AUTOFOCUS

Palo Alto Networks, provider of the industry-leading next-generation firewall, has made the world's highest-fidelity repository of threat intelligence, sourced from the largest network of sensors,[1] available for any team or tool to consume.

AutoFocus™ contextual threat intelligence service is your one-stop shop for threat intelligence. Your teams will receive instant understanding of every event with unrivaled context from Unit 42 threat researchers, and you can embed rich threat intelligence in analyst's existing tools to significantly speed investigation, prevention, and response.

Benefits

- Get unique visibility into attacks crowdsourced from the industry's largest footprint of network, endpoint, and cloud intel sources.
- Enrich every threat with the deepest context from world-renowned Unit 42 threat researchers.
- Give analysts a major time advantage with intel embedded in any tool through a custom threat feed and agile APIs

Current Challenges with Threat Intelligence

Security teams require deep context to quickly prioritize and respond to sophisticated attacks. Threat intelligence gives analysts an edge, but today's approaches provide limited value to security operations because the methods are so complex. Teams must manually collect and incorporate multiple low-value feeds into the tools they use for investigation and response. They also must choose between feeds with limited visibility on a narrow vertical or general-purpose commodity indicators with limited context. It's time for a different approach.

The AutoFocus Difference

AutoFocus gives you instant access to Palo Alto Networks massive repository of high-fidelity threat intelligence so you can consume it as a feed. Crowdsourced from the industry's largest footprint of network, endpoint, and cloud intelligence sources, you get unique insight into real-world attacks. Every threat is enriched with the deepest context from world-renowned Unit 42 threat researchers. Your analysts save significant time with intel embedded in any tool through a custom threat feed and agile APIs.

Access our continuously growing threat intelligence repository to get unique visibility into real-world attacks sourced from more than 65,000 enterprise customers over more than a decade.

[1] "Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 2Q19," Gartner, September 20, 2019, https://www.gartner.com/document/3968037.

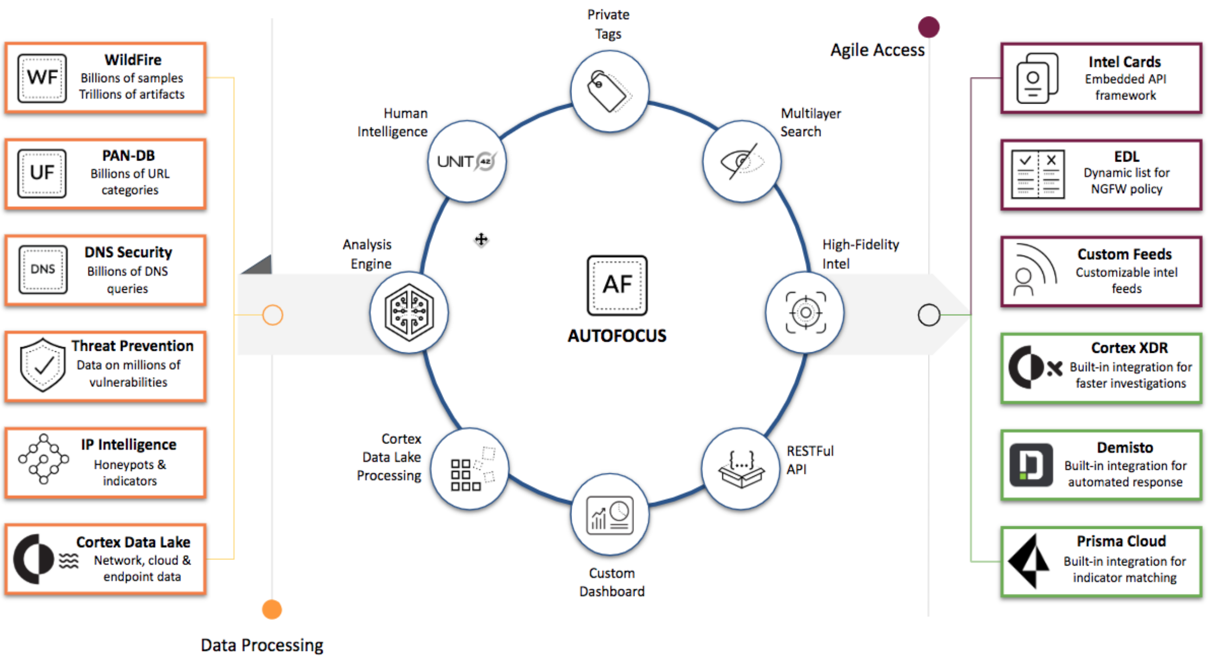


Figure 1: AutoFocus architecture

Access our continuously growing threat intelligence repository to get unique visibility into real-world attacks sourced from more than 65,000 enterprise customers over more than a decade.

Table 1: Threat Intelligence in AutoFocus

Intel Source	Intelligence
WildFire® malware prevention service	More than 14 billion samples collected More than 7 trillion artifacts analyzed
PAN-DB	2 billion URL queries processed daily
DNS Security service	46 million real-world DNS queries processed daily
Traps™ endpoint protection and response	Telemetry and samples from millions of Traps endpoint agents
Prisma™ Access	Millions of samples collected continuously from hundreds of SaaS applications
Unit 42 research	More than 2,700 hand-curated tags and more than two dozen tag groups covering thousands of variants of attack campaigns
Third-party sources	In-house data augmented by millions of samples shared across Cyber Threat Alliance contributors, including vendors like Cisco, Fortinet, and Check Point

Hand-Curated Intelligence for Every Threat

Enrich every threat with the deepest context from the world-renowned Palo Alto Networks threat research team, Unit 42. As an agile, global team, Unit 42 meticulously analyzes real-world threat data to uncover and provide in-depth research on adversaries, malware families, and attack campaigns. Unit 42 adds human-curated intelligence to AutoFocus by creating tags, providing researcher-curated context, and prioritizing identified threats, boosting your security team with their knowledge.

Table 2: Unit 42 Global Threat Intelligence

AutoFocus tags	Gain rich context and a better understanding of advanced threats with more than 3,000 expert-curated Unit 42 tags. Tags include details about adversaries, campaigns, malicious behaviors, malware families, exploits, and techniques, enabling teams to quickly distinguish and prioritize the most important threats from commodity attacks.
AutoFocus custom tags	Collaborate with team members by creating custom tags based on your own search criteria.
AutoFocus tag groups	Search based on tag groups to surface categories of threats for broader visibility and action. Pre-built tag groups include: ransomware, banking trojan, hacking tool, and more.
Unit 42 publications	Stay up to date with Unit 42's latest research, published more than 100 times per year. Research is conducted in pair analysis, leveraging the combined expertise of a threat hunter and a reverse engineer. Unit 42 Threat Research

Table 2: Unit 42 Global Threat Intelligence (continued)	
Unit 42 Adversary Playbooks	Get in-depth visibility into adversary tactics, tools, and procedures in a structured data format available to anyone who wants to expand their knowledge. Unit 42 Adversary Playbooks
"Don't Panic" podcast	"Don't Panic" is the official Unit 42 podcast, where expert researchers address issues at the top of cybersecurity practitioners' minds—and help resolve them so they can get their sanity back. Unit 42 "Don't Panic" Podcast

Instant Access to Intel When You Need It Most

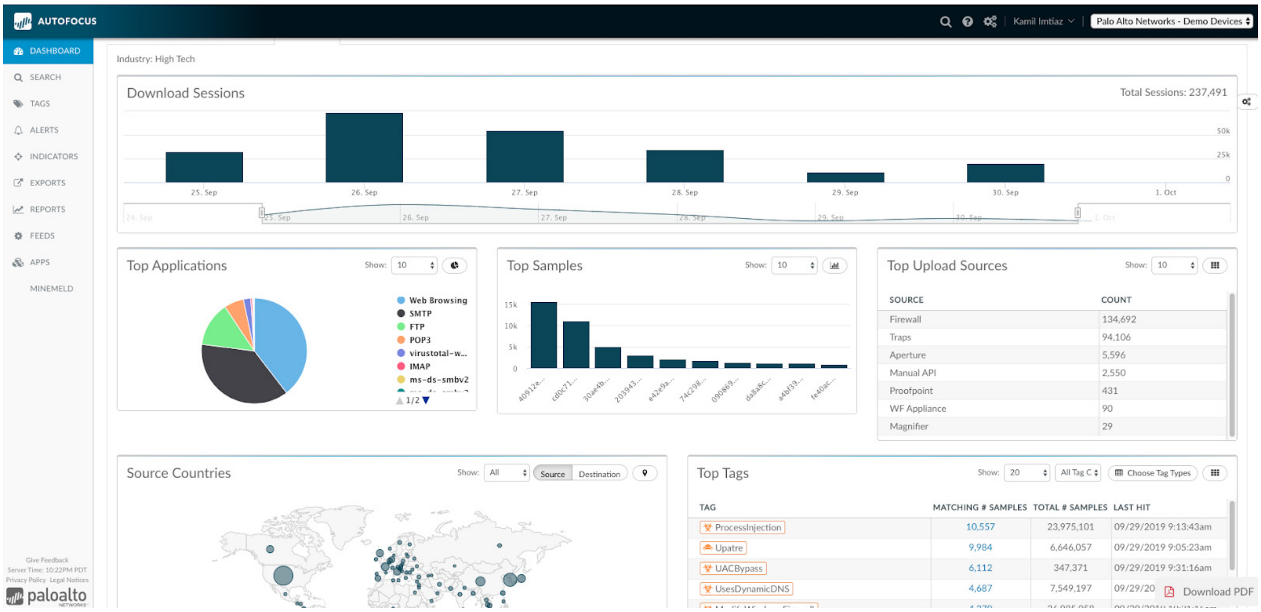
Give analysts a significant time advantage with intel embedded in any tool through a custom threat feed and agile APIs:

- Power up any detection, investigation, and prevention tool with a custom feed builder to extract and share the most relevant, continuously updated threat intelligence. You can also leverage a built-in, curated feed updated every 24 hours.
- Take advantage of embedded intel cards for Palo Alto Networks and third-party tools to automatically surface indicator groupings directly in existing products.
- Provide threat intelligence to security information and event management (SIEM) tools, in-house systems, and hundreds of other third-party tools with an open and agile RESTful API.

Table 3: API Framework	
Feature	**Benefits**
Intelligence cards	Get instant access to relevant intel around IPs, hashes, URLs, or domains from a single API query, eliminating the need for your security personnel to manually search and correlate relevant indicators.
RESTful API	Enjoy quick access to samples, file analysis, aggregate data, tags, and much more via the agile API framework. This framework allows security teams to enrich their existing tools in real time to enable fast analysis and automate responses. AutoFocus API References
Threat Feed Builder	
Custom feed builder	Build your custom threat intelligence feeds by choosing from many high-value indicator types, including file hashes, URLs, domains, confidence, and more. Automatically export and publish feeds to enable quick enforcement through prevention controls.
Daily feeds	Stay ahead of attackers with a curated feed published daily, ready for consumption by any security tool.
Other Tools and Standards	
MineMeld™ application	Aggregate and correlate any third-party intelligence source within AutoFocus, and automatically identify as well as extract high-value indicators from all sources, leveraging native intelligence to combine power. You can combine the two with more than 200 plugins for threat feeds. Learn more about MineMeld
Standard data formats	Standardize threat intelligence with various compatible formats, such as STIX, JSON, TXT, and CSV, making it easy to integrate with any security tool set.
Maltego Transforms for AutoFocus	Visualize relationships between indicators through AutoFocus transforms. Query disparate data sources and present a view of the retrieved data in a single view. Download Maltego Transforms for AutoFocus

Visibility into the Current Threat Landscape

Gain deep visibility into your organization's threat landscape through the AutoFocus dashboard. Create custom dashboards and widgets, and compare your security posture with the rest of the industry. Have daily, weekly, monthly, or yearly reports generated and emailed directly to your inbox.



Industry: High Tech

Total Sessions: 237,491

Show: 10

Show: All

Top Upload Sources

Show: 10

SOURCE	COUNT
Firewall	134,692
Traps	94,106
Aperture	5,596
Manual API	2,550
Proofpoint	431
WF Appliance	90
Magnifier	29

Top Tags

Show: 20 All Tag C Choose Tag Types

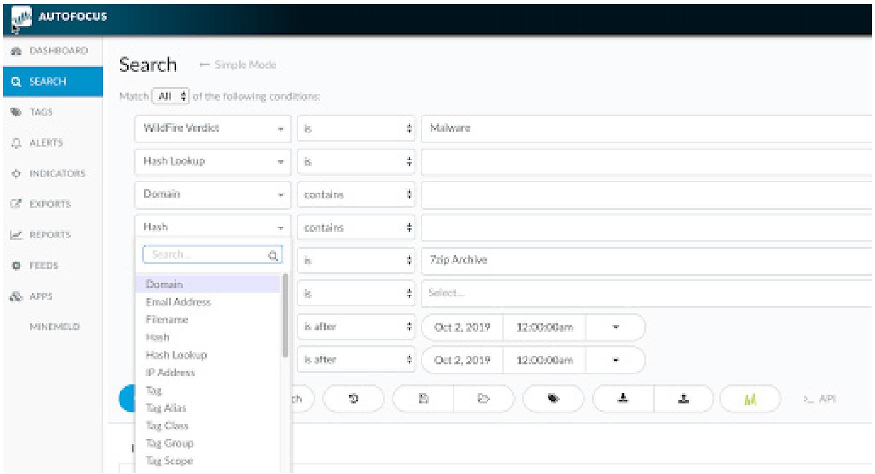
TAG	MATCHING # SAMPLES	TOTAL # SAMPLES	LAST HIT
ProcessInjection	10,557	23,975,101	09/29/2019 9:13:43am
Upatre	9,984	6,646,057	09/29/2019 9:05:23am
UACBypass	6,112	347,371	09/29/2019 9:31:16am
UsesDynamicDNS	4,687	7,549,197	09/29/20

Figure 2: AutoFocus custom dashboard

Table 4: AutoFocus Dashboard	
Feature	**Benefits**
Custom dashboard	Create custom dashboards, widgets, reports, and alerts with an easy-to-use interface.
Scheduled reports	Stay up to date with current industry trends by running daily, weekly, or monthly reports.
Priority alerts	Enhance your existing security workflows by sending priority alerts via email or HTTP post when an indicator matches a defined tag.
Unit 42 research feed	View Unit 42 latest research directly in the AutoFocus dashboard, giving you additional visibility into recent malware campaigns with details about their techniques, tactics, and procedures (TTPs) without leaving the UI.
Indicator-based repository	Access a repository of millions of stored indicators available for search and analysis. All indicators from WildFire, DNS Security, PAN-DB, and third-party intelligence feeds are extracted in near-real time and delivered to the store.

Granular Search with Unlimited Combinations

Rapidly pivot through billions of samples and trillions of artifacts by combining more than 130 search dimensions in unlimited ways, making it easy for teams to quickly get to the information they need without the knowledge or expertise of an advanced threat hunter.



Match All of the following conditions:

WildFire Verdict is Malware

Hash Lookup is

Domain contains

Hash contains

is 7zip Archive

is Select...

is after Oct 2, 2019 12:00:00am

is after Oct 2, 2019 12:00:00am

Figure 3: 130+ search dimensions in an easy-to-use interface

Table 5: Granular Search	
Feature	**Benefits**
Multilayer search	Build sophisticated multilayer searches at host- and network-based artifact levels. Create your custom search using more than 130 dimensions, giving you countless ways to search and pivot. Share saved searches with team members to dramatically reduce the time it takes to investigate and hunt for advanced threats.
Quick search	One-click search for common attributes like IPv4, IPv6, domain, hash, and URL indicators across networks, endpoints, and clouds.
Remote search	Sweep for indicators in both Palo Alto Networks and third-party external systems directly from AutoFocus. You can define up to 10 external systems, letting you seamlessly access your entire infrastructure for analysis, such as correlating logs from next-generation firewalls or triggering searches in SIEM tools.

AutoFocus Data Privacy

AutoFocus has strict privacy and security controls in place to prevent unauthorized 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 anonymized data with other users. AutoFocus does not allow access to any customer-sourced files within the service, only providing analysis results for samples observed in each respective customer's network, without disclosing the original file content. You can find further information in the AutoFocus Privacy Datasheet.

AutoFocus Requirements

AutoFocus is offered as a SaaS-based security service that does not require any configuration changes to your Palo Alto Networks next-generation firewalls and does not negatively affect the devices' performance. As AutoFocus is not hardware-dependent and does not require any device changes, no specific PAN-OS® software version or additional hardware is needed. However:

- To use the service, you must have a valid Palo Alto Networks Support account.
- We recommend subscribing to WildFire and PAN-DB (both of which require PAN-OS 4.1 or higher) as well as DNS Security (which requires PAN-OS 9.0 or higher) to take full advantage of AutoFocus.

AutoFocus Licensing

AutoFocus is offered as a per-seat, annual subscription. Please contact your partner or Palo Alto Networks reseller 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