest software version will now work properly

again.

Release: Build 195

File Date: 31 Mar 2023

Purpose of the Release

This release contains major feature updates as well as **important defect fixes**. We deem these fixes to be especially critical, and as such, **we strongly recommend that all customers update to this release as soon as they can**.

New and Improved

- **Golden Image Support Plus Activation Improvements (#401)**
  - With this release, we now officially support golden image stamping by our boxbuild partners and our MSP partners for mass-rollout use. Previously, some manual steps were required when onboarding a golden-image-stamped installation, and now that is no longer the case, since we now regenerate a full set of unique keys on every successful activation. As part of this, we have also further streamlined the activation process, to allow for the elimination of the initial non-deterministic 10-15 minute wait times upon new activation. These new mechanisms greatly reduce the onboarding time for new installations, regardless of origin.
- **AWS Gateway Load Balancer and AWS Cloud Formation Support (#408, #435, #436)**
  - Customers using us to protect AWS infrastructure now have a new architectural way to do so! Previously, we deployed exclusively into existing AWS VPCs for specific subnet protection by virtue of the 'AWS middlebox architecture' onboarded with simple shell scripts. We still support that legacy mechanism (since it is of great value for many installation needs), but now we have extended our AWS solution to support their Gateway Load Balancer (GWLB) approach. Advanced AWS customers requiring service chaining of multiple solutions will likely appreciate the flexibility that the AWS GWLB architecture provides. Note that our support for the AWS GWLB architecture includes the ability to use AWS Cloud Formation to fully configure the solution, which greatly simplifies onboarding into AWS infrastructure for GWLB modes.
- **AWS Boot Time Improvements (#409)**
  - With this release, we have streamlined the bootup sequence on AWS deployments to curtail certain types of kernel behavior. Worst case bootup times, even on low end cloud hardware such as 2 core environments, now takes just one or two minutes vs up to 25 minutes previously on initial installation and on certain kernel/security updates.
- **Cyber Intelligence Fallback (#411)**
  - We recently made a massive performance improvement with our cyber intelligence feed architecture to use the effectively 'infinitely scalable' AWS S3 service. Unfortunately, some customers, by virtue of specific external policies forced upon them, are not able to allow communications to AWS S3 services. To adjust for this, we've added a feature where we will detect an AWS S3 failure, and in the event of such a failure, we'll fallback

to the older significantly less-performant cyber intelligence delivery approaches that we used in the past. To be clear, our strong recommendation is to make sure you are able to use AWS S3 if at all possible for the best possible performance (read: you'll get cyber intelligence updates MUCH faster this way), but for those that can't, this will ensure that they are still able to receive updated intelligence, albeit in a much less performing way (read: it will take significantly longer, which means you're at risk longer -- in cyber security, even small numbers of seconds can matter, which is why we transitioned to world-class AWS S3-driven delivery in the first place!)

- **Miscellaneous Internal Improvements (#431)**
    - A variety of internal improvements were made for backend performance and operation, as well as paving the way for some exciting new backend features coming later in the year. Stay tuned!

Defect Fix Description(s)

- **Feed Synchronization Intermittent Issues After Initial Activation (#427)**
    - During internal testing, we noticed one instance where feed synchronization did not work properly immediately after the initial one-time activation that happens during initial onboarding. The workaround was to reboot the instance, at which point everything proceeded as normal. We were able to identify the root cause of this issue and it is now fixed in this release.
- **Secure Boot Modes Not Properly Identified (#429)**
    - The software detects secure boot modes and informs the user that it should be disabled in the BIOS for our software to install and run correctly, however, in one case on a set of low-end hardware that a partner was attempting to deploy, we found that the secure boot detection paradigm was flawed, and it erroneously detected secure boot when it was not actually present. This kept the software from being able to install and run properly. This is now fixed with this release.
- **Properly Handle Double VLAN-tagged Frames (#430)**
    - During some internal testing we noticed that packets with double VLAN tagging were not being evaluated, and were being passed through in all cases. Given how we are typically deployed on networks, it is unlikely that this would be a real issue, which is probably why it escaped notice for so long. On that note, we know of no customer deployment where this was a concern, but out of completeness, we have addressed this and in the unlikely case we are placed on a network span containing double VLAN-tagged packets, we will properly evaluate them now against our threat intelligence for allow/block considerations.
- **Already-Established (Inflight) Connections Not Being Reevaluated (#432)**
    - Very recently (March 2023), a defect was discovered by one of our customers (you know who you are - thank you!) in our recent feed synchronization architectural changes that caused already inflight connections to not be properly re-evaluated when cyber intelligence updates occurred. This means that if an existing connection was already up and new intelligence suggests that the far-end IP is malicious, the connection would have been maintained. Previously (and correctly) it would have been torn down. The issue impacted only inflight connections - new connections were and remain properly blocked as appropriate. The workaround was to make (any) kind of innocuous policy

change (such as adding an empty allow list to a policy) that would force re-evaluation, since this defect was localized just to the contents of existing attached lists. **Having said that, we consider this a critical defect, and as such we strongly urge all customers to update to this release as soon as possible.**

- **Unmanageable Process Crash on Azure (#433)**
  - Outside of our control, Microsoft's Azure service takes some … liberties … with how it can willy-nilly change out hardware, even network interfaces, from its underlying virtual machines. For a network security control relying on fast-path communications to known network interfaces, this is absolutely horrific, but it is what it is. On that note, we discovered in internal testing on a system in Azure that had been running for close to 30 days that it suddenly failed when such an event occurred. We are working around this underlying issue in Azure by detecting such an occurrence, and when we detect it, we reboot the instance to make sure that all fast-path hardware is properly re-identified. The process takes no more than a minute or so when it happens. Note that we do not expect it to happen often, but it was important that this was properly handled. If and when Azure does something more intelligent here, we'll back this undesirable 'fix' out.
- **Policy Mappings Incorrect When Renaming Sources (#434)**
  - A customer recently reported (late March 2023 - you know who you are - thank you!) that list metadata and sources were erroneously being mapped in the policies and logs when the source was renamed. This has been fixed. Although it is not common for list names to be renamed by customers once they've been created, **we still consider this a critical defect, and as such we strongly urge all customers to update to this release as soon as possible.**

Release: Build 189

File Date: 2 Feb 2023

Purpose of the Release

This release contains a set of **major feature updates**, and as such, **we strongly recommend that all customers update to this release as soon as they can**. It works alongside our newly released redesign in our SaaS admin console, which enables a significantly improved user experience, especially with regard to configuring protected networks and ports (previously referred to as Resource Groups and Service Groups in the software). These parameters are now exclusively managed from our SaaS admin console, and will be especially beneficial for customers with multiple instances deployed, since management for protected-side networks can now be done entirely from the admin console. Only customers running this build or later will be able to use those new features.

In addition to those major new feature additions, this release also brings a **massive set of improvements** in the feed architecture, allowing us to drastically reduce feed synchronization times to a fraction of what they were previously. This is most notable when first onboarding a new instance, but also affords significant standard over-time feed updates. As part of this work, we have also drastically increased the number of attributable lists, and we know of no customer even remotely

close to our new internal limits of 255 lists, per type.

Last but not least, this release comes with a **drastically reduced set of minimum specifications**. Specifically, we can now run lossless 1Gbps bidirectional throughput on systems with just 2 cores and 4GB of RAM! Previously we required 4 cores and 8GB of RAM. It certainly doesn't hurt to have the extra cores and RAM, and we will use what is available, but for those clients installing in low-bandiwth environments, or in cloud or virtual environments (or for our growing MSP customer segment deploying on low-cost endpoint hardware or as virtual blades), these reduced resource requirements will likely prove to be a godsend.

New and Improved

- **Stop Background Browser Health/Alert Checks When No One Is Logged In (#7)**
    - Previously, even when a user was not logged in, the browser log in would run background checks, which have no meaning and would only serve to eat browser resources. This no longer occurs. The background checks are now run only when a user is logged in locally.
- **CLI Admin Menu System Information (#40)**
    - We extended our onboarding CLI scripts to be able to display relevant system information from the CLI, which can be useful when onboarding new instances and/or working with our remote Customer Success teams for local serial port or SSH access.
- **Feed Rearchitecture (#158, #388, #404)**
    - This exciting feature effectively slashes our feed synchronization times by up to an order of magnitude or more, which is especially noticeable when onboarding a new instance. It also greatly improves feed synchronization over time.
    - In addition, we now support up to 255 uniquely attributable lists for each list type (allow, block, threat). This is up to 4x our current known largest set of customer-facing attributable lists.
- **Protected Networks Support for New UX Redesign (#399, #416, #418, #420, #421)**
    - Previously, resource groups and service groups had to be manually configured on each and every physical (or virtual) instance. With this release, we are happy to report that this is no longer the case. These are now 100% managed in our SaaS based admin console, and automatically synchronized to your instances over time as changes are made.
    - Your existing settings will automatically and seamlessly be imported into our SaaS admin console for management therein.
- **New Minimum Specifications: 2 Core / 4GB RAM for Lossless 1Gbps Bidirectional Throughput (#158, #181, #390, #410)**
    - Previously, to support up to 1Gbps bidirectional lossless throughput, we required 4 cores and 8GB RAM. We are happy to report that the changes in this release have allowed us to reduce our 'absolute' minimum requirements to just 2 cores and 4GB RAM!
    - **There are of course a few downsides to fewer resources, so make sure you understand them before racing to minimum specs when deploying new systems.** These downsides include but are not necessarily limited to:
        - longer bootup times,

        - the UI will be more sluggish (since there are less resources available for non-network activity),
        - software update times will take longer on reduced resource systems (15-20 minutes for 2 core/4GB systems, vs. the more typical 5-10 minutes for 4 core/8GB systems),
        - reduced number of total loadable IPs and domains. Note that the system will alert you if you begin to reach limits of your chosen hardware; the system will still function but will alert you as you reach any inherent limits, which could limit your total protection. It is worthwhile to note that it would be very difficult for most users to reach any such limits; if such limits are reached and you are alerted as such, you'll likely want/need to move to beefier hardware.
    - Lastly, note that 2 core / 4GB RAM variants are primarily meant for targeting virtual infrastructure (such as AWS, Azure, Vmware, KVM, etc.). Most folks with on-premise 1Gbps deployments or public cloud deployments will likely find it preferable to stick with systems with at least 4 cores and 8GB RAM, not just to reduce the impact of the 'downsides' but also because of real-world supply chain implications in today's environment, where it is often easier to procure 4 core/8GB RAM systems than it is lower-end 2 core/4GB RAM systems, since fewer manufacturing cycles are being devoted to low-core-count CPUs and low RAM stick sizes.
- **Traffic Filtering Selection (#336)**
    - With more and more customers deploying into the cloud, virtually, and BYOH (bring your own hardware) without hardware bypass, we've added an in-your-face way on our Welcome page to enable or disable Traffic Filtering in software. When enabled, all traffic is protected in both directions. When disabled, it's the equivalent of a software bypass mode, where all traffic will flow in both directions with no logging.
    - In no way does this change how existing customers with hardware bypass use and configure the hardware bypass function - this is above and beyond that, and provides direct software control of software traffic filtering.
- **Support for DPDK 22.11.1 LTS (#374, #384, #398, #412, #413, #422)**
    - We updated the underlying DPDK infrastructure to the latest and greatest LTS release, which allows for more hardware/NIC support and better cloud support on Azure and AWS.
    - This also updates our checksumming approaches for ICMP Unreachable and TCP Reset response methodologies to comply with new DPDK-associated invocations, especially as they apply to 10G environments.
- **Shell Password Reset (#406)**
    - We now provide a means to reset the stock shell password in Ubuntu 22.04 LTS via our UI menus. This may be useful when performing advanced troubleshooting with our Customer Success team if shell access is required but a customer has forgotten or misplaced their credentials.
- **Cloud and Virtual Instances Bridge State and Related Health Check Reporting Adjustments (#386, #395, #407, #419)**
    - We noticed that cloud and virtual instances were sometimes displaying with invalid bridge state detail in the admin console, given that they don't by definition have hardware bypass circuitry (unlike most on-premise physical deployments). We've fixed

this so that it reports information that the SaaS admin console can properly parse and display, and we're paving the way for more detailed information being available for display in the admin console.

- **Miscellaneous Internal Improvements (#377, #385, #393, #394, #396)**
  - A variety of internal improvements were made for backend performance and operation, as well as paving the way for some exciting new backend features coming later in the year. Stay tuned!

Defect Fix Description(s)

- **SNMP Fixes for Azure Infrastructure (#376)**
  - SNMP services were not functioning properly on Azure environments. This is now fixed.
- **Software Upgrade Fixes (#380, #382)**
  - The significant recent upgrade to Build 153, which incorporated the underlying OS upgrade to Ubuntu 22.04 LTS, went largely flawlessly, but we did notice a few minor issues with some customers. All such things that we discovered while supporting those upgrades are fixed in this release.
- **Startup Configuration Fixes for AWS and Azure Infrastructure (#383, #405, #415)**
  - We noticed a few intermittent AWS and Azure startup issues, especially on new deployments, which we fixed in this release. We don't expect these to be customer impacting, but are tracking them here for completeness.
- **Import Settings Wasn't Working on a First Attempt After a New Installation (#397)**
  - We noticed this during a wiped-unit test run. The workaround would be to reattempt the import, which would succeed. Regardless, it is now fixed.
- **Internal Defect Remediation (#378, #391, #392, #400, #402, #414)**
  - A variety of internal defects were found and fixed. These internal defects are tracked here for completeness, but are not otherwise expected to be customer impacting.

Release: **Build 154**

File Date: 4 Nov 2022

Purpose of the Release

This release is primarily meant for our box build partners who have already built and stocked equipment with Build 153 installed, but need to remediate the recent community-announced vulnerabilities in OpenSSL 3 so as not to drop-ship new equipment susceptible to the OpenSSL 3 flaws.

Every new software installation by way of an ISO image or automated download always undergoes a live (real-time) `apt update` and `apt upgrade` cycle, to ensure the latest underlying Ubuntu LTS operating system security patches are available and installed from the official Ubuntu LTS repository servers. Recently, the open source community identified a set of vulnerabilities with a rating of HIGH for the popular OpenSSL 3 library, which is leveraged by Ubuntu 22.04 LTS, which we started leveraging with Build 153. The Ubuntu LTS team has backported those fixes into the LTS-maintained

package versions.

Although existing customers who have installed Build 153 are able to login and use our out-of-band security update feature via our UI to pick up the security fixes, our box builder partners cannot. The simplest way for our box build partners to ensure they have the latest updates is to reinstall this new Build 154 via USB/ISO overtop of any existing Build 153 stock. Given the timing of the release, anyone installing Build 154 by any means (ISO or automated admin console download) is assured of having all relevant OpenSSL 3 security updates at the time of the install.

Note that end customers who may have installed Build 153 **after** the OpenSSL 3 community fixes were released mid-day Tuesday, November 1, 2022 are fine, since every software update always involves pulling the latest security fixes at the time the update is installed.

However, existing customers who aren't sure or who updated to the previous Build 153 **prior** to the OpenSSL 3 community fixes and aren't precisely sure if they have followed previously supplied instructions to run the out-of-band security updates could certainly choose to install Build 154 to be absolutely sure they have the latest updates. Put another way, if you successfully install Build 154, you are guaranteed to pick up the latest OpenSSL 3 fixes.

New and Improved

- **N/A**

Defect Fix Description(s)

- **N/A (No defect fixes are in this release, however, see 'Purpose of the Release' above for notes about community OpenSSL 3 vulnerability fixes.)**

Release: Build 153

File Date: 18 Oct 2022

Purpose of the Release

This is an important release which adds exciting new capabilities, including support for Microsoft Azure's recently GA'd gateway load balancer support, several ongoing MSP partner-related improvements, adds support and improves upon low-cost hardware deployments, and lays the groundwork for top-level domain blocking (which will be finalized soon).

But most importantly, this release updates the base level operating system from Ubuntu 18.04 LTS to Ubuntu 22.04 LTS. **It is critical that customers update to this release as soon as possible to ensure that their installations remain secure, since community support for security updates to Ubuntu 18.04 LTS will end in early April 2023.** If you fail to update by the time community support ends, your software update will fail, and your only recourse to update our software stack will be via USB install. As such, it is our super-strong recommendation that you update to this build (or a later build) as soon as possible. ***Don't wait until the last minute.***

Because of the nature of the underlying OS upgrades that will occur as part of this update, you should budget for 30-45 minutes for this particular software update to complete. Systems that support hardware bypass will enter that mode prior to the update sequence, so that traffic will still flow, but it will be unprotected during that time. Systems that do not support hardware bypass will stop passing traffic until the update completes. As such, we recommend that you perform this update in a maintenance window of your choosing. You can either use the fully automated software update capability from within our SaaS platform in on-demand fashion when you're ready, or you can schedule it for an off-hours update cycle of your choosing. **Systems will reboot several times during this upgrade. This is normal. They will also need internet access during the upgrade in order to download packages from the sites mentioned at the top of this page.**

New and Improved

- **Block the Entirety of a Top Level Domain (#18)**
  - We now have the ability to block by top level domain. However, this feature will not be usable until we've enabled support for propagating top level domain detail via our SaaS admin console. Stay tuned to future release notes from our admin console team for information on when it is available!
- **Simplified CLI Admin Menus (#44)**
  - Now that our recent installers are done the standard "Ubuntu way", the admin menus are always initiated from a shell, which means that in the off-chance you need a shell, there's no need to drop to a new shell from the menu - you just leave the menu. We've updated the menu to reflect that.
- **Support for Low-Cost Intel I225 NIC Hardware (#297)**
  - Several new low-cost hardware variants being introduced by various hardware vendors leverage the Intel Ethernet Network Adapter I225 series, which is a relatively new type of NIC chipset released by Intel in 2021, and just now making its way into mainstream low-cost hardware. With this release, we now fully support that chipset when auto-detecting ports for creation of a bridge pair in the UI. This may be of interest to MSP customers deploying low-cost hardware that they're procuring through their own supply chain channels for small-site deployments.
- **Support for Microsoft Azure's Recently GA'd Gateway Load Balancer Architecture (#319, #373)**
  - Microsoft recently moved their "gateway load balancer" (GLB) feature in Azure from a special preview-only mode to generally available, and as such, we are now able to fully support the mechanism. This is a watershed moment for Azure since the GLB feature is technically superior to the legacy Microsoft network virtual appliance (NVA) mode which required special NAT'ing controls that adversely impacted feature, useability and performance. With GLB, all of that is mitigated. Customers who are already using or want to use our software to protect their Microsoft Azure-resident traffic or who wish to protect such traffic will certainly find things much easier.
- **Migrate to Ubuntu 22.04 (#305, #343, #347, #361, #362, #366, #367, #370, #372)**
  - This is the primary driver for this release. Previous builds have leveraged Ubuntu 18.04 LTS, and this build updates the underlying OS and subsystems to Ubuntu 22.04 LTS. **It is critically important that customers update to this release or a later release no later than the end of March 2023, since community support and related security**

updates for Ubuntu 18.04 LTS systems end in April 2023.

- **Syslog Export Now Matches If a Corresponding IP Is In Any Category (#328)**
  - Previously, when syslog export messages were generated, the Threat List field (actual field name: `tl`) in the syslog message was reported only if the category the IP is in was also enabled for a particular policy. We've extended this such that it will now fill the Threat List field if the IP in question is in any category, regardless of whether or not it is selected on the associated policy. This is very useful for assisting in configuration auditing to check for things being allowed that possibly shouldn't be due to policy misconfiguration.
- **Rebranding Script Improvements for Our MSP Partners (#329, #340, #341, #349, #350, #351)**
  - A ton of improvements were made to our partner rebranding script - at least two of our MSP partners helped us flush this out (you know who you are - thank you!):
    - User-specific IP, password, and shell credential management has been improved.
    - The favicon can now be updated (previously, only the logo could be updated).
    - Co-branding vs. rebranding logo handling are both supported, and fully under partner control within the confines of the SVG that they supply to the rebranding script.
    - Hover text references where applicable are genericized, to avoid any confusion.
    - EULA acceptance via script command, which keeps MSP end customers from having to perform this step themselves.
    - Private SSH key login is now supported. This is especially important for MSP partners who are spinning up in cloud infrastructure, where the only way to login to an instance or virtual machine initially is typically via secure SSH private keys. Included with this capability is an automatic way to propagate new keys into AWS infrastructure, for those MSP partners spinning up there.
- **Improved Low-End Hardware Line Rate Support (#332, #355)**
  - We have implemented and tested proper CPU isolation on the lowest-end hardware we could get our hands on meeting our minimum requirements, and are happy to report that we are now able to achieve full 1Gbps line rate performance on such systems, the same as is possible for our standard turnkey offerings. This could be of interest to MSP partners and/or customers who procure their own low-cost hardware or have very small satellite offices that they want to protect, but couldn't justify beefier hardware requirements for those locations.
- **SSL Certificate Handling Improvements (#334)**
  - A common source of confusion is errors associated with SSL certificates when customers are performing SSL inspection on separate security controls in their stack. Previously, the error messages generated in our UI stemming from certificate errors were… cryptic at best (no pun intended!) We've improved these messages measurably in this release, to assist customers in remediation of the problem in their alternate security controls.
- **Support for Non-Bypass Turnkey 10G Systems (#335)**
  - Our turnkey 10G line rate systems are generally Dell R340 or equivalent servers with an embedded Silicom card supporting hardware bypass. However, astute customers

wanting to do HA the right way typically do not want hardware bypass, since it can adversely affect failover for full traffic protection. We've had the ability to support such non-bypass environments for quite some time with manual reconfiguration of the bridging pair in our UI to choose non-Silicom ports. With this release, we're now able to turnkey-ship 10G non-bypass configurations to those customers requesting them without any special reconfiguration required.

- **Rebaseline System Shell User Profiles (#342)**
  - Customers that for whatever reason have enabled and utilize serial port, keyboard/monitor, and/or secure shell (SSH) access should pay attention to this item; those that do not can ignore it.
  - Starting with this release, all installations will rebaseline the shell user profiles for consistency of shell user login across all deployment environments. All systems will now have a stock "`ubuntu`" shell user with appropriate sudo privileges, and any users that may have been installed by older builds will be removed, and any stock '`root`' user disabled as best-practice.
  - Customers leveraging shell login should now use the default "`ubuntu`" user and default password (customers unfamiliar with the default password should consult our Customer Success team) and change the password, in the same way we recommend this when installing a system from USB. Be sure to use a strong password, and if necessary, write it down and store it in a protected place. If you forget your password, there's no way to recover it, and in that case your only recourse would be to reinstall the system via USB if downstream shell access is required.
  - The collection of these things makes the shell users on the system the same, no matter what version was initially installed or where it is deployed (on-premise, cloud, etc.) It also reduces the risk of having default passwords on the box.
  - In no way does this impact the HTTPS UI that the software employs or its users; this impacts only shell user configuration, which is typically needed only for initial system configuration, or in the event of certain specific troubleshooting needs when working alongside our Customer Success team.
- **Administration IP Configuration Safeguards (#360)**
  - When configuring a static administration IP address for a deployment, new installations and/or changes to the administration IP are now required to use a non-routable IP address from the following RFC-compliant non-routable pools only:
    - 10.0.0.0/8
    - 172.16.0.0/12
    - 192.168.0.0/16
  - Note that if you are running a relatively recent software build, you can see your administration IP in our cloud based management portal on the suitable Appliance card for your deployment(s).
  - Previously, the software allowed a public IP to be configured for use as the administration port's static IP address. To our customers' credit, very few of you have done this, as you know the importance of making sure access to your security controls are properly locked down with no possibility of unauthorized external access, ever. Adding this new feature will protect against inadvertent customer misconfiguration moving forward.

    - If you've erroneously configured your system to use a public-facing administration static IP address, it will still work. That is, this feature does not impact existing deployment configurations as they currently sit. However, the requirement will apply if you attempt to edit the administration static IP for an existing configuration.
    - We **super-strongly** recommend that if you are using a routable static IP address for your administration IP that you adjust your network cabling immediately and source it with a private non-routable static IP address. Your IT teams will be able to assist you, and you can always reach out to our Customer Success team for help.
    - These new rules do not apply to DHCP. When the administration IP is configured to use DHCP (including static DHCP), it will register and use whatever IP address your DHCP server provides it, and these extra safeguards will not be applied. For the < 1% of customers who may need to use something in the publicly routable pool which is guaranteed by virtue of their network architecture to be internally-facing only (such as some IP ranges in use by certain ISPs), this is the way you should handle it; but even then, it would be our **strong** recommendation to consider using a true non-routable IP, to avoid any possibility of external network configuration changes inadvertently made by your IT team(s) resulting in the exposure of the system's administration port to untrusted public infrastructure.
- **Miscellaneous Internal Improvements (#333, #335, #337, #338, #346, #358)**
    - A variety of internal improvements were made for backend performance and operation, as well as paving the way for some exciting new backend features coming later in the year. Stay tuned!

Defect Fix Description(s)

- **Correct SNMP Bridge Naming for Non-Standard Systems (#330)**
    - Some legacy customers with dual-bridging environments noticed that SNMP bridge naming was not correct in all scenarios. This is now fixed in this release, and proper bridge names are applied for these legacy environments.
- **SNMP Subsystem Configuration Updates (#331)**
    - A defect was introduced in Build 130 where an internal process handling name change resulted in an inconsistent SNMP data file. The workaround was to delete and re-add the SNMP user. We have now fixed this issue, and the workaround is no longer required.
- **Users List Endpoint Failing (#339)**
    - A very unlikely defect was introduced in Build 130, and was seen by one customer who helped us get to the bottom of the problem (you know who you are - thank you!) If a user happened to be locked out of the local UI and then performed the Build 130 auto-update from our SaaS admin console, the lockout condition caused a problem with user migration for that particular user. The result was that the affected user is unable to log in, and the associated users listing endpoint in the UI would fail to render a page view. This is now fixed in this release.
- **Feed Synchronization Can Hang (#348)**
    - A customer (you know who you are - thank you!) noticed a scenario where a feed sync operation could hang, and was not restarted in a timely fashion. This is now fixed, ensuring feed synchronization stability against our backend feed services.

- **Maximum Tag ID Handling (#364)**
    - A customer (you know who you are - thank you!) noticed a scenario where a very large number of feeds were causing internal loader resets due to a wrapping tag ID counter. We've fixed this.
- **TCP Reset (RST) Logging is Unnecessary When Blocking a RST packet (#371)**
    - During internal testing we discovered a defect where an incorrect 'error' log message was being registered which could inadvertently cause customer confusion surrounding RST packet handling, so we've removed the offending log message.
- **Internal Defect Remediation (#29, #32, #345, #352, #359, #365)**
    - A variety of internal defects were found and fixed. These internal defects are tracked here for completeness, but are not otherwise expected to be customer impacting.

Release: Build 135

File Date: 18 Oct 2022

Purpose of the Release

This release is an internal, jump-point release. Its sole purpose is to facilitate movement to Build 153+ which leverages the Ubuntu 22.04 LTS underlying operating system. Prior builds leveraged Ubuntu 18.04 LTS. **There is no need for customers to update to this release; instead, it is automatically used behind the scenes when a customer upgrades from an earlier release to a 153+ release.** That is, this release is internally managed by our automated software update mechanism as a transient portion of the update process. When updating to a 153+ release, you may see your system temporarily report this release number before automatically arriving at its final release build destination.

New and Improved

- **N/A**

Defect Fix Description(s)

- **N/A**

Release: Build 130

File Date: 28 Jul 2022

Purpose of the Release

This is an exciting release where we continue our march towards fewer and fewer resource requirements. The highlight of this release is the elimination of the internal use of the Mongo database. In addition to driving down resource needs, this also improves the overall update process

and security posture, since Mongo requires separate non-standard security package pulls, which from this release forward will no longer be required. Additionally, this release also makes use of some recent feed performance improvements in our backend architecture, which means a better overall user experience and faster operation when certain types of feed changes occur. Last but not least, the landing page has been completely revamped to actually contain useful information as opposed to partially rehashing what already was available in our cloud based management system.

Please note that as a result of the enhancements implemented in this software release, customers are now advised to ensure access is allowed to the following three domains in your firewall rules:

- ati-files.prod.s3.amazonaws.com
- s3-w.us-east-1.amazonaws.com
- s3-1-w.amazonaws.com

New and Improved

- **Open Up Timezone Lists (#185)**
  - Previously we limited the time zone list to a subset of timezones. This is no longer the case. Now we permit and allow all possible timezones of the host Ubuntu operating system. This feature improvement will be useful for some of our newer international customers who had some difficulty choosing an appropriate timezone.
- **Resource Reductions: Elimination of Mongo (#212)**
  - We had previously leveraged Mongo for certain configuration and statistics. This has now been fully deprecated, and starting with this release, Mongo is no longer required. Operation is seamless and there is zero customer or usage impact.
- **Out-of-Band OS Security Updates (#237)**
  - Recent improvements in our auto-detect and installer mechanisms now permit us to support out-of-band OS security updates. This means that users can now, via our UI, update the common OS components for any security considerations without having to wait for a new software release. Effectively, this results in an out-of-band ‘apt update && apt upgrade’ cycle.
- **Allow Menu-Driven Network Selections Regardless of Installation Scheme (#251)**
  - Previously, our network selection console menuing system only applied for certain ‘box builder’ installation schemes. Since we’ve intelligently used the common netplan configuration used by the underlying OS, we’ve gone ahead and opened this up to all installation modes, which should simplify configuration and onboarding for those customers employing arbitrary hardware.
- **Warning Banner When No Bridging Pair Is Yet Configured (#240)**
  - We now incorporate a warning banner when a bridging pair has yet to be configured. This is a useful indicator for arbitrary auto-detectable hardware deployments so that the user doesn’t forget to configure one, since obviously no traffic can be protected until the bridging pair is configured.
- **Warning Banner When Cloud-Specific Configuration is Incomplete (#241)**
  - We now incorporate a warning banner relating to pertinent cloud-configuration detail that remains. For AWS, this generally means finalizing the middlebox interfaces, and for Azure this generally means finalizing the NAT configuration.

- **Logo Rebranding for our MSP Partners (#291)**
    - We've had multiple MSP partners (you know who you are - thank you!) ask us to be able to rebrand our logo to use their logo on our software pages. With this release, we provide a simple script-driven mechanism to achieve this. MSP customers wishing to leverage this ability should contact our Customer Success team for access to an example bash script to trivially utilize a new SVG logo meeting specific requirements.
- **New Landing Page (#296, #302, #313)**
    - We're super-excited about this new feature. We've completely revamped the landing page after a successful software login. Previously, it was a 'placeholder' page with a few charts with incomplete data, which wasn't nearly as accurate or useful as the data already appearing in our cloud based platform. Now, rather than duplicate information, we've changed the landing page to be things specific to the software itself, and aligned more towards troubleshooting considerations, since that's the main reason folks log into the instance (vs. the cloud based management platform) in the first place. Many of our customers have asked us for something similar for quite some time (you know who you are - thank you!) and we're happy to have delivered it! If there's other troubleshooting information you think would benefit from being included on the Landing Page, please don't hesitate to let our Customer Success team know!
- **Certificate Store Standardization (#301)**
    - We now incorporate our certificates in the local/standard Ubuntu certificate system instead of the sideloaded arrangements we previously employed. This has several advantages, including: simplifies root CA path determination, allows customers to put their own trusted certs on the box (useful for SSL inspection for those that do it), and provides us the ability to quickly change certificate vendors in the future if the need arises.
- **Support for Server-Side Feed Refactor (#324)**
    - We recently completed a major refactoring of our backend intelligence feed architecture, and this is the first software release to fully make use of the new capabilities. The result is much faster and more robust feed synchronization times, including when adding and/or removing individual feeds (to include Marketplace feeds).
- **Miscellaneous Internal Improvements (#176, #249, #288, #303, #304, #306, #307, #308, #309, #310)**
    - A variety of internal improvements were made for backend performance and operation, as well as paving the way for some exciting new backend features coming later in the year. Stay tuned!

Defect Fix Description(s)

- **Improve Auto-Detect Hardware Recognition (#290, #315, #316)**
    - Our auto-detect hardware had some difficulty detecting a few specific box builder implementations, specifically surrounding certain types of Intel NIC cards in the X710 and X540 series. We also corrected a few scenarios where manual NIC, promiscuous mode detection, and/or configuration changes could have kept the system from booting properly. These are all addressed in this release.
- **Packet Handler Process Duplication (#293, #294)**
    - This was discovered during a customer troubleshooting event (you know who you are -

thank you for your assistance in determining the root cause!) Duplicate processes were sometimes created whenever certain system processes were recycled. We've addressed this in this release. The symptom was discovered when duplicate DNS processes were contending for similar resources which caused DNS behavior anomalies. Previously the 'workaround' was to reboot the system.

- **For Cloud, Remove Features That Do Not Apply in Cloud Deployments (#219, #317, #323)**
    - During routine testing, we noticed that for AWS and Azure that a few mechanisms were left over from on-premise deployment architectures that may confuse cloud users and/or generate misleading log messages. We've removed the offending detail.
- **Fixes for SNMP Display of Bridging Interface Detail (#279)**
    - A customer routinely leveraging SNMP (you know who you are - thank you!) pointed out that our SNMP detail was missing for bridging interfaces. We've addressed that in this release.
- **Remove Duplicate Syslog Message (#292)**
    - An internal defect discovered during internal testing showed that a duplicate syslog message could be generated in internally contrived scenarios. Although we had never seen it occur in normal operation, we went ahead and fixed this to eliminate the possibility of it happening moving forward.
- **DNS Requests Now Properly Bridge in Azure Environments (#311)**
    - We fixed a recently introduced problem in Azure environments that previously required a manual workaround. The workaround is no longer needed and DNS requests are now properly bridging in Azure deployments.
- **Syslog Export Engine Resetting on Rapid Configuration Changes (#320)**
    - An internal performance/stress test scenario uncovered a problem with our Syslog Exporter where the process could recycle abnormally. Even though the chances of this happening in the wild are extremely remote, we went ahead and fixed it.
- **AWS Middlebox ICMP Unreachable and TCP Reset Generation (#321)**
    - Some internal test scenarios uncovered situations where the ICMP Unreachable and TCP Reset packets were not being properly generated when traffic was being blocked. This now works as designed.
- **Internal Defect Remediation (#287, #298, #299, #300, #312, #314, #318, #322, #325, #326)**
    - A variety of internal defects were found and fixed that related specifically to this release. One of these was related to a potential NTP anomaly at bootup and/or on certain unlikely DHCP request/renew cycles. These internal defects are tracked here for completeness, but are not otherwise expected to be customer impacting as they are unlikely to be associated with prior releases.

Release: **Build 118**

File Date: 14 Jun 2022

Purpose of the Release

This is a hotfix release that piggybacks on the recent Build 116 fixes, and addresses a second problem for certain hardware types only discovered when working with a recent customer with an atypical hardware configuration (you know who you are - thank you!), with non-standard ethernet port startup configurations that could cause their device names to change from one boot to the next.

New and Improved

- **N/A**

Defect Fix Description(s)

- **PCIe vs MAC Address Startup Discrepancies for Admin Ports on Atypical Hardware (#295)**
    - We discovered (and have now fixed) a problem with admin port determination on startup that could impact certain hardware types. It was seen in at least one customer scenario when attempting an upgrade from build 109 to build 116.

Release: Build 116

File Date: 25 Apr 2022

Purpose of the Release

This release fixes a nasty problem introduced with Build 114 for certain hardware types only, with non-standard ethernet port startup configurations that could cause their device names to change from one boot to the next. We have only seen this happen on one specific model (a Lanner NCA-1515A), but it could conceivably happen on other hardware. **As such, we STRONGLY URGE all customers running Build 114 to upgrade to Build 116 immediately.**

New and Improved

- **N/A**

Defect Fix Description(s)

- **Admin Interface Non-Responsive After Update to Build 114 (#284)**
    - It was discovered that some Lanner NCA-1515A admin interfaces were not responding upon updating to build 114. We tracked the problem down to the fact that the kernel update applied in build 114 is causing the shuffling of Ethernet device names randomly due to a new OS-side parallel interface initialization paradigm. We fixed this nasty ‘problem’ in this release by no longer relying on the discovered name, and instead relying on the known MAC. **As this problem could conceivably render devices unreachable, we recommend all customers who have installed build 114 to update to build 116 as soon as possible.** For customers who have upgraded to build 114 and are exhibiting this problem, you should contact customer support so that they can provide you guidance on how you can recover with a USB ISO reinstall.

Release: Build 114

File Date: 15 Apr 2022

Purpose of the Release

IMPORTANT: after installing this release or any release with a build number coming after it, our software will begin to connect to a new set of top-level URLs. You may need to update your other security controls as appropriate to make sure that our software can reach the new URLs (please work with our Customer Success team as needed). If you are using raw IP management in your firewalls (recommended), you're probably fine already since the static IPs have not changed. On the other hand, if you are using domains and/or SSL inspection, you will likely need to make adjustments to your external firewall configuration, to ensure that they allow traffic to and from the new top-level URL.

This release focuses primarily on a set of resource reduction requirements, which allows our software to be installed on systems with just 4 CPU cores and 8GB RAM when targeting environments with up to 1Gbps line rates. To achieve this important resource reduction milestone, the release heavily leverages technologies introduced in our recent auto-detect capability set released as builds 103 and 109. Additionally, for existing beefier systems, this software release contains some optimizations resulting in better use of existing system resources, and as always, this release contains the latest available security updates. Last but not least, we've also included some of our corporate rebranding in this release.

Although we have identified no critical need for existing customers to upgrade to this release right away, it is always our recommendation that customers upgrade at a time that is reasonably appropriate for them, to ensure that any routine underlying security updates in the underlying operating system components are properly installed.

New and Improved

- **Resource Reductions: 4CPU and 8GB RAM (#244, #245, #262, #263, #264, #265, #280)**
    - Leveraging our new auto-detect capability, coupled with a variety of internal software improvements, we are now able to install our software suite on systems with just 4 CPU and 8GB RAM.
    - For existing larger systems, a series of related internal optimizations improve overall system performance while reducing the energy footprint (for example, by reducing unnecessary CPU usage).
    - This includes installations regardless of whether they are on-premise, Vmware, KVM, and AWS.
    - However, Azure still requires larger systems, not due to the CPU and RAM, but instead because Azure's lower end systems don't support the proper number of multiple NICs required for a layer 2 bump in the wire architecture. As such, our Azure customers should continue to run their environments on 8 CPU + 16GB RAM cloud systems. If Microsoft/Azure ever supports a proper multiple-NIC environment on their lower end

cloud systems, then we will be able to adjust the recommendation.

- **Rebranding (#192, #266, #267, #268, #269, #270, #277)**
    - This release includes some work surrounding our recently publicized rebranding. None of these modifications are customer impacting, but you will notice slightly different UI screens and choices in some cases.
- **Kernel Updates / Latest Security Patches (#244)**
    - We continue to build out capabilities on top of our recent auto-detect release, and paramount amongst these is ensuring that the latest kernel security updates are readily available and seamlessly integrated into our new packaging schemes. This release extends on that, and we've implemented the ability to properly leverage multiple kernel versions as appropriate across our on-premise, virtualized, and cloud environments. Relevant kernel updates are automatically handled as part of the software upgrade process.
- **Allow Full Network Configuration for Auto-Detect Builds from our Console / Serial Tools (#281)**
    - With the advent of our auto-detect capability, we had made a choice to lock down some of our legacy serial/console network configuration capability in anticipation of users wanting to do this completely separately, but it appears we were quite mistaken in that belief. On that note, for any and all systems that we source direction and/or are installed via ISO, we now always enable full network configuration in our standard serial console menus, reachable via `/sbin/admin_shell` after suitably logging into the console.

Defect Fix Description(s)

- **Auto-Detect Install Fails on Some Supermicro Variants (#278)**
    - A customer (you know who you are - thank you!) reported a problem with our new auto-detect installation procedure on a specific Supermicro variant. We tracked this down to a missing software package, and have addressed that in this release. The previously identified workaround to manually install the missing package is no longer required.
- **Various Software Update & Install Fixes (#282, #283)**
    - A variety of minor fixes were addressed for things we discovered during internal update and install testing. None are directly customer-impacting.
    - We have also now fully deprecated the 'legacy' recovery console. Full recovery is now accomplished by a new ISO install, with up-to-date ISO images available from our Customer Success team.

Release: **Build 109**

File Date: 11 Mar 2022

Purpose of the Release

This is a fast-follow release to our milestone Build 103 auto-detect release. This addresses some non-critical, yet still important (and annoying), defects uncovered since build 103 was released. **Even**

though there are no critical items of concern, to avoid the potential for any downstream issues, it is our strong recommendation that all customers upgrade to this release as soon as possible.

Until this release is installed, it is possible that a small number of users will see 'sticking' updates - that is, you could find that you stick on Build 88 (our jump-point build) or stick on Build 103 (our auto-detect MVP release), when attempting to initiate the auto-update capability from GMC to this or to a newer release. If this happens to you, you should use the legacy manual update procedure to update, and you can certainly always contact our Customer Success team should you require more targeted assistance.

New and Improved

- **Start in Proper Core Mode when Feasible to Minimize Fan Noise (#252)**
    - Our auto-detect release was being a bit over-aggressive and was spinning up more cores than needed for some lower end deployments. This can cause larger energy consumption, which in turn causes more heat to be generated, which in turn can cause an increase in cooling requirements. The result of that is… louder fans, which can be, well, very annoying. This update to the auto-detect engine can now intelligently detect some of these scenarios, and if it can definitively determine low-interface speed operation, it'll reduce the core operational modes which will reduce the fan noise.
    - Note that this does **not** apply for higher-end systems with 10G-capable hardware (even if that hardware is currently being used in lower bandwidth deployments). That is, 10G-capable systems, even when operating at <=1G rates, will use the higher performance modes when running the auto-detect software, which means the fan noise will likely be louder on those systems.
- **Automatically Configure a Default NTP Server (#257)**
    - Up until this release, systems were shipped with no NTP server configured by default. Generally, one of the first things the end user would do when onboarding a new device would be to configure a valid NTP server. In the same way our auto-detect engine automatically configures a valid initial DNS server, we now also configure a valid NTP server. With this release, we set the default NTP server to time.google.com. The user, as always, is free to delete the reference or change to another clock source if they so choose via the appliance UI.
    - A side effect of this improvement is that it also fixes a possible auto-detect software update failure mode resulting from certain types of time discrepancies which can happen when a system has not been configured with an NTP source.

Defect Fix Description(s)

- **SMTP Config Reloads (#224)**
    - This one has nothing specific to do with the auto-detect build, but we rolled the fix in anyway. A customer reported an issue (thank you - you know who you are!) a while back where after making some local SMTP alert changes, the configuration was not reloading until the appliance was rebooted. This is now fixed, and the SMTP configuration updates will take place upon submission.
- **Recovery Console Fixes for Auto-Detect Engine (#243)**

    - The recent auto-detect release was not playing nicely with the recovery console in a few situations. We've addressed those findings. Note that our recovery console is being deprecated in favor of industry-standard best-practices USB reinstalls when needed, but in the interim we are attempting to make sure existing customers who may not be aware are still able to leverage the legacy recovery console.
- **Various Software Update & Install Fixes (#250, #253, #254, #255, #256, #259, #260, #261)**
    - Some customers ran into a variety of minor issues when attempting to update from a pre-auto-detect build to our Build 103 auto-detect release. We've addressed all known issues in this release.
    - One important consideration deserving special mention is that our auto-detect build, being our first build that can run on arbitrary hardware - even NICs without network bypass capability - now intelligently uses an internal 'software bypass' mode when performing updates, to mimic the same behavior of our hardware-bypass-capable deployments. This was important since obviously you can't rely on hardware bypass for special-case traffic propagation on systems that don't have the hardware to support it!
- **Internal Logs (Packet) Memory Usage (#258)**
    - In some internal testing we noticed incorrect memory assignments for the internal packet logs, which resulted in very little memory being reserved for them. We've fixed this. Note that although many of our smaller customers will notice significantly more packet log in-memory storage space on their appliances, it remains our **strong recommendation** to always, always, always (did we say always? yes!) export the internal logs via our RFC-compliant syslog export engine to an external syslog server of your choice. This guarantees that you have logs history dating back as long as you need for downstream analysis, limited only by the storage associated with your external system of choice. Most organizations are leveraging a SIEM of some sort to sink these logs, but the cost-conscious can always use a variety of open source tools running on low-end servers, such as syslog-ng. Anything capable of sinking RFC-compliant syslogs can be seamlessly used.

Release: **Build 103**

File Date: 17 Feb 2022

Purpose of the Release

This is an incredibly important milestone release for us. It incorporates new, advanced technologies allowing us to further coalesce our on-premise, virtualized, hybrid, and cloud-based best-in-class protection capabilities into a singular *auto-detect* architecture. We now truly have a single image build for every single architecture we support, packaged internally as an internal debian software update package which in turn is seamlessly managed for software updates through our standard cloud-based GMC, just like it has been for quite some time now.

Immediate benefits include much faster future software update times, one less device reboot on every update, and perhaps most importantly for our larger multi-device customers, the ability to install our software on arbitrary hardware meeting minimum system requirements. Previously, we supported

installation only on specific physical systems (ie, certain Lanner, Supermicro and Dell variants) that were often able to be procured only directly from us. Contact our Customer Success team for details if that is of interest to you for new deployments. For example, this gives you quite a bit of leeway in regards to what types of hardware you choose to deploy on.

In addition to providing new features and improvements, we've also incorporated minor bug fixes.

Last but not least, as with all recent software releases since Build 81, this release ensures that all of the latest Linux security fixes are applied during the update.

New and Improved

- **Auto-Detection of Hardware Base System (#21, #211)**
    - This was the primary driver of this release. Our software stack can now seamlessly integrate into any hardware meeting minimum system requirements. Gone are the days of specific model number mappings. This was critical to our ability to support customers (especially larger customers) with specific needs in the midst of a global supply chain crunch thanks to the ongoing COVID-19 pandemic.
    - As part of this critical capability, we now are also able to optionally and seamlessly install and run on systems **without** network bypass, which will be of interest to customers who want to do HA the "right" way. Put another way, we have removed the previous hard limitation that a network bypass card was required for the software to run in on-premise environments. That is no longer the case. This means that when installed in a scenario **without** the network bypass function, in the event of a catastrophic failure, traffic will stop on that leg. If you are using best practices HA, your HA management (typically a SIEM, orchestrator, or even a set of managed scripts) layer would switch over to the other leg. When bypass is in play, that is much more difficult, since it can be difficult for some external HA management systems to detect whether the system is actually down or not. Of course, we still fully support our existing and future network bypass card deployments for those customers that choose to continue to leverage the legacy bypass modes of operation, although it is our strong recommendation that customers consider implementing "real" HA practices with two redundant HA paths.
- **System Logging Improvements (#23, #208)**
    - We cleaned up many system log messages, improving severity level reporting drastically. Gone are the "errors that weren't really errors" that had caused so much customer confusion!
- **Default DNS Configured for New Shipments (#200)**
    - A common onboarding problem we've run into is folks forgetting to configure DNS the first time. This can result in a few hours of head scratching until the problem is identified. We've finally gotten around to just … fixing this. All new shipments will now ship with stock initial DNS settings using a primary DNS of 8.8.8.8 (Google) and a secondary of 1.1.1.1 (Cloudflare). As always, the end user is free to change these to whatever they'd like, but this ensures that initial onboarding connectivity works out-of-the-box.
- **DPDK 19.11.11 LTS (#235)**
    - We now ship with DPDK 19.11.11 LTS, which includes recent performance

improvements and fixes for DPDK.
    - Importantly, this version also incorporates several patches that we ourselves contributed back to the community for proper support of virtualized environments in Azure.
- **New One-Size-Fits-All ISO Installer (#202; #203, #204, #205, #206, #207, #209, #210, #215)**
    - With our new auto-detect build we now also have a new ISO installer. This is a true one-size-fits-all installer, suitable for any environment. We have successfully used it to install on our existing hardware, on third-party hardware, on Vmware, VirtualBox and KVM. Unlike our old ISO installer that leveraged some internal proprietary technologies that were hard to support and maintain, this new installer leverages standard Ubuntu Linux installer principles and best practices. Advantages include standard Ubuntu Linux installation screens that IT personnel familiar with Ubuntu Linux will have seen before. Another great advantage is that this allows us - for the first time - to seamlessly support **both** legacy BIOS and UEFI installation and booting. Previously, our systems supported only legacy BIOS modes of operation, which was quickly becoming a limiting factor in the modern world. Our Customer Success team is authorized to share our ISO image and related instructions with any of our customers who wish to burn their own USB for example for installation onto their own hardware (or virtual) infrastructure meeting our minimum system requirements.
- **Miscellaneous Internal Improvements (#17, #25, #162, #177, #214, #246)**
    - Relevant system information is now queried directly from the running system; no more reliance on hardcoded model number information.
    - Enhanced file replacements on updates for cruft cleanup.
    - Improved health and related communications to GMC.
    - Improved internal license management functions.
    - Improved internal process management.
    - Improved kernel SysRq handling to avoid startup serial port issues.

Defect Fix Description(s)

- **On-Demand Domain Search Was Incorrectly Case-Sensitive (#225)**
    - The on-demand domain search function in the device-side UI was erroneously treating string input as case sensitive. This is incorrect since domains are supposed to be considered case insensitive according to the RFCs. This is now fixed, such that all on-demand domain searches in the UI are now treated in case insensitive fashion.

Release: **Build 88**

File Date: 16 Feb 2022

Purpose of the Release

This release is an internal, jump-point release. It's sole purpose is to facilitate movement to our new Build 103+ *auto detect* architecture. The auto detect architecture is an exciting set of technologies that we are employing to further coalesce our product across on-premise, cloud, and hybrid environments. **There is no need for customers to update to this release; instead, it is**

automatically used behind the scenes when a customer upgrades from an earlier release to a 103+ release. That is, this release is internally managed by our automated GMC software update mechanism as a transient portion of the update process. When updating to a 103+ release, you may see your system temporarily report this release number before automatically arriving at its final release build destination.

New and Improved

- **Software Upgrade Support for new Auto-Detect Build 103+ Architecture (#24, #216, #221, #226, #229)**

Defect Fix Description(s)

- **N/A**

Release: Build 87

File Date: 29 December 2021

Purpose of the Release

This release contains a fix for a defect discovered internally that was exacerbated by Build 86. When the customer manually changes the administration IP (which is a very rare occurrence, typically only happening once at initial device onboarding), a database lockup could result, which could cause the system not to function properly. The workaround for the problem is to reboot after manually changing the administration IP. This release fixes that problem so that a reboot is no longer required. It is not required for customers to update to this release unless they are specifically impacted by the defect.

New and Improved

- **N/A**

Defect Fix Description(s)

- **Database Lockup Due to Administration IP Change (#197)**
    - A long-running defect in the code relating to the administration IP being changed can cause a database lockup, which happened to be exacerbated by the recent Build 86 fixes. This is now fixed.

Release: Build 86

File Date: 6 December 2021

Purpose of the Release

This release contains two important fixes. One is especially important as it fixes an issue we found

during internal testing where the root drive could fill up due to an internal database cleanup operation that was not always running properly. **Although we have not yet seen this issue impact a customer, out of an abundance of caution, we strongly urge all customers to update as soon as possible to avoid the potential for the root partition running out of usable space.**

New and Improved

- **N/A**

Defect Fix Description(s)

- **Database Cleanup Fixes (#8, #191)**
    - One of our internal boxes exhibited a problem with the root drive filling up, and we tracked the problem down to an internal database cleanup operation that was not being handled properly. We've fixed this. **Although we have not yet seen direct issues occurring on fielded systems, the potential for this happening absolutely exists, and as such, to avoid any possibility of unscheduled downtime, we strongly urge customers to update to this release as soon as possible.**
- **Eliminate Possibility of ICMP Unreachable Message Loops (#179)**
    - During some routine customer interactions, we discovered a scenario where an ICMP unreachable message loop was being generated. We've added a conditional check to ensure that the software will not source such message loops, even if they are requested, to avoid network swamping effects.

Release: **Build 85**

File Date: 28 October 2021

Purpose of the Release

This release contains a set of minor fixes. One set of fixes improves the onboarding experience when doing new installation activation where a license is retrieved for the first time. The second set of fixes addresses a defect relating to support for dual bridging in a specific legacy dual bridging hardware configuration (the BT-MS2-01C / PW-ESE-MS2-01C).

New and Improved

- **N/A**

Defect Fix Description(s)

- **Dual Bridging Fixes for the PW-ESE-MS2-01C (#146)**
    - We had previously addressed a portion of this in a prior build (Build 81) but identified a separate defect that could have caused dual bridging identification problems after a software update. This fixes that issue. It impacts only customers with the specific associated legacy dual bridging hardware platform.

- **Improve Initial Onboarding Activation (#186)**
    - In some scenarios, depending on network timing, the device UI could stay on the activate page even though a valid initial license had been obtained. This caused user confusion, which was worked around with a page refresh. This is now fixed.
- **Allow DNS to be Configured During CLI Installs/Onboarding (#187)**
    - We previously had no ability to configure DNS from our command line interface, making it difficult for users to fully activate (in lieu of using our web-based UI) especially when using a static IP to reach our cloud-based central SaaS servers for initial license activation. We've fixed this feature gap by enabling the ability to configure DNS from our standard CLI, so that users who need the ability to fully configure via our command line interface can seamlessly do so.
- **Minor Internal Improvements (#184)**
    - Minor internal improvements to our R&D build paradigm. These are not customer impacting.

Release: **Build 83**

File Date: 30 August 2021

Purpose of the Release

This release is a minor update for cloud support in AWS and our beta KVM support. It is not necessary for customers to upgrade to this release unless they are specifically leveraging KVM or AWS deployments.

New and Improved

- **N/A**

Defect Fix Description(s)

- **Missing Keys for KVM and AWS From-Scratch Installations (#164)**
    - During beta testing of our KVM customer-facing deployment scheme, a partner company (you know who you are - thank you!) found a bug with internal key propagation in KVM environments which also could theoretically impact AWS environments. We've fixed this. Our KVM support remains in beta mode, and our plans remain to bring it to full release status later this year.
- **Minor Internal Improvements and Fixes (#163, #165)**
    - Minor internal problems relating to our internal test paradigms. These were not customer impacting.

Release: **Build 81**

File Date: 18 August 2021

Purpose of the Release

This release is an important update fixing several minor defects (a few of which were customer-reported; you know who you are - thank you!), and adds some exciting new features. One big feature is the elimination of registration codes for new device registration! This **greatly** simplifies both on-premise and cloud deployments for our customers.

New and Improved

- **Faster Startup (#12, #143)**
    - We made some internal optimization improvements to our device startup time, especially when loading dynamic lists immediately after boot-up. Generally this is only valuable after software updates have finished and the system is rebooted during customer-scheduled maintenance windows, but the end result is reduced wait times for the system to be fully functional again after being updated.
- **Positive Acknowledgement on Logout (#15, #154)**
    - We've always had a positive acknowledgement message when a user manually logs out of the device UI, but now we also show a meaningful dialog upon device-side UI logout due to configured inactivity periods.
- **Detailed NTP Information (#20)**
    - Our Date & Time display now shows detailed synchronization information about the system NTP configuration. This can be very useful when troubleshooting timing problems due to specific customer-side NTP usage.
- **Base System Bootstrapping Automation (#138)**
    - We built an automation to ensure that we are picking up the latest security fixes for the base Ubuntu LTS system on each and every build, and fully test the complete system configuration as part of each build cycle. Previously this was a more time-consuming manual process. In addition to freeing up developer time, this should also ensure that we don't inadvertently miss important base system security updates.
- **Registration Code Elimination (#140)**
    - We no longer require registration codes when onboarding new on-premise or cloud devices, which greatly simplifies the onboarding process. In place of entering a registration code, customers onboarding newly purchased on-premise devices (or deploying new cloud based architectures) simply log into GMC from a proxy screen presented by the device, which performs full registration and licensing automatically.
- **Support for 6-core Configurations (#142)**
    - We're doing our level best to reduce the overall system requirements over the long-term. This is phase one of that. We are now able to support full line rate performance on 6-core systems, even when running at our flagship 10 gigabit full bandwidth bidirectional rates. Previously we required 8-core systems in such environments.
- **(BETA) Support for Deployment on a KVM Host (#149)**
    - We've used KVM internally for R&D purposes for quite some time, but after some customer interest, we're releasing support for installing in KVM environments as beta. We'll bring this to full release later this year.
- **DPDK 19.11.9 LTS (#152)**

    - We now ship with DPDK 19.11.9 LTS, which includes recent performance improvements and fixes for DPDK.
- **Support for Lanner NCA-1515A Set Top Hardware (#155)**
    - Our preferred Lanner set top hardware is the NCA-1510D, however, we now also support the NCA-1515A. It's very similar in feature and function to the NCA-1510D. The NCA-1515A is a few inches deeper in dimension and embeds a small fan (vs. the NCA-1510D which is entirely passively cooled). The main reason we are supporting the NCA-1515A is we anticipate having to ship a few of those in lieu of NCA-1510D equipment due to world-wide supply chain issues that continue to result from the impact of the ongoing COVID-19 pandemic. Our software runs identically on both device types.

Defect Fix Description(s)

- **DNS Caching (#50)**
    - We had a rather nasty defect where the device could generate DNS resolution requests for our primary endpoint connections tens of thousands of times per day. This is now fixed.
- **REACT Missing from Reasons Dropdown (#132)**
    - We noticed during some internal testing that 'REACT' was missing from our Reasons drop-down in our internal logs view. This is now fixed.
- **UNNAMED_TAG Internal Markers Showing Up Where They Shouldn't (#134)**
    - A missing code pathway when deleting a source/tag value for a feed could result in UNNAMED_TAG attribution labels. This is now fixed.
- **Link State Change Logs Not Working (#136)**
    - During internal testing we noticed that we were no longer seeing log messages detailing change of link state on the inside and outside port. These log messages have now been restored.
- **Import Resource Group Fixes (#139)**
    - We fixed a few problems encountered when assisting customers upgrading from our legacy 1.0 codebase to our new 2.0 codebase, specifically surrounding some nuances with importing and configuring resource groups and policies.
- **GRE and Related Long-Lived Connection/Packet Decisions (#147)**
    - We had some internal timeout vs. harvesting considerations that could have caused some long-term connection packets to be evaluated incorrectly. This was seen in a live customer environment with GRE packets, but could have had a similar effect with other nuanced packet types. This has been fixed.
- **Intermittent Startup Failures on a VMware Host (#148)**
    - When doing some internal testing we noticed a very intermittent startup problem relating to some non-deterministic VMware startup nuances on our internal VMware test cluster that we use for ongoing device software testing. We fixed this by adding some detection/synchronization logic when operating on a VMware node.
- **Software Update Scripts Have Sporadic Trouble with AWS S3 Stores (#150)**
    - We noticed an internal problem when processing software updates for some AWS S3-hosted files (which is our preferred software update delivery platform). We fixed this, and also modified some backend control processes to make sure that units impacted by this defect are still able to process software updates.

- **Minor Internal Improvements and Fixes (#4, #5, #10, #11, #141, #146, #156, #159)**
    - We also made a series of internal minor improvements and fixes, mostly associated with some specialty legacy configurations as well as some minor nuances in our installation/CLI screens.

Release: Build 76

File Date: 24 March 2021

Purpose of the Release

This release is a small update to fix a few minor issues. It is not necessary for customers to upgrade to this release unless they are specifically impacted by these fixes.

New and Improved

- **N/A**

Defect Fix Description(s)

- **Internal Software Download Clutter (#14)**
    - During internal testing, we noticed that some of the software update directories were getting cluttered with old versions. We cleaned those up out of an abundance of caution, since it appeared possible that the 'wrong' update (an older one) could conceivably have been updated instead of a desired newer version.
- **REACT Lists not Synchronizing Properly (#130)**
    - Very few of our customers are leveraging our legacy REACT list functionality, since it is effectively an albatross now. That's because our innovations in denied list and allowed list handling obviate the need for our legacy REACT style operations. However, some of our customers who have migrated from our legacy architecture to 2.0 are still reliant on the old REACT APIs, and we had one customer report an issue where the REACT lists weren't synchronizing properly from GMC down to the device. We tracked this down to a problem localized to our recent Build 75 release. Customers that have installed Build 75 **and** make use of our REACT functionality will want to upgrade to this release in order for the REACT functionality to work properly.
    - Also, if you are one of those customers, we do recommend that you consider migrating off of our legacy REACT architecture and use standard denied and allowed lists instead. This is because at some point in the near future we will likely be deprecating the legacy/redundant REACT features.
- **Export Configuration Tab Missing on the UI for Cloud Installations (#131)**
    - During internal testing, we discovered that a bug existed in the UI presentation for our cloud variant in AWS, which kept the export tab from appearing on the Import/Export configuration screens in that environment. The page was still available and could be manually accessed, but now we've gone ahead and fixed the UI bug.

Release: Build 75

File Date: 4 March 2021

Purpose of the Release

This release is an important update that adds new features while fixing several defects. Some of the defects were discovered by customers - you know who you are, and we thank you!

Important security updates are included in this release, including remediation for the highly publicized Linux vulnerability CVE-2021-3165, as well as a new set of updates to DPDK. There was also a **critical** fix in our own software stack this release, relating to an out-of-bounds condition on ASN indexes which was exacerbated after February 19, 2021 with new ASN mappings that came online. **This is critical - devices without this fix will continue to use the ASN and country registration information as of February 19, 2021, and will not be able to receive updated ASN information from our central GMC management platform until this software release is installed. As such, we urge all of our customers in the strongest of terms to upgrade to this release as soon as possible.**

New and Improved

- **New 'Description' Field for Syslog Export Configurations (DEV-1449)**
  - Our customers that use our syslog export capability (and if you're not, you should!) may or not be aware that you can export the logs to as many external sources as you'd like. When you've got more than one, it can be difficult to know which is which. To improve the user experience, you can now add an optional free-form text description to your syslog export configurations, so that you can more easily identify what you're connecting to at a quick glance.
- **Dell+Silicom Hardware Now Support Hardcoded Speed and Duplex Settings (DEV-1776)**
  - We now support software-configurable hardcoding of speed and duplex for our Dell server + Silicom card solutions. This can be a useful workaround for customers with very old networking or firewall equipment that don't support auto-negotiation standards.
  - No, this feature is not available on our lower-end equipment, due to hardware limitations on the lower-end equipment. For those devices, auto-negotiation is typically required.
- **Completion of Certificate Management Subsystems for UI Security (DEV-1939, DEV-2061)**
  - We had never finished the certificate management subsystem, which meant that customers had to utilize browser features to accept security exceptions in order to connect to the device UI 'securely'. We have now completed this work, and we believe it now has comprehensive support for importing a certificate created from a certificate signing request (CSR), plus also support for full PKCS12 certificate chains, including intermediate certificates.
  - This means that customers that want to sign access to their devices with a recognized CA should now be able to do so.
- **Using a Common Access Dialog Framework in the Device UI (DEV-2011)**

    - We consolidated some of our access dialog stuff in the device UI for a more consistent user experience across the various views.
- **Intelligent Policy Assignment for Resource Group Imports (DEV-2065)**
    - When importing resource groups, we now check to see if a matching policy exists in GMC, and if we find one, we automatically apply it. This is a fantastic time-saver when importing information during device configuration.
- **Reduction in Download Image Sizes (DEV-2068)**
    - We underwent a series of internal build system optimizations and in so doing were able to greatly reduce the total size of our download images, both for on-premise and cloud deployments. This will result in more rapid system updates.
- **Cloud Deployment Assistance (DEV-2070)**
    - We added some extra error checking when logging in to a cloud deployment to make sure the system was spun up properly. If we detect an anomaly, we point the user at our comprehensive cloud deployment documentation via hyperlink from the software itself so that they can address any issues in their AWS environment to ensure a proper deployment architecture.
- **DPDK 19.11.6 LTS (DEV-2072)**
    - We now ship with DPDK 19.11.6 LTS, which includes recent performance improvements and fixes for DPDK.
- **New Domain Resolution Logs Export (DEV-2085)**
    - By popular demand, we have an **exciting new log export** now that contains DNS resolution details for A and CNAME responses! There is no device UI view for this - it is only available if you export the logs via our RFC-compliant syslog export mechanism after updating your device configuration's *Logging > External Syslog* configuration appropriately. Additionally, we've updated our comprehensive syslog export documentation with detailed formatting for this feature, which you can get from our Customer Success site or by contacting our Customer Success team.
    - The new exported detail can be very useful information to assist with detailed logs analysis and correlation with other available details, such as when exporting our detailed logs to powerful external SIEM tools, or even simple ultra-low-cost syslog-ng sinks where you're simply storing the data for analysis downstream as simple text files (which is what we do ourselves!).
- **Internal Improvements to Better Track Feed Synchronization (DEV-2087)**
    - We've been blind to some recent feed synchronization issues (often resulting from customer-side networking considerations), and these improvements will help our Success team when working with customers to troubleshoot such issues.
- **Add More Info to the System Information UI Panel (DEV-2093, DEV-2102, DEV-2108, DEV-2113)**
    - When available, we now include the system uptime and certain serial number information in the System Information panel in the device UI.
- **Improve Audit Logs Relating to License Removals and Additions (DEV-2094)**
    - We now have customers contemplating moving infrastructure to the AWS cloud, and we support the ability of a customer to remove a license from one unit and attach it to another. However, we weren't being very verbose about this in the Audit Logs, which was causing some confusion, and so we've extended the Audit Logs to have more

meaningful information included when license swapping is undertaken.

Defect Fix Description(s)

- **A ‘bus error’ Caused by Use of a Domain Name in Syslog Export Configs (DEV-1961)**
  - A ‘bus error’ message is kind of a catch-all error message in some system components, and we had a customer run into one. We tracked it down to the use of a domain name in a syslog export configuration, which wasn’t properly supported. We have updated the configuration handlers to properly support the use of DNS names in the syslog export configuration, so customers that would prefer to use them instead of numeric IPs can do so now.
- **A 422 Error is Reported in the SNMP Dialog (DEV-2010)**
  - We fixed this minor error. Note that the internal error was an extra PUT operation after a POST, where the PUT caused the 422, but the desired operation actually succeeded.
- **Missing Risk Threshold Categories on Device-Side UI Display (DEV-2031)**
  - The device UI was missing recently added Risk Threshold categories. This is now fixed.
- **Importing a Configuration Block Doesn’t Show Up in the Audit Log (DEV-2071)**
  - When assisting a customer with an upgrade, we noticed that importing a configuration didn’t get audited properly in our logs. We’ve fixed this.
- **Minor Internal Fixes (DEV-2077)**
  - We fixed a few other internal non-customer impacting things in this cycle as well, such as some internal marketing-related naming changes in some of our cloud-based stuff.
- **Source and Destination Port Information Now Appear in our Domain Logs (DEV-2084)**
  - In our ongoing efforts to make our exportable device logs (via our Syslog Export features) better and better, we have added source port and destination port information to our Domain Logs.
- **Warning/Error Banner Fixes in the Device UI (DEV-2089, DEV-2095)**
  - At the top of the device UI we embed a small banner area where we can display warning/error messages that may be meaningful to the user, such as when there is a device licensing problem or when GMC connectivity is sporadic. There were a set of defects relating to the timely display (and clearing) of such information that we have now addressed.
- **Double Quotes in ASN Names (DEV-2091)**
  - We’ve stripped double quotes appearing in ASN names. Our system handles this condition properly, but it could cause problems in downstream systems attempting to parse the syslog export data. We noticed a nefarious Ukrainian service attempting to use this scheme, which could conceivably be used as an attack vector against poorly constructed syslog parsers in use in various SIEM or SIEM-like tools.
- **Loose State Handling (LSH) Algorithm Collision (DEV-2096)**
  - We’ve revamped our loose state handling algorithms to be more deterministic. A defect where a non-deterministic decision could have resulted when resource group matches occurred has been addressed. Additionally, we are now applying LSH algorithms only to TCP traffic. For UDP traffic, packet direction trumps in LSH determination.
- **Internal Routines Now Requery License Settings (DEV-2097)**
  - A license migration error, most often seen when performing a legacy device upgrade to our newest software, could have caused some internal processes to use the wrong

license. We have been internally working around this problem manually in our production database. This is now fixed.

- **Mitigate CVE-2021-3156 (DEV-2105)**
  - **Because of the critical nature of this defect in the underlying Linux architecture, we recommend, in the strongest possible terms, that customers upgrade immediately to this build.** CVE-2021-3156 is a critical defect that impacts most worldwide infrastructure leveraging open source Linux over the past decade. The defect was a least-privilege escalation bug with a standard variant of the popular sudo tool, which ships as a stock part of most Linux distributions, including Ubuntu 18.04 LTS Server which our system is currently based on. On an impacted Linux system, this defect would allow any logged in shell user to potentially gain root access. We have fixed the defect - as has most of the world at this point, if they're smart. If you have other Linux-based systems in your infrastructure, we strongly recommend that you update them (and/or work with your vendors to do so) as soon as humanly possible.
- **Domain Lookups for Block and Allow Determination Should be Case-Insensitive (DEV-2109)**
  - **Because of the critical nature of this defect, which we have discovered exists in all previously released versions of our software, we STRONGLY advise all customers to update immediately.**
  - We found that a malicious actor could conceivably bypass our domain protection by using mixed-case domain names. We have corrected this, and now all domain name checks are properly performed in case-insensitive fashion.
- **NTP Servers Not Being Recognized (DEV-2111)**
  - Build 68 introduced a defect where configured NTP servers were being ignored. This is now fixed. Please note that you may see a pair of 'red' error-level messages relating to the ntpd system daemon show up in the internal system logs early in the startup sequence on first-boot after installing this release. That is normal, and they can be safely ignored.
- **Metadata Healthcheck Information Timestamps Incorrect (DEV-2112)**
  - The metadata health check information that is occasionally sent back to our centralized GMC platform was being timestamped as local timezone, but should have been UTC. It is now UTC as required by our backend metadata logic.
- **Internal Process Cleanup Fixes (DEV-2114)**
  - As part of an internal review, we identified a few processes that were not cleanly exiting on various abort conditions. These are now fixed, and standardized.
- **Miscellaneous Internal Fixes (DEV-2115, DEV-2116, DEV-2120, DEV-2124, DEV-2126, DEV-2128, DEV-2129)**
  - Various internal, non-customer impacting fixes were made. This included serial number propagation, multiple startup failure logging fixes/improvements, internal hanging transaction cleaning, internal build system modifications, and some minor systemd follow-up work stemming from our previous Build 68 release.
- **Extension Support for License Expiration (DEV-2117)**
  - An internal ordering problem which precluded license extensions from working is now fixed. A workaround did exist for this problem, but involved a system reboot. Once this code is installed, that workaround is no longer required for a license to be extended

after expiration occurs.

- **Deleting a Resource Group Displaying Incorrect Error Messages (DEV-2118)**
  - An issue with resource group deletion on the device that could have resulted in erroneous error messages being generated was fixed. However, even though the messages could be displayed, the resource group was still correctly removed.
- **Extend the Total Number of Supported ASNs (DEV-2130, DEV-2132)**
  - The internal device ASN limits were reached, and we have extended them in this release. **This is critical - devices without this fix will continue to use the ASN and country registration information as of February 19, 2021, and will not be able to receive updated ASN information from our central GMC management platform until this software release is installed. As such, we urge all of our customers in the strongest of terms to upgrade to this release as soon as possible.**

Release: Build 68

File Date: 23 December 2020

Purpose of the Release

This release is an important update that adds new features while fixing several defects. Some of the defects were discovered by customers - you know who you are, and we thank you! Critical new additions in this release include the migration from Python 2 to Python 3, as well as the migration from DPDK 18.11 to 19.11. Because of these important changes, **we strongly recommend that all customers upgrade to this release as soon as possible**. We say that because community support for Python 2 is drying up, which means that unpatched Python 2 and related library security holes become a real concern over time. Similarly, community support for DPDK 18.11 has ended, with long term support guidance now attached to DPDK 19.11.

New and Improved

- **Support our new Dual Rate (1G and 10G) Capable Hardware Coming in 2021 (DEV-1937, DEV-2024)**
  - We'll soon be shipping new hardware that will be able to be configured in software for either 1G or 10G operation. This will provide a nice software upgrade path for current 1G customers when they need to migrate to 10G downstream, without requiring hardware upgrades, as long as the medium choice (copper or fiber) is consistent.
- **Internal Logs Wrap Predictions (DEV-1966)**
  - A message is now displayed on our internal logs screen(s) that gives the user an idea of how long it will take the internal logs to wrap given recent usage patterns. We also note the importance of using our RFC-compliant syslog export feature for long term logs storage.
- **DPDK 19.11.5 LTS (DEV-2041)**
  - We now ship with DPDK 19.11.5 LTS, which includes recent improvements and fixes for DPDK. Note that the prior LTS version of DPDK, 18.11.8, is no longer under active support by the community, **so we consider it imperative to upgrade to this release to**

ensure timely support for any future DPDK security fixes and performance improvements.

- **Python 2 to Python 3 Migration (DEV-1825)**
    - This was a critical change that was needed given that Python 2 is now, for all intents and purposes, a dead language, and the community support for it is rapidly drying up. We have therefore migrated all internal subsystems that utilized Python 2 to Python 3. Because of this, **we strongly recommend that all customers upgrade to this release as soon as possible.** We say that because community support for Python 2 is drying up, which means that unpatched Python 2 and related library security holes become a real concern over time.
- **Ability to Move Licenses (DEV-2039)**
    - This is a key new feature that allows users to more easily move licenses between systems. This has a variety of uses, but the main use case driver was for customers with on-premise installations that are migrating infrastructure to the cloud. This feature now allows them to seamlessly turn down service for one of their on-premise devices and transfer the license for use at another location, to include the cloud.
- **AWS Feature Merges (Various)**
    - This release, and all subsequent releases, marry our cloud and on-premise technology, which means that the same build versions can be applied to both your on-premise installations as well as any cloud installations that you've deployed in AWS.
        - Our current cloud offerings exclusively deploy via AWS Marketplace with a bring-your-own-license (BYOL) model, allowing you to protect your AWS-native cloud infrastructure with the same technology that our customers rely on for their on-premise infrastructure.
        - For questions about deploying us on AWS, please contact our Customer Success team.
        - In 2021, we'll be rolling out support for Microsoft Azure and Google Cloud Platform. Our current projections have us finishing up this work no later than the end of June 2021.
- **Other minor internal improvements (DEV-1828, DEV-2000, DEV-2040)**
    - A variety of minor internal improvements were also made. These included:
        - some internal database logging changes for more efficient troubleshooting,
        - a migration to systemd for improved system bring-up and management, and,
        - an increase to our threat intelligence filter sizes.

Defect Fix Description(s)

- **Updated Bypass Control for Lanner Set-Top Boxes (DEV-1797)**
    - We have updated the control software that we use for bypass control, and are now operating it as a kernel module to eliminate any possibility of bypass driver contention. We had not explicitly seen any directly attributable adverse effects in the wild, but this was a prudent change made out of an abundance of caution.
- **Domain Log Searches Failing When Using IP Source or Destination Filters (DEV-2062)**
    - We've fixed a problem with domain log searches in our internal logs. Prior to this fix, using the IP source or destination filters when searching the domain logs would produce incorrect results. This has been fixed. A big "Thank You!" goes out to the customer that

identified this problem for us.

- **Configuration Import Defects (DEV-2063, DEV-2064, DEV-2067)**
    - There were three defects identified by one of our customers that were found when they were attempting to export and re-import device configuration data:
        - First, resource imports were not properly considering resource direction which caused an invalid error message to be generated.
        - Second, the ‘check all’ import box wasn’t working properly. There was a workaround to manually check each box individually, but with this fix the ‘check all’ function works as intended.
        - Third, imported service groups were erroneously reported as being managed by GMC, which is not yet possible (although that is a feature we’ll be working on in 2021). Both of these have been fixed and we thank the customer who identified them for pointing them out to us!
- **Special Characters Precluded Default ASN Data From Loading Properly (DEV-2069)**
    - This was a minor issue that we discovered internally when doing some routine testing. When a device is first installed (typically at one of our box-build partners), prior to being configured for connection to GMC, there is a default ASN list that exists in the installation. That list was not loading properly due to special character handling. This has now been fixed. Note that this defect is not believed to impact any customer, since once customers are properly bolted to GMC, the GMC-provided lists override the default lists, and the GMC lists do not exhibit this issue.
- **Automatic Software Update Could Result in a Defunct Process (DEV-2073)**
    - This is a minor internal issue, but we noticed the possibility of a defunct process resulting from the automated software update mechanism. This is now fixed.
- **Integer Math Overflow Error (DEV-2075)**
    - We fixed an internal logs wrap prediction messaging problem relating to an integer overflow math defect that could cause a UI error message to pop up.

Release: **Build 59**

File Date: 3 December 2020

Purpose of the Release

This release fixes four defects, two of which were found internally, and two of which we found when troubleshooting directly with one of our customers. To that customer - you know who you are - thank you for helping us get to the bottom of these issues!

New and Improved

- **N/A**

Defect Fix Description(s)

- **Data Validation on an Internal File (DEV-2037)**

    - An internal data validation issue existed for a specific set of informational data. We don't believe that there was any possibility of impacting customer use, but we fixed it anyway out of abundance of caution.
- **List Tag Inconsistency On Removal (DEV-2042)**
    - We discovered an internal condition where removal of entries from a list did indeed properly remove from the database, but they could still erroneously be tabulated in logs as still existing in the source it was removed from. This is now fixed.
- **DNS Proxy Failing for Sizes > 512 Bytes (DEV-2056)**
    - An internal buffering problem occurred for certain DNS requests larger than about 512 bytes, causing the request (and/or the reply) to not be propagated. This is now fixed.
- **Software Watchdog Timer Race Condition Caused a List to Hang (DEV-2057)**
    - An internal timing problem with a specific software watchdog as it relates to list management could result in the list being hung, which kept it from populating, although the system would otherwise proclaim everything was fine. It wasn't. This is now fixed.

Release: **Build 58**

File Date: 19 November 2020

Purpose of the Release

This release fixes a few minor defects. If you're already on build 57 (the prior release to this one), there's no explicit need to install this update unless you are impacted by one of the defects documented below.

If you are currently on build 57 and want to upgrade to this new build 58, note that this is the first time you'll be able to use our cool automated software update feature from the GMC Assets page, since the automated update feature requires a minimum installed build of 57 to function. Give it a try!

New and Improved

- **N/A**

Defect Fix Description(s)

- **CPU Clobbering By an Internal Process (DEV-2038)**
    - During routine internal testing, we noticed an internal process that was not properly giving up CPU resources, which caused a CPU core to spin needlessly. This did not in any way impact system performance, but it did unnecessarily consume system resources. This is now fixed.
- **New User Creation (DEV-2043 and DEV-2044)**
    - Our new user creation routines had two defects. The first defect was that we weren't properly enforcing the password rules for required character groups, which caused confusion on initial password entry when adding a new user. The second defect was that after creating a new user, the system didn't actually create it. A workaround to coax it into creating it was to go back to the users list and edit the new user's credentials to

re-enter the password. Both of these defects are now fixed.
- We'd like to thank one of our (potential!) customers/partners for discovering these two defects and letting us know about them! You know who you are! Thank you!

Release: **Build 57**

File Date: 29 October 2020

Purpose of the Release

This release fixes a couple of minor bugs, provides rebranding, and adds an exciting new feature to simplify and automate the software download process moving forward.

New and Improved

- **Automated software download support (DEV-1684)**
  - We're excited to release our new automated software download scheme. Our users still have 100% control over the download process, and we've left the old manual mechanism in place, but this exciting new feature allows our users to, at their discretion, perform an automated or scheduled download (or, when applicable, even reverting). This means you'll no longer have to manually download our full secure images only to turn around and manually upload them.
- **Rebranding (DEV-2032, 2033, 2034, 2035, 2036)**
  - We've rebranded!

Defect Fix Description(s)

- **Database connection slot problem (DEV-1958)**
  - We had seen this problem at two separate customer sites over the past several months, and in both cases it was cleared by a system reboot. We were finally able to internally reproduce this issue and we tracked it down and have now fixed the root cause issue to this extremely rare problem.
- **Internal buffer size problem (DEV-2027, partial)**
  - We noticed a buffer size problem with an internal DPDK buffer that we went ahead and fixed. We hadn't seen any issues either internally or in customer environments related to this, but regardless, it is now corrected.

Release: **Build 51**

File Date: 9 October 2020

Purpose of the Release

This is a minor release adding a specific software build number for one of our box-build partners.

There is no need for end users to install this release (but it doesn't hurt if you do).

New and Improved

- **Adjusted software build configuration number (DEV-2029)**
    - We added a new internal configuration (extends on DEV-1938) software model for some new COTS hardware being used by one of our box-build partners.

Defect Fix Description(s)

- **Initial box-build installs not properly starting list update services (DEV-2030)**
    - We introduced a problem recently when adjusting some of our list naming conventions which kept list services from properly starting on the device for brand new installs shipping from our box-build partners. The issue had no bearing on previously installed customer equipment. Regardless, this is now fixed.

Release: **Build 49**

File Date: 25 September 2020

Purpose of the Release

This is a minor release adding a specific customer requested feature relating to SNMP support. If you don't need SNMP support for bridge pair monitoring, then there's really no need for you to install this release.

New and Improved

- **SNMP monitoring of bridging interfaces (DEV-2016)**
    - We now have the hooks in place to leverage SNMP for monitoring our DPDK-managed bridging interfaces. We had a customer ask us for this since they were used to leveraging SNMP on our legacy software to monitor their bridge pairs, and wanted to be able to do the same on our newer software.
- **Other minor internal improvements (DEV-1938)**
    - We added a new internal configuration for some future stuff we have planned.

Defect Fix Description(s)

- **Minor fix to catch an error and create a missing directory (DEV-2023)**
    - A very minor internal error is now handled properly. It was causing no real issue since the defaults that were used on fallback were correct, but regardless, it is now fixed.
- **Corrected a loose state handling configuration problem on an initial box build (DEV-2025)**
    - This one impacted our hardware build partners/integrators, but does not impact our end customers. We missed an initial box-build configuration step related to the loose state handling feature we added in build 48. This means our build partners will be shipping

new systems with build 49.

Release: Build 48

File Date: 16 September 2020

Purpose of the Release

This is an exciting release, as it finalizes our planned work and improvements for our already exciting syslog export features. Several new features while fixing several important defects, including two serious defects, one of which is a security vulnerability - **and thus it is our strong recommendation that all customers upgrade to this release as soon as possible**.

New and Improved

- **Final planned round of major syslog export improvements (DEV-1974, 1981, 1984, 1996, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2015)**
    - With this release, we have finished our last planned major round of feature extensions and improvements to our already-powerful syslog export features. We have streamlined the key value pairs, so you may need to update your parsers if you were pulling out connection information from our exported packet logs related to denied lists, allowed lists, and threat lists, especially.
    - Furthermore, with this release, we have fully documented our user-facing official RFC-compliant syslog export format as “version 1”. For a detailed descriptive document, feel free to reach out to our Customer Success team. Of course, we will continue to have minor improvements to our syslog export features over time, but we’re really excited since this release contains the last big-ticket items that we had planned.
    - For one of these items, we’d like to explicitly thank the good folks at Gravwell, who pointed out that we really ought to consider publishing the RFC-compliant APP-NAME field to uniquely identify our application. Consider it done! Gravwell is a preferred partner of ours for analysis and visualization of our awesome syslog export detail, and we highly recommend you check them out at https://gravwell.io. We also recently partnered with Gravwell to create a built-in “Kit” that customers can download directly from the Gravwell ecosystem for out-of-the-box queries and dashboards against our powerful syslog exports.
- **Add loose state handling detail to internal logs and syslog exports (DEV-1802)**
    - We now publish our loose state handling (LSH) connection direction determination data for cases where we were unable to “see” the initial SYN or SYN/ACK packets. Generally, our loose state handler operates by performing high-port-number analysis in real-time. When we leverage LSH (which is rare as usually we can definitively determine the direction), we now show these occurrences with small UI elements on the Internal Logs page. Additionally, when leveraging loose state handling, we also export a new key-value pair “lsh=true” in the associated syslog export, which can be parsed if desired in connected SIEM tools.
- **Minor improvements to our administration and recovery menus (DEV-1834, 1873, 1965,**

1991)
    - These include better software version visibility, a CLI shutdown option, DHCP configuration, and more.
- **Other minor internal improvements (DEV-1823, 1894, 1994)**
    - These are a variety of internal features, wording changes, and behind-the-scenes improvements to performance, towards our perpetual goal of always improving the overall customer experience.

Defect Fix Description(s)

- **Allow only TLS 1.2 for secure connections (DEV-2009)**
    - **<u>We consider this a significant security vulnerability and strongly recommend that all customers upgrade to this release as soon as possible.</u>**
    - We would like to thank one of our customers (you know who you are!) for pointing this out to us; after an independent vulnerability scan, they found that in addition to properly allowing TLS 1.2, we were erroneously allowing TLS 1.0, TLS 1.1, and SSLv3 by default. This is bad since TLS 1.0, TLS 1.1 and SSLv3 all have known security vulnerabilities that can result in insecure communications when exploited by a clever attacker. This is now fixed, and we now only allow TLS 1.2 for secure communications channels.
- **Historic session purging was broken, potentially causing UI login lockout (DEV-2022)**
    - **<u>We consider this to be a significant defect and strongly recommend that all customers upgrade to this release as soon as possible.</u>**
    - This particular problem was discovered internally, and has not been witnessed in the field yet, but it could show up, so we thought it best to get it fixed as soon as possible. There was an internal database contention problem keeping historical session logs from being properly cleared, which, in the worst case, could have resulted in access by either API or the UI being denied. This has been fixed.
- **Corrected a potential stale-data condition in system log exports (DEV-2014)**
    - A minor internal condition existed where a structure was not being cleaned, which could have resulted in stale data being output in some system log export scenarios. This was discovered internally, and has not yet been witnessed in the field. Regardless, it has been fixed.
- **The threat category roll-up information sent to GMC needed to be more intuitive (DEV-2017)**
    - You could argue that this is a feature improvement, but it caused enough questions amongst our customers that we decided to classify this as a defect. We had gotten ahead of ourselves a bit with all of the cool attribution that our software has in place, and we over-complicated some of the metrics, which caused some confusion. This is in comparison to our legacy software which was very limited in its ability to do attribution, but more intuitively mapped to our GMC security posture dashboards. With this fix, we made sure that the data being rolled up to GMC was as intuitive as it used to be, without sacrificing our ability to do detailed attribution in our awesome syslog exports. What does this mean? Basically, it means that the “Allowed by Category” and “Denied by Category” GMC dashboard graphs will no longer show excessive data/counts. They are now intuitive in that the “Allowed by Category” graph means a category was found but

allowed through because its score was below a configured threshold. And “Denied by Category” means a category was found to be associated with a connection that was denied (for any reason). We apologize for getting ahead of ourselves and over-complicating this statistic - and a huge shout out to one of our best customers (you know who you are!) for helping us get our heads around the best way to “solve” this nagging concern!

Release: **Build 42**

File Date: 10 August 2020

Purpose of the Release

This release is a hotfix release for two specific problems. One was discovered internally, and one was brought to our attention by a customer. We also included a key improvement to an existing feature that will have great value in an upcoming update to our GMC SaaS application.

New and Improved

- **Include Bypass Information in all Healthcheck Data (DEV-1989)**
    - We recently revamped our GMC backend and frontend architecture ahead of some exciting new features that are coming soon. One of these features includes the ability to show more detailed information about a company’s devices at the GMC level, to include information about whether a given system is in bypass mode or not. We had some of this information being transmitted between the TI Firewall and GMC already, but this feature provides the data ubiquitously.

Defect Fix Description(s)

- **Intermittent Device Synchronization Problem with GMC Manual IPv4 Lists (DEV-1987)**
    - We ran into a rather nasty intermittent device synchronization problem, reported by one of our customers. A sincere “Thank you!” goes out to that customer for reporting the problem to us and working with us on resolution! You know who you are!
    - We were able to identify a workaround, but it was not an especially easy to apply workaround. Thankfully, we’ve been able to isolate the issue, and this fix should remedy it. Since it manifests intermittently, we believe that other customers may run into this problem sporadically. Since it is extremely important that manually added IPv4 list entries (such as, for example, to add a false positive IP to an existing manually crafted allowed list) take effect properly every time, all the time, we decided it was important to push this release immediately out-of-band as a hotfix.
    - **We consider this a serious defect and we urge all customers on a prior build to update to this build as soon as they can, and especially if they run into problems adding IPv4 addresses to manually crafted allowed and denied lists.**
- **TCP Reset Packet Handling Fix (DEV-1993)**
    - Our TCP Reset packet handler on drops is a fairly typical and recommended approach

for notifying a protected system of an outbound TCP connection that was blocked. There was a defect in the handling that could cause the controlling process to fail on non-TCP traffic. Our internal software watchdogs were able to detect this and fix things behind the scenes, but we removed the possibility of this happening in the future with this update, thereby ensuring performant and accurate TCP Reset generation.

Release: **Build 40**

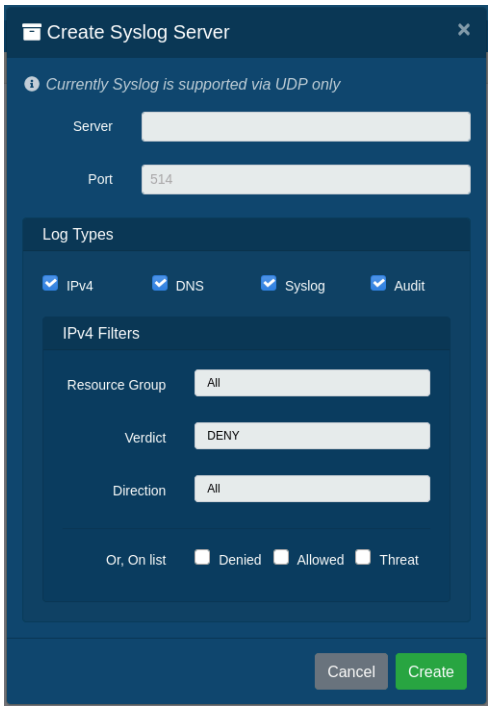
File Date: 31 July 2020

Purpose of the Release

This release continues our trend of significant improvements to our syslog export engines, adds a few other nifty features, as well as addresses a few minor defects.

New and Improved

- **Logs Clearing (DEV-1661)**
  - Our in-memory device logs are always cleared on reboot, but now they can be cleared on-demand at runtime with no impact to network and security performance. This can be very useful when doing security triage in real-time.
- **Jumbo Frame Support (DEV-1895)**
  - We now support jumbo frames in our enterprise-caliber Dell R340-based 1G-X and 10G-X systems, which we outfit with special bypass NIC cards leveraging robust Intel chipsets. No extra configuration is required, as our software stack natively configures the hardware for maximum jumbo frame support, up to the capabilities of the specific chipset. Generally, for our 1Gbps systems, the maximum jumbo ethernet (including header and CRC) frame size supported is 9234 bytes. For our 10Gbps systems (which leverage different Intel chipsets), the maximum jumbo ethernet (including header and CRC) frame size supported is 15872 bytes. Note that these frame sizes are subject to change, depending on a variety of hardware and software factors.
- **Logs Export Filtering Extensions (DEV-1907)**
  - Our syslog export capabilities continue to be extended and are now even more powerful. We can now incorporate things showing up on any defined list type, yielding the boolean export expression: `(Resource Group && Verdict && Direction) || Denied || Allowed || Threat`:



  - For example, you could choose to send just the information about connections that were blocked across all of your resource groups in both directions, but also additionally send any logs that appeared on any combination of allowed, denied, and threat lists. That can be really interesting ways to reduce your third-party SIEM costs since it limits the amount of data ingested by a SIEM to just the things you care about. In the above example, we cared about blocks plus anything that might have been on a known list. That can be a great way to utilize a SIEM tool of your choosing to centrally triage what is being blocked and allowed across the things you care about.
- **Allowed and Denied Lists Naming Convention in the UI (DEV-1963)**
  - In the same way we've recently changed our naming conventions in our Global Management Center (GMC) UI with respect to renaming Blacklists and Whitelists to Denied Lists and Allowed Lists, respectively, we've done the same thing on our devices.
- **Allowed and Denied Lists Naming Convention in Syslog Export (DEV-1964)**
  - We've also updated to the new allowed and denied list naming convention in our syslog export data. Previous quantities `blacklists_…` and `whitelists_…` are now `deniedlists_…` and `allowedlists_…`, respectively.
- **URL Updates (DEV-1976, 1977, 1978)**
  - With the recent major updates to our cloud-based GMC SaaS, we updated several of the internal URLs in the device to map to the newest, most up-to-date URLs.

Defect Fix Description(s)

- **Internal Logs View Display Errors on Time-Based Searches (DEV-1969, 1972)**
  - A customer-reported defect resulting in an error when searching the internal logs directly on the device with certain date constructs has been fixed. While fixing this, we also extended the functionality a bit, with pagination now possible on either side of the resulting position in the logs.
- **Other minor internal fixes and improvements (DEV-1918, 1970, 1975, 1979)**

- A variety of minor internal fixes and improvements were also made.

Release: Build 38

File Date: 13 July 2020

Purpose of the Release

This is a fast-follow to our MVP (Minimum Viable Product) build 37 release which was our very first release supporting a single 10Gbps bridge pair on new 10G-capable products.

New and Improved

- **Line-Rate Small Packet and Burst Performance (DEV-1967)**
  - We had already blown away our MVP projection by being able to support 150,000 connections per second at 256 byte packets. But now, we're able to proudly claim that we can support line rates at 10Gbps even at the smallest 64 byte packet sizes, with minimum measurable impact to latency, thanks to our patented filtering architecture!
  - This improvement also really helps with some loss that could conceivably occur at very high transient burst rates, especially on lightly loaded 10G fiber circuits.

Defect Fix Description(s)

- **Other minor internal fixes (DEV-1968)**
  - A minimal impact memory reference error resulting in memory being read that wasn't needed was addressed.

Release: Build 37

File Date: 30 June 2020

Purpose of the Release

This is our MVP (Minimum Viable Product) release supporting a single 10Gbps bridge pair on new products that are now generally available. If you'd like to inquire about purchasing a 10G-capable product, please contact your sales representative. Like all of our software releases, this release is cumulative and also supports our non-10G equipment. This release also fixes a few recently discovered defects.

New and Improved

- **10Gbps Device Support (DEV-1483, DEV-1926, DEV-1947, DEV-1948, DEV-1952, DEV-1953, DEV-1954, DEV-1956)**
  - We are excited to release our first official 10Gbps threat intelligence firewall product. For information about ordering our 10G-capable device, please contact your sales

representative.
    - Our 10Gbps MVP release target was to be able to support 100,000 connections per second with average packet sizes of 256 bytes, to truly stress the system -- that is to say, we didn't skate by with simplistic "large packet" testing. Instead, we stressed the system with lots of small packets so as to better represent highly stressful real-world environments. We're happy to report that our MVP release not only met the 100,000 connections goal at 256 byte packets, but our tests demonstrate that our MVP release can handle 150,000 connections per second with 256 byte sized packets without adverse packet loss.
- **Syslog Export Defaults (DEV-1940)**
    - To avoid data deluge, by default our syslog export function will export information about packets that have been blocked. If your specific SIEM or other syslog target can handle information about all allowed and denied packets, you can still of course select everything for export in the syslog export configuration screen.
- **General Internal Performance Improvements (DEV-1946, DEV-1951, DEV-1960, others)**
    - This includes better CPU and memory management and isolation, compiler optimization updates, plus better queue management, especially useful for TCP-related activity at very high connection rates.
- **Removed Extraneous Script Restart Alert (DEV-1957)**
    - We removed some misleading, extraneous script restart alerts that were showing up erroneously in the logs.

Defect Fix Description(s)

- **REACT Stats Propagation to GMC (DEV-1945)**
    - A problem with the propagation of REACT meta-statistics has been addressed.
- **Policy Evaluation Defect (DEV-1962)**
    - A defect with policy evaluation resulting in improper direction assignment is now addressed.

Release: **Build 34**

File Date: 12 June 2020

Purpose of the Release

This release adds some minor feature improvements including the latest DPDK 18.11.8 LTS build, which is responsible for packet performance improvements and several security fixes. This release also fixes a few recently discovered defects.

New and Improved

- **DPDK 18.11.8 (DEV-1903)**
    - We now ship with DPDK 18.11.8, which includes the latest set of improvements and fixes for DPDK to include security fixes for recently announced security vulnerabilities

CVE-2020-10722, CVE-2020-10723, and CVE-2020-10724.

- **Proper Logout Endpoint Cleanup (DEV-1935)**
  - A proper auth/logout endpoint now exists. Previous logout attempts did indeed log the user out, but internal active session lists were not immediately being cleaned up. With this improvement, the active session lists are now able to be cleaned up immediately.
- **Removed Internal/Extraneous License Detail (DEV-1936)**
  - We removed some misleading, extraneous internal licensing information present in a specific UI screen after receiving several support calls where it had sparked confusion.

Defect Fix Description(s)

- **Memory Error (DEV-1930)**
  - A possible buffer overflow error in an internal library used by an internal registration tool was fixed.
- **Tombstone Policies (DEV-1934)**
  - A set of related problems existed which could cause policies that had been removed from GMC to not be fully removed from associated devices, resulting in a tombstone effect where policies were still being loaded and evaluated internally in the device even though they were not truly marked as being in-use. This has now been fixed.
- **UI Session Timeout (DEV-1943)**
  - The UI session timeout feature was not functioning properly. It now properly logs out after the session timer expires.
- **Other minor internal fixes (DEV-1941, DEV-1942)**

Release: **Build 32**

File Date: 22 May 2020

Purpose of the Release

This release provides exciting new features, the highlight being support for Domain Attribution. The release also addresses several important defects.

New and Improved

- **Domain Attribution (DEV-1893)**
  - Our packet logs have always supported full attribution, and now our domain logs do too!
- **95/5 Tracking (DEV-1656)**
  - We've added new industry-standard 95/5 bandwidth utilization tracking features, which enables us to provide more downstream billing configuration options to better meet diverse customer needs over time.
- **Alerts for Bypass Engagement (DEV-1752)**
  - Alerts are now generated if the bypass circuit is engaged, for any reason. This is an important alert since traffic is always passed-through on circuits placed in bypass mode,

bypassing the internal protection engines.

- **Hardware Support for some of our X-Series Legacy Devices (DEV-1924, DEV-1925)**
  - We're happy to report that we've been able to certify our software on some of our older X-series hardware.

Defect Fix Description(s)

- **Disk Full Condition Due to Database Activity (DEV-1921)**
  - We internally identified a set of conditions that could result in the root disk partition becoming full due to runaway database activity. This has been fixed.
- **Remove Extraneous Connection Error Message for DHCP Admin Access (DEV-1906)**
  - An incorrect GMC connection error message was being reported for an internal condition surrounding DHCP admin port connections. The scenario was not actually an error, and the internally generated error message has been removed.
- **Other minor internal fixes (DEV-1871, DEV-1928)**

Release: **Build 30**

File Date: 9 April 2020

Purpose of the Release

This release provides exciting new features relating to our syslog export capability. The release also addresses several important defects.

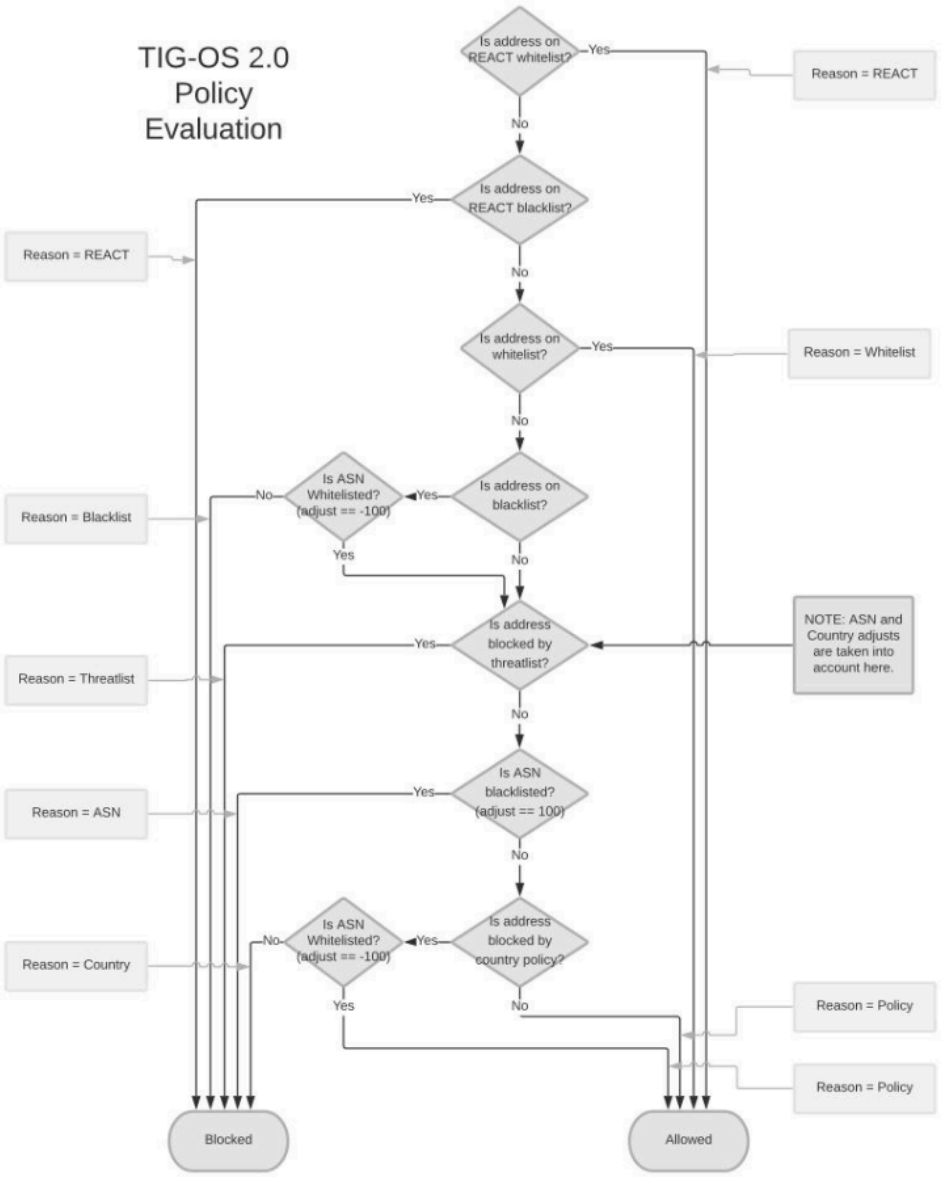
New and Improved

- **External Syslog Connection New Features and Improvements**
  - Although most tools don't specifically care about syslog export formats, our export headers are now fully compliant with RFC 5424. We've verified compatibility with syslog-ng, Gravwell, and Splunk.
  - When configuring the connection to an external syslog server, we now support individual selectors for packet logs, DNS logs, internal system message, and audit logs.
  - Packet logs can now be filtered by a configurable combination of Resource Group, Verdict and Direction, allowing end users to send only the data of interest to their external syslog servers, which can greatly reduce system cost when the target system (such as Splunk and others) charge users based on the amount of data that is ingested.
  - The syslog export data now supports all possible combinations of multiple list and multiple category outputs, with header name changes to include `whitelist -> whitelists`, `blacklist -> blacklists`, `threatlist -> threatlists`, and `category` is removed and has been separated into `matched_categories` and `denied_categories`.
  - Threat list categories are now output to the syslog export channel(s) as `matched_categories` and `denied_categories`. The `matched_categories` will be populated whenever a threat list category match is detected regardless of score, and

it will also appear in the `denied_categories` list if its relevant category score was above the risk threshold setting for the associated policy.
    - The TIG's hostname is now output to all syslog export types, appearing between the standard syslog timestamp field and the log type name. This can allow users (or SIEMs or other systems) to pull such information directly from the log stream as opposed to being forced to use metadata attached by third-party external syslog server or other software.

Defect Fix Description(s)

- **Policy Change Impact to Already-Established Connections (DEV-1882)**
    - Previously, if a suitable policy change was made, an already-established connection that should begin to be denied by virtue of the policy change was still being allowed. This is now fixed.
- **Buffer overrun (DEV-1884)**
    - A potential internal buffer overrun condition resulting from filter size errors has been corrected. This could have resulted in anomalous blocking behavior in rare situations where GMC-supplied filters were incorrectly oversized. This addresses the problem in a more consistent fashion than the rapid hotfix that was originally supplied in Build 25.
- **Whitelists not properly applied to packet analysis in some scenarios (DEV-1897)**
    - A possible problem with whitelist vs blacklist determination for some packets has been addressed. With this fix, REACT blacklists are a higher priority than standard whitelists, which is the desired behavior. We've updated the customer-facing documentation to match the corrected policy. Purely for reference, the current policy evaluation as of build 30 is as follows:



Release: Build 25

File Date: 5 March 2020

Purpose of the Release

This release serves as a hotfix to address a single, critical defect that was internally discovered after the release of Build 24.

Due to the critical nature of this defect, we strongly recommend that all current users running Build 24 immediately upgrade to Build 25 after first rebooting their device.

Defect Fix Description(s)

The identified defect caused the software to behave erratically and not follow its configured policy

settings when receiving certain oversized filters. The result was incorrect traffic allowed/denied patterns which can erroneously impact your network and your network's security.

Normally, a reboot is not required prior to a software update, but the specific defect in Build 24 could have resulted in internal memory corruption, and therefore it is safest to first reboot a system that is currently running Build 24 before updating the software to Build 25. To reboot your device, log into the TIG's local web administration GUI from your favorite browser, select System > Reboot on the left-hand navigation pane, and then click the OK button in the modal that appears. After a few minutes the system will finish rebooting and you can then safely follow the standard software update procedure.

Release: **Build 24**

File Date: 20 February 2020

Purpose of the Release

We are pleased to announce the release of version 2.0 of our software stack. This release includes significant improvements to our stack as listed below.

New and Improved

New features Include:

- **Significant Performance Improvements** - our software can now support over 150M unique IP and domain indicators. This upgrade in performance offers unprecedented protection from a broad range of today's IP and domain threats.
- **Threat Feed Source Attribution** - Our on-device logs now associate IPs and domains with specific threat intelligence feeds and lists. This enhanced context improves visibility into specific threats, the ability to investigate threats, and most importantly, provides a mechanism to measure ROI and efficacy (i.e. false positives) for specific threat intelligence sources.
- **Improved Blacklisting & Whitelisting** – Our REACT functionality now has the ability to provide both whitelists and blacklists. Blacklist policies are now configured based on specific resource groups which provide mode granular policy management and enforcement capabilities.
- **Enhanced Visibility and Policy Control –** Through the use of expanded resource groups for global policy information, as well as JSON-based configuration import functionality, users can identify changes and quickly configure multiple deployments across their network.
- **Usability Improvements –** A snappier and more responsive interface, improved IP lookups, and "context at a click" with intuitive icons throughout.
- **New threat feeds and whitelists –** New, out-of-box Feodo threat feed that tracks botnet C&Cs associated with Emotet (Heodo) and Dridex. A new IPv4 whitelist that helps mitigate false positives and provide richer contextual information about connection information. A new, curated, GitHub whitelist available for all users to easily configure and enable.