Omicron Seit 1995

paloalto NETWORKS®

AUTOFOCUS

Outcome-driven threat intelligence, analytics and prevention

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.

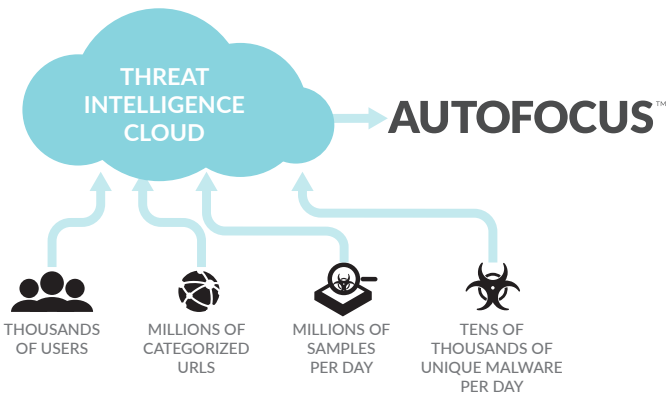
Weaponize your threat intelligence

- High-fidelity threat intelligence on day zero through native integration with the WildFire dataset.
- Unique researcher-curated context from Unit 42, 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 Next-Generation Security 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 ability 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 cyber-attacks, while providing the threat intelligence and tooling to speed identification, response and prevention workflows.

AutoFocus extends the Palo Alto Networks Next-Generation Security 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 pubic data with tags. Unique to AutoFocus, tags decorate threat events with malware families, campaigns, threat actors, malicious behaviors, and exploits used. When a tag matches an event on your network, a priority alert is sent 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, Unit 42, the Palo Alto Networks threat research team, your own organization, and the global community of AutoFocus experts 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

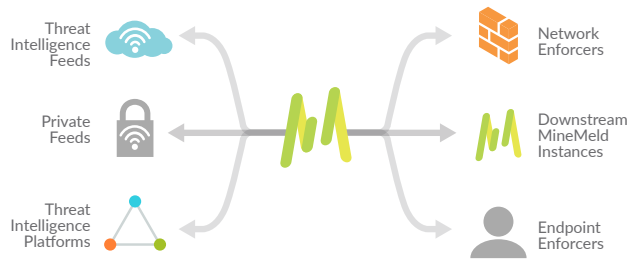
Security teams require more than just raw threat intelligence – they need to automatically transform it into actionable controls that prevent future attacks. AutoFocus simplifies workflows to create and enforce new controls, from fully automated to user directed, within the same unified security platform:

- Full automation of extraction to prevention of high-value indicators of compromise (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 platforms (using PAN-OS® security operating system 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 allows you to build sophisticated multi-layer 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, as well as third-party sources, at your fingertips, dramatically cutting the time it takes to conduct analysis, forensics or hunting efforts.



The MineMeld application

Many organizations rely on multiple source of threat intelligence to ensure the widest possible visibility into emerging threats, but struggle to aggregate, correlate, validate and share indicators across different feeds. As part of AutoFocus, the MineMeld application 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 platforms 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 indictors 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 answer questions such as:

- 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.

AutoFocus architecture and intelligence sources

AutoFocus is built on a large-scale, distributed computing environment hosted in the Palo Alto Networks Threat Intelligence Cloud. Unlike other solutions, 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. The service correlates and gains intelligence from:

- WildFire™ cloud-based threat analysis service, the industry's largest malware analysis environment
- PAN-DB URL Filtering service
- The MineMeld application, enabling aggregation and correlation of any third-party threat intelligence source directly in AutoFocus.
- 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 or 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 the MineMeld application, AutoFocus API, remote sweeping capability, and support for the STIX data format.

- The MineMeld application enable the creation of custom threat intelligence feeds, sourced from AutoFocus intelligence and any third-party provider, which can be easily be consumed by other security systems.
- The AutoFocus API built on an easy to use, RESTful framework, allowing simple integration into hundreds of use cases, such as feeding intelligence into existing security information and event management (SIEM) tools, making data available for additional threat analysis, or custom threat blocking automations.
- 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.
- 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 optional "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, customers must have a valid Palo Alto Networks support account, including those who 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), in order to take full advantage of AutoFocus.

paloalto NETWORKS®

4401 Great America Parkway
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com