

AUTOFOCUS

Prioritize attacks with threat intelligence for quick attribution, context and correlation

Palo Alto Networks® AutoFocus™ contextual threat intelligence service makes threat analytics, with full context, available to every security organization, not just those with specialized security staff. This hosted security service arms security operations professionals with the high-fidelity intelligence, correlation, context and automated prevention workflows needed to identify and respond to events in real time.

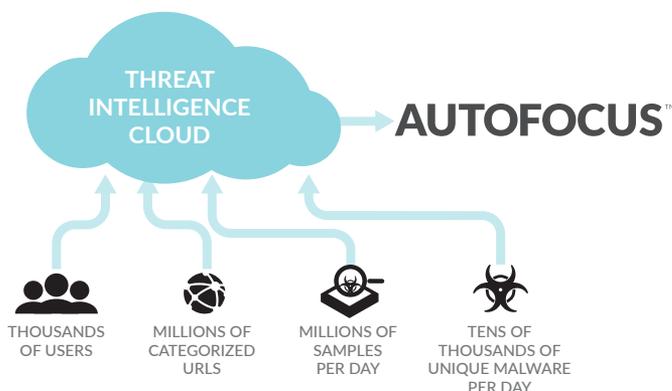
Weaponize Your Threat Intelligence

- High-fidelity threat intelligence on day zero through native integration with the WildFire data set.
- Unique researcher-curated context from Unit 42, the Palo Alto Networks threat research team, including information on malware family, adversaries, campaigns, malicious behaviors and exploits used.
- Aggregation and correlation of any third-party threat intelligence provider with the MineMeld application for AutoFocus, including the automated extraction and sharing of high-value indicators for prevention.
- Extension of the Palo Alto Networks Security Operating Platform, with AutoFocus threat context available natively in PAN-OS and Panorama, as well as an open API for integration into third-party systems.

Extending the Palo Alto Networks Platform

Security teams are inundated by alerts and threat data, lacking the time to follow up on each event, let alone investigate advanced, targeted attacks. The issue isn't a lack of information, but rather the inability to surface high-impact threats and drive automated prevention from the intelligence you already have. This new reality requires a prevention-first approach that automatically stops successful cyberattacks while providing the threat intelligence and tooling to speed identification, response and prevention workflows.

AutoFocus extends the Palo Alto Networks Security Operating Platform with local, industry and global threat intelligence with attack context to accelerate analysis, forensics and prevention workflows. Together, the platform and AutoFocus allow security teams to move away from legacy approaches that rely on aggregating detection-focused alerts and post-event mitigation. Now, the majority of attacks will be automatically prevented, with proactive threat analytics and hunting enabled through AutoFocus.



Priority Alerts

AutoFocus enables security teams to distinguish the most important threats from everyday commodity attacks, contextualizing events on your network or public data with tags. Unique to AutoFocus, tags label threat events with malware families, campaigns, threat actors, malicious behaviors and exploits used. When a tag matches an event on your network, AutoFocus sends a priority alert via email, within the AutoFocus dashboard, or via HTTP post, with the full tag context included. Alerts are highly customizable, enhancing your existing security workflows with prioritization and context for the most critical threats.

Tags

Tags enrich your visibility into the most critical threats with highly contextual intelligence. They can be created for any host- or network-based indicator in AutoFocus, alerting you when a specific threat has been observed in your organization or industry. In addition to priority alerts, all tags are searchable, allowing you to instantly pivot to associated malicious samples or indicators. As new threats are identified, your organization, the global community of AutoFocus experts and the Palo Alto Networks threat research team, Unit 42, add new tags to the service.

Unit 42 Threat Intelligence Team

AutoFocus is the primary analysis tool used by Unit 42 to identify new threats, correlate global data, identify connections between malicious samples, and build adversary or campaign profiles. You can view the latest research by Unit 42, identified with AutoFocus, [here](#). Within the service, Unit 42 adds human-curated intelligence to AutoFocus by creating tags based on their research, providing context and prioritization for identified threats, extending your security team with their knowledge.

Automatically Prevent Attacks

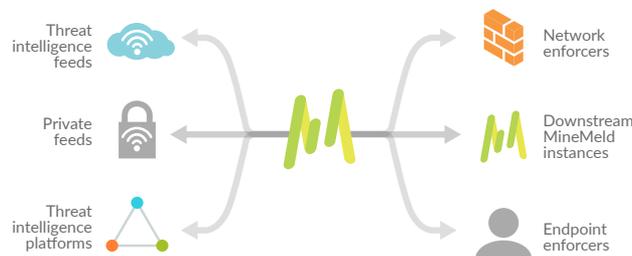
Security teams require more than just raw threat intelligence – they need it to automatically transform into actionable controls that prevent future attacks. AutoFocus simplifies workflows to create and enforce new controls, from fully automated to user-directed, within the same unified security platform:

- Fully automated extraction to prevention of high-value indicators of compromise, or IoCs. Security teams can leverage the hosted MineMeld application within AutoFocus to automatically gather IoCs from intelligence native to the service or third-party intelligence sources, driving enforcement on Palo Alto Networks devices without any human intervention required.
- User-directed hunting of high-value indicators, grouping them for export to Palo Alto Networks platform deployments – using PAN-OS® external block lists or Dynamic Address Groups – or third-party security devices in a standard CSV format.

Any indicator can be collected and exported from AutoFocus using MineMeld, direct export or via the API.

Search

During an active attack, the speed of investigation and the ability to meaningfully correlate data is critical. AutoFocus enables you to build sophisticated multilayer searches at the host- and network-based artifact level – and target your search within industry, time period, and other filters – allowing you to make previously unknown connections between attacks and pivot across your intelligence. AutoFocus puts the entire wealth of Palo Alto Networks threat intelligence and that of third-party sources at your fingertips, dramatically cutting the time it takes to conduct analysis, forensics or hunting efforts.



MineMeld Application

Many organizations rely on multiple sources of threat intelligence to ensure the widest possible visibility into emerging threats, but they struggle to aggregate, correlate, validate and share indicators across different feeds. As part of AutoFocus, the MineMeld™ threat intelligence syndication engine provides a single, unified threat feed and indicator management system. Security teams can leverage MineMeld to:

- Aggregate and correlate any third-party intelligence source within AutoFocus.
- Automatically identify and extract high-value indicators from all sources, leveraging the high fidelity of native AutoFocus intelligence to validate IoCs.
- Feed real-time, prevention-based controls to Palo Alto Networks security platform deployments for enforcement.
- Create custom threat intelligence feeds to simplify sharing for third-party service services or trusted partners.

Learn more about MineMeld, including the open source version, on the [official site](#).

Statistical Analysis Engine

When conducting threat analysis, security teams must quickly identify which indicators represent the best path for additional research. Each file has hundreds, potentially thousands, of artifacts, with only a small number of unique IoCs able to tie back to the larger profile of an adversary or related attacks. AutoFocus uses an innovative statistical analysis engine, correlating billions of artifacts across a global data set, bringing forward high-value indicators associated with active attacks. The service automatically applies a unique visual weighting system to identify unique and critical IoCs, guiding analysis, response and prevention efforts down the most relevant path.

Extending the Platform With Threat Intelligence

AutoFocus helps the entire IT security team become advanced threat hunters, instead of relying on a small group of highly specialized security operations professionals. Threat intelligence from the service is made directly accessible in the Palo Alto Networks platform, including PAN-OS and Panorama™ network security management. AutoFocus speeds the security team's existing workflows, allowing for in-depth investigation into suspicious activity. When further analysis is required, users can sweep between AutoFocus and PAN-OS or Panorama, with pre-populated searches for both systems.

With AutoFocus and the platform, users can ascertain:

- How targeted or unique a threat seen on the network is.
- Related malicious samples for further investigation.
- Domain resolution history to identify suspicious DNS queries.

Realize the Power of the Application Framework

AutoFocus is part of the Palo Alto Networks Application Framework, letting you quickly consume the latest cybersecurity innovations as apps. The Application Framework makes it easy to adopt cloud-delivered capabilities like AutoFocus – so you can gain immediate security value and spend less time provisioning and managing infrastructure.

AutoFocus Architecture and Intelligence Sources

AutoFocus is built on a large-scale, distributed computing environment hosted by Palo Alto Networks. Unlike other offerings, the service makes threat data accessible and actionable at the IoC level, going beyond showing summarized logs from multiple sources in a dashboard. AutoFocus has unprecedented visibility into the threat landscape, with the collective insight of thousands of global enterprises, service providers and governments feeding the service. It correlates and gains intelligence from:

- WildFire® cloud-based threat analysis service – the industry's largest malware analysis environment
- URL Filtering with PAN-DB
- MineMeld application
- Traps™ advanced endpoint protection
- Aperture™ SaaS security service
- Unit 42 threat intelligence and research team
- Technology partners like Proofpoint™
- Palo Alto Networks global passive DNS network

AutoFocus makes billions of samples and sessions, including billions of artifacts, immediately actionable for security analysis and response efforts.

Simple Third-Party Integrations

Threat analysis, forensics and incident response teams often rely on a broad range of scripts, open source tools, security devices and services to investigate potential incidents. AutoFocus can dramatically cut the time required for investigation by enriching third-party services through:

- **MineMeld:** Custom threat intelligence feeds, created by MineMeld with intelligence sourced from AutoFocus and any third-party provider, can be easily consumed by other security systems.
- **AutoFocus API:** Built on an easy-to-use RESTful framework, the AutoFocus API allows simple integration into hundreds of use cases, such as feeding intelligence into existing security information and event management, or SIEM, tools, making data available for additional threat analysis or custom threat-blocking automations.
- **Remote sweeping capability:** Users of AutoFocus can sweep from indicators in the service to both Palo Alto Networks and third-party external systems directly from AutoFocus. Teams can define up to 10 external systems, letting them continue their analysis seamlessly across their entire infrastructure, such as correlating logs from next-generation firewalls or triggering searches in SIEM tools.
- **STIX™ data format:** AutoFocus provides out-of-the-box integration with STIX infrastructure, with data available for export in the STIX data format.

Maintaining Privacy

AutoFocus has strict privacy and security controls in place to prevent access to sensitive or identifiable information. The service only allows authorized users to view data associated with their organization, with an “opt-in” mechanism to share anonymous data with other users. AutoFocus does not allow access to any customer-sourced files within the service, only providing the analysis results for samples observed in each respective customer’s network, without disclosing the original file content. AutoFocus strictly segregates any third-party intelligence source brought into the service through the hosted MineMeld application, which only allows visibility and access to the submitting organization. You can find further information in the [AutoFocus privacy datasheet](#).

AutoFocus Requirements

AutoFocus is offered as a hosted security service that does not require any configuration changes to your Palo Alto Networks Next-Generation Firewall and does not impact the device’s performance. In order to use the service, you must have a valid Palo Alto Networks support account, even if you have purchased a next-generation firewall or Traps. As AutoFocus is not hardware-dependent and does not require any changes to the device, there is no specific PAN-OS software version or additional hardware needed. We recommend subscribing to WildFire (PAN-OS 4.1 or higher) to take full advantage of AutoFocus.

Licensing Information

AutoFocus is offered as a per-seat annual subscription. Please contact your partner or reseller of Palo Alto Networks for additional licensing information.



3000 Tannery Way
Santa Clara, CA 95054
Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087
www.paloaltonetworks.com

© 2018 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at <https://www.paloaltonetworks.com/company/trademarks.html>. All other marks mentioned herein may be trademarks of their respective companies. autofocus-ds-042318