PREVENTION ARCHITECTURE METHODOLOGY

Applying Prevention Capabilities to Defeat Cyberattackers

Prevention-oriented architecture is transforming the way we operate, maintain and defend cyber environments. This document explains the methodology and capabilities Palo Alto Networks delivers to prevent successful attacks and protect our digital way of life.

Table of Contents

Setting Expectations for Prevention Readiness

We Learn More Every Day

We continue to learn more about measuring prevention readiness and making threat prevention an organic part of IT architecture. As an element of this, we are building confidence that our mission at Palo Alto Networks® – to protect our digital way of life – is achievable.

When we speak with IT and security leaders, we consistently observe a couple of things:

1. They lack confidence that they know what is happening in their enterprises.
2. They look to the cybersecurity community – which includes us – to help them create modern architecture strategies based on prevention. The legacy best-of-breed approach and auditing relationship between IT and security professionals fails to protect organizations from successful attacks.

Given the challenges in information security today, both observations make sense. Collectively, we have a significant amount of intelligence about the attackers we face, including:

- Their techniques
- Their attack vectors
- Their tools
- Indicators of compromise

However, we don't use our aggregated intelligence about attackers to defeat the them. In fact, much of the time, organizations don't know what's actually happening inside their own environments.

That's why Palo Alto Networks created a standard Prevention Architecture Methodology to help set expectations with new customers and update them with existing customers. As part of the methodology, we created metrics to measure our customers' progress. More and more of our customers are seeing the value in this approach, and it is making a difference.

The methodology is critical to your organization's security strategy and will help you achieve:

- Cohesion between your IT and security teams
- Improved operational efficiency
- Better prevention automation
- Reduced business risk

It isn't simply a shortcut to better security, however. It is a holistic plan to build a prevention-oriented architecture for your organization's long-term success.

The methodology provides complimentary, standardized deliverables to ensure customers make full use of all integrated capabilities of our platform across the architecture. Our account teams provide these deliverables on a regular basis so customers can use them as part of their standard cadence. We are scaling this entire methodology as part of our commitment to prevent successful attacks and protect our digital way of life.

Our Purpose-Built System of Systems

The inability to take global action on attacker intelligence hinders IT and security industry professionals working to protect their organizations. A primary cause of this inability is legacy technologies that lack native integration to prevent attackers across all known threat vectors. Furthermore, it remains commonplace in the industry to focus on detection and response instead of prevention. Palo Alto Networks sought to overcome this dilemma by creating an integrated, purpose-built, prevention-oriented platform that makes preventive decisions to actively defend customers around the globe.

When WildFire identifies a malicious file, the platform performs an automated, global reconfiguration in as few as five minutes to prevent the file from gaining access to our customers. When we work together to configure and confirm our prevention readiness, a customer in Europe will be protected from a malicious file in minutes, even if the file is identified in Asia. Prevention is not limited to traditional organizational perimeters, instead operating on a global scale – our entire customer base – for internal networks, data centers, external mobile systems and the cloud.

This approach is a fundamental shift in how we operate, maintain and defend cyber environments, which benefit professionals on IT infrastructure, application and security teams. Figure 1 highlights how the native system-of-systems integration automates prevention and control throughout an enterprise.

Palo Alto Networks engineers designed the components of the Next-Generation Security Platform to extend and automate capabilities that protect globally distributed organizations by acting immediately on attacker intelligence. The intent of this platform is to provide complete visibility for all applications, users and content. Once visibility is achieved, we can take steps to reduce the attack surface. From there, we prevent known threats and use automation, analysis and machine learning to prevent unknown threats. The following are descriptions of some core platform components.

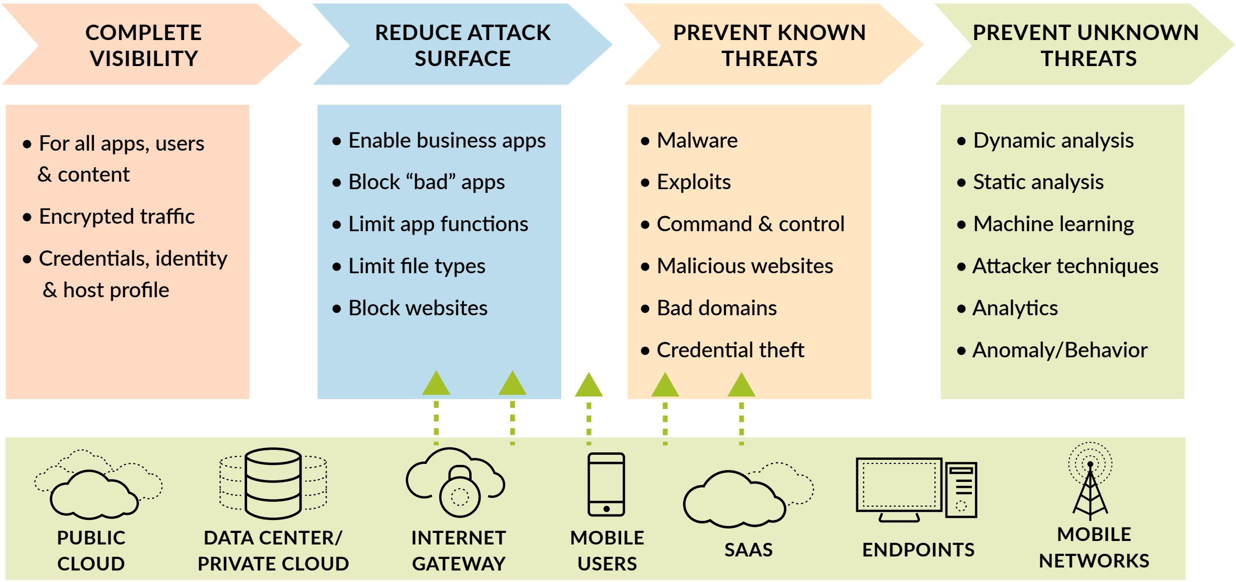


Figure 1: Purpose-built platform – system of systems

Next-Generation Firewall

Palo Alto Networks Next-Generation Firewall is responsible for enforcing policy on all network traffic everywhere the enterprise exists, including traffic to and from mobile devices or laptops. Our control and protection hold consistently because of the extensible nature of the design. In fact, the only difference between any two models of our firewalls is the data throughput. We built the network component of the platform on a common operating system to control and protect enterprises natively – no handing off traffic to "best-of-breed" blades of hardware. In addition, all components are available in a virtualized form factor, enabling the platform to scale anywhere, including in cloud or SaaS environments. The next-generation firewall provides unprecedented visibility across all network traffic to control and protect all applications, users and content everywhere.

Advanced Endpoint Protection

Advanced endpoint protection provides a novel way to protect endpoints, introducing exploit prevention to take back ground from attackers. Even if an endpoint is unpatched, exploit prevention holds for all known exploit techniques used to stage, prepare and inject malicious code into processes. Attackers can no longer access enterprises by using known, proliferated, advanced tactics that point products cannot prevent, nor can they exploit known or unknown vulnerabilities. This is a crucial part of defeating attackers before they can execute malicious code on a system.

SaaS Protection

The use of software-as-a-service applications is creating gaps in security visibility that raise the risk of malware propagation, data leakage and regulatory noncompliance. Data within an enterprise-enabled SaaS application is not visible to an organization's network perimeter. The platform provides SaaS security services that deliver complete visibility and granular enforcement across all user, folder and file activity within sanctioned SaaS applications. It can connect directly to sanctioned SaaS applications to provide data classification, sharing/permission visibility and threat detection within the application. Additionally, it provides detailed analysis and analytics on usage without requiring any additional hardware, software or network changes.

WildFire

WildFire® cloud-based threat analysis service provides oversight for our entire global install base. All deployed platform components automatically push unknown files from any location on all customer networks. WildFire receives and detonates these files to identify malicious content and gather threat indicators. At the same time, it automatically converts the intelligence indicators to signatures and deploys them to all platform components in network traffic and on endpoints. This process is fast and getting faster – today, it can gather new intelligence and deploy associated signatures around the globe in as few as five minutes after the moment of discovery.

Together, these platform components change the game for the protection of global enterprises. Just imagine the tight automation gained from our endpoint agent defeating an unknown piece of malicious malware on a user's endpoint. As our endpoint agent blocks a given instance of malware from executing, the file is extracted from network traffic, detonated and disseminated in the form of threat intelligence in as few as five minutes. This happens no matter what port or application the attacker uses as a threat vector. IT operations and defense professionals gain essential time, automation and efficiency while your company shrinks its attack surface, reduces risk and improves protection of your growing interests – all without interrupting business continuity.

Prevention Architecture Transformation Evaluation Toolset

Palo Alto Networks provides multiple tools to evaluate your organization's transformation to a prevention-oriented architecture. These tools help our trusted prevention architecture advisors regularly provide you with updated insights into your current transformation status. We are committed to helping your IT and security professionals accurately measure your progress toward a modern, prevention-oriented strategy.

These tools include:

1. Prevention Posture Assessment
2. Best Practice Assessment for NGFW and Panorama
3. Metrics to build IT and security leadership confidence

As a platform provider, we know it is insufficient to focus our account teams and partners on individual IT and security projects. Instead, we want to help make prevention a core component of your global enterprise architecture. What follows will explain the Prevention Posture Assessment in more detail, including how we use it to help integrate prevention into your IT infrastructure.

> *"Know the enemy and know yourself; in a hundred battles, you will never be defeated. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are sure to be defeated in every battle."*
>
> – Sun Tzu, *The Art of War*

Prevention Posture Assessment

Know the Enemy and Know Yourself

We created the Prevention Posture Assessment, or PPA, to help with setting expectations about prevention as well as creating a prevention-oriented architecture strategy to build alliances between IT and security professionals.

Two underpinning observations led us to create the PPA:

1. The cybersecurity community continues to amass intelligence about attackers. For example, we know which tools, techniques, indicators of compromise and vectors attackers use to successfully attack organizations. However, despite this knowledge, the community lacks the ability to effectively counteract these things.
2. Most IT and security leaders aren't confident that they know what is happening in their enterprises.

The general's words are as relevant today as ever, especially in the cybersecurity domain. To prevent successful attacks, you must know the adversary's tools and your own defenses.

Deliberately Aligning Architecture With the Attack Lifecycle

Figure 2 shows how we use the Prevention Posture Assessment to set expectations about prevention and help our customers develop a prevention-oriented architecture strategy.

First, we separate the architecture into three areas, as shown in Figure 2:

- Enterprise, mobility and SaaS
- Data center, cloud and SaaS
- Endpoint

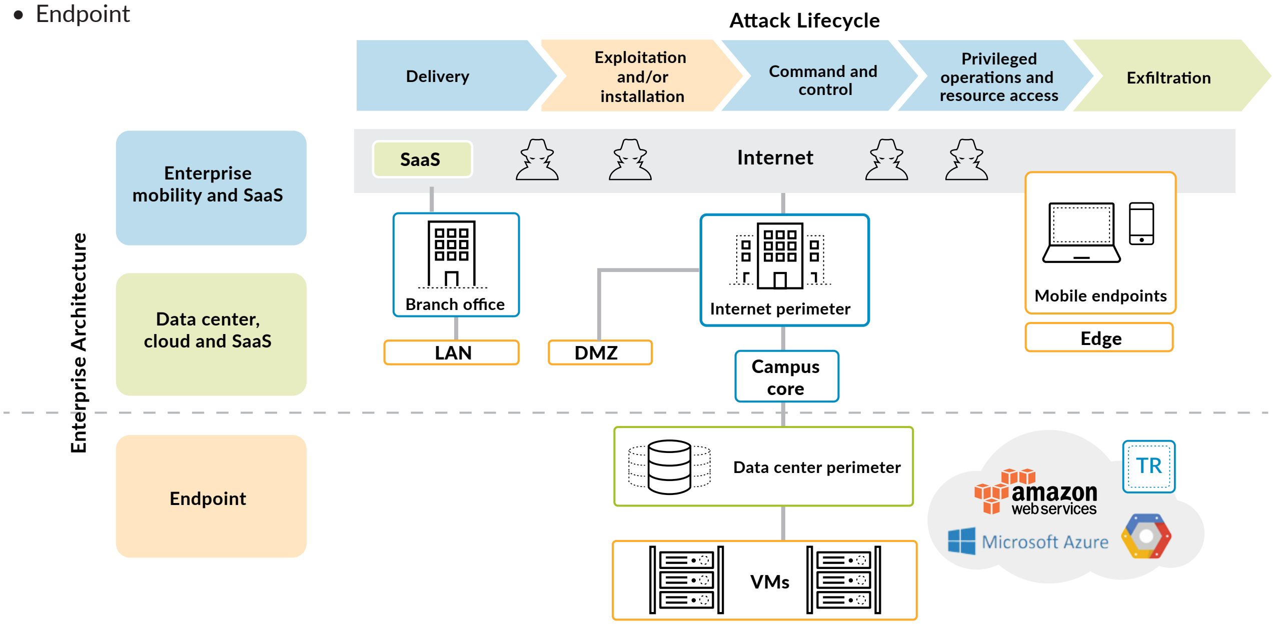


Figure 2: PPA approach

This ensures the “know yourself” aspect of our methodology is consistently accounted for across the architecture. The separation of the architecture ensures prevention capabilities are distributed across the entire architecture. In addition, it helps make the point that we need to work directly with an organization’s IT and security architects.

Second, we align the three architecture areas with specific stages of the attack lifecycle. See the relationship between these color coded in Figure 2.

This alignment aids a discussion about the difference a modern, extensible approach to prevention can make in protecting organizations. Positioning prevention capabilities across all three areas of the architecture provides the most well-rounded defense while maintaining confidence that the enterprise is operating as intended and remaining aware of everything happening in controlled environments.

Deliberately Extending Prevention Capabilities Across Global Architecture

AREA OF ARCHITECTURE	ATTACK LIFECYCLE STAGE	ACTIVE PREVENTION AND CONTROL CAPABILITIES
Enterprise, mobility and SaaS	Delivery (perimeter breach)	IPS (all port, in-line, both sides of traffic)
		URL filtering (all ports)
		Segmentation (zones)
		Anti-malware (all ports and in-line)
		Sandboxing (all ports and in-line)
		Decryption
		User and application control (Layer 7)
		SaaS malware delivery protection
		Email store and forward
	Command and control (outbound)	IPS (all ports and in-line)
		URL filtering (all ports)
		Unknown app blocking
	Privileged operations and resource access	Active hunting
		IPS (all ports and in-line)
		Anti-malware (all ports and in-line)
		Sandboxing (all ports and in-line)
		Credential theft protection
		Segmentation
		User and application control (Layer 7)
Data center, cloud and SaaS	Exfiltration	North-south IPS (all ports and in-line)
		User and application control (Layer 7)
		Microsegmentation
		East-west IPS (all ports and in-line)
		Anti-malware (all ports and in-line)
		Sandboxing (all ports and in-line)
		Automated demand provisioning
		Public cloud protection, visibility and control
		SaaS enforcement and reporting
		Behavior analytics detection
Endpoint (workstations/servers)	Exploitation and/or install	Exploit prevention (physical workstations and servers)
		Remote forensic capture
		Outdated Windows® server and workstation protections
		Sandboxing
		Sandbox indicator scaling
		Endpoint application control
		Endpoint control and restrictions

Figure 3: **Prevention architecture capabilities**

Figure 3 lists the prevention capabilities covered in the Prevention Posture Assessment. As you read through the list, note the following:

1. The capabilities are redundant across areas of the architecture and stages of the attack lifecycle. This is an important part of delivering comprehensive prevention capabilities throughout the architecture, rather than being limited by the hardened perimeters of a status quo approach.
2. We don’t assess detect-and-respond capabilities, such as IDS, because they are not prevention-focused and we do not believe they are part of prevention readiness.
3. All prevention capabilities are parts of the fully integrated, system-of-systems platform approach. We encourage customers to include all capabilities to get the full value of their investments.
4. These capabilities are relevant to IT and security infrastructure professionals alike, so we always perform the assessment jointly with the IT and security architects, helping to build cohesion and alliances between the IT and security communities.

We typically find that existing customers work to improve capabilities that cover the delivery and command-and-control stages of an attack. However, very few customers adequately protect and control encrypted traffic. Today's threat actors frequently use encrypted application traffic to deliver malware and control their attacks.

As this practice and the amount of encrypted traffic both continue to grow in organizations, customers must move deliberately to decrypt traffic and extend protection capabilities to eliminate blind spots.

We also consistently see customers with immature or nonexistent prevention capabilities covering the internal stages of the attack lifecycle. Limiting the extension of prevention capabilities across an architecture leaves that architecture at risk and may allow an attacker to move unchecked throughout the network.

Now that we have discussed the capabilities we assess to prevent successful attacks, in the next section, we will discuss how we measure prevention capability readiness. As prevention readiness improves, so does our confidence that we understand and have control over everything happening in a controlled enterprise.

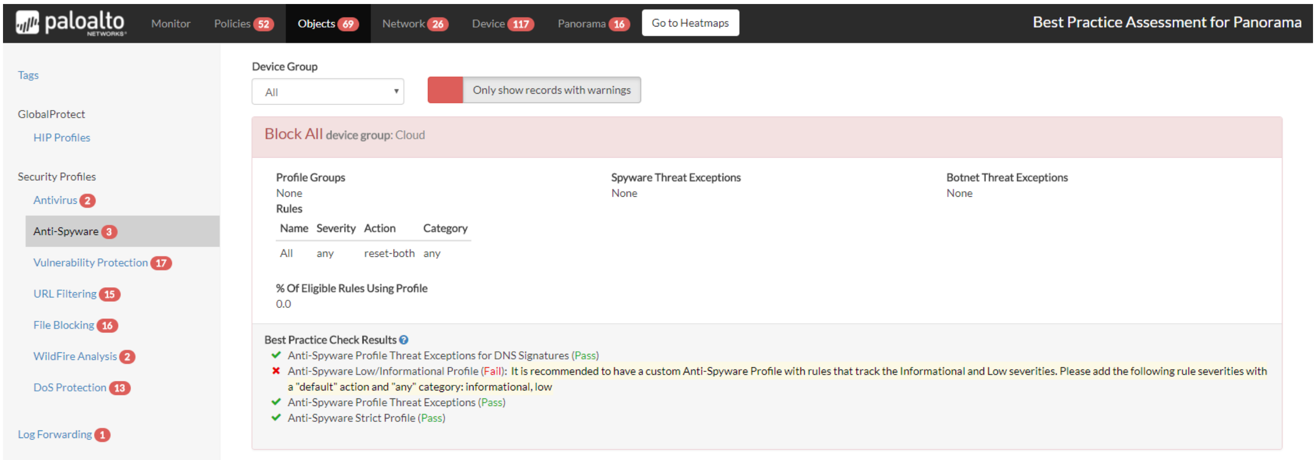
Prevention Transformation Measurement

An organization that is serious about preventing successful attacks must be able to measure its prevention readiness. This section explains how our assessment works. The output metrics give leadership confidence that the enterprise is operating as intended, with the modern capabilities required to prevent successful attacks.

Best Practice Assessment for NGFW and Panorama

A limitation of the Prevention Posture Assessment, we found, was the lack of "factual" data to back up the assertions made in the assessment. For this reason, we created the Best Practice Assessment and a family of Configuration Heatmaps for NGFW and Panorama™ network security management.

The Best Practice Assessment, or BPA, assesses configurations, identifies risks and provides recommendations on how a customer can remediate issues. The assessment compares current configurations to best practices, producing a guide to which best practices are, and are not, being utilized. This guide includes details of best practice recommendations per feature. Figure 4 shows an example of this output.



Device Group: All

Block All device group: Cloud

Profile Groups: None

Spyware Threat Exceptions: None

Botnet Threat Exceptions: None

Rules

Name	Severity	Action	Category
All	any	reset-both	any

% Of Eligible Rules Using Profile: 0.0

Best Practice Check Results

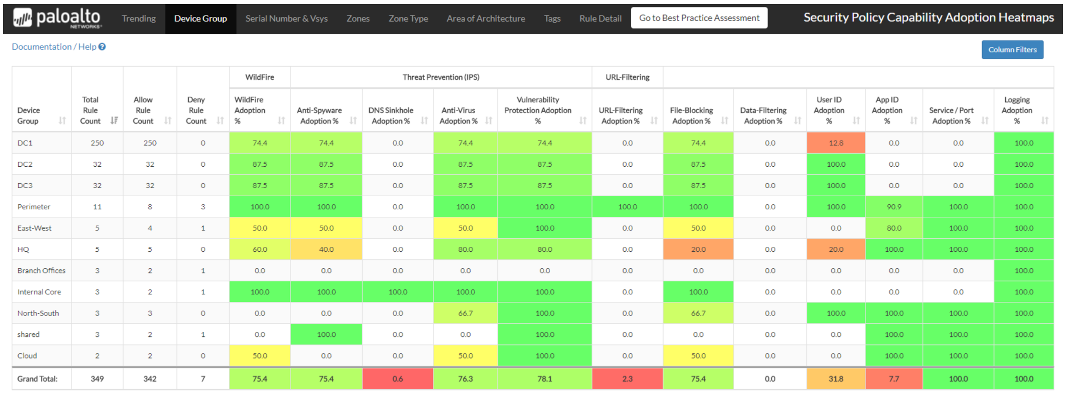
- ✓ Anti-Spyware Profile Threat Exceptions for DNS Signatures (Pass)
- ✗ Anti-Spyware Low/Informational Profile (Fail): It is recommended to have a custom Anti-Spyware Profile with rules that track the Informational and Low severities. Please add the following rule severities with a "default" action and "any" category: informational, low
- ✓ Anti-Spyware Profile Threat Exceptions (Pass)
- ✓ Anti-Spyware Strict Profile (Pass)

Figure 4: BPA output for a device group

Heatmaps provide visual representations of the configuration of prevention capabilities on the platform, helping to measure the extensible configuration for all areas of the architecture.

Figure 5 shows a view of capabilities and their configurations based on device groups. Prevention capabilities are listed across the top, with adoption for each part of the architecture provided below each capability. All heatmaps are based on "enable/allow" rules configured on the platform, along with profiles that are activated on the rules. Don't be discouraged by the color-coding – red does not mean "bad." The goal of these heatmaps is to determine if the IT and security teams have configured the platform as intended. The color code can be of your choosing, and we have customers who change it often.

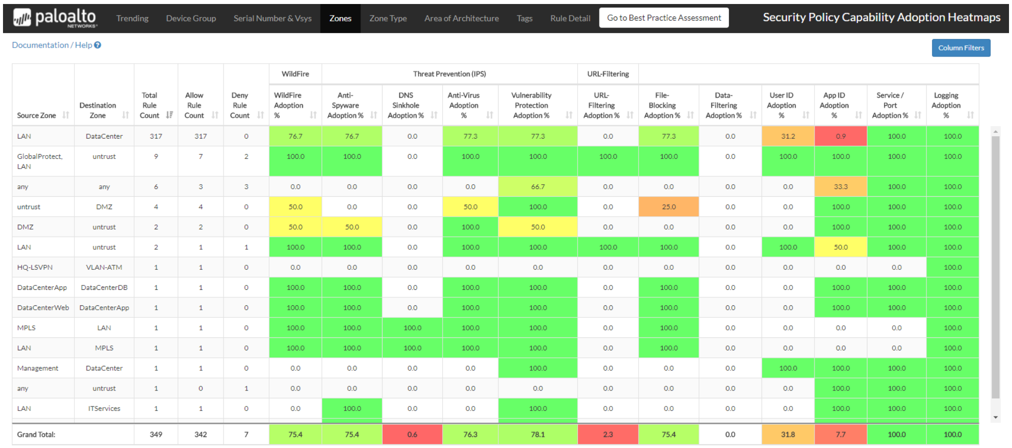
Figure 5 also shows a "broad brush" heatmap limited to overall device configuration, without detailed understanding of individual rules and capability profiles. However, it still helps IT and security professionals collaborate on using the platform to protect and control their perimeter and data center locations.



				WildFire	Threat Prevention (IPS)				URL-Filtering						
Device Group	Total Rule Count	Allow Rule Count	Deny Rule Count	WildFire Adoption %	Anti-Spyware Adoption %	DNS Sinkhole Adoption %	Anti-Virus Adoption %	Vulnerability Protection Adoption %	URL-Filtering Adoption %	File-Blocking Adoption %	Data-Filtering Adoption %	User ID Adoption %	App ID Adoption %	Service / Port Adoption %	Logging Adoption %
DC1	250	250	0	74.4	74.4	0.0	74.4	74.4	0.0	74.4	0.0	12.8	0.0	0.0	100.0
DC2	32	32	0	87.5	87.5	0.0	87.5	87.5	0.0	87.5	0.0	100.0	0.0	0.0	100.0
DC3	32	32	0	87.5	87.5	0.0	87.5	87.5	0.0	87.5	0.0	100.0	0.0	0.0	100.0
Perimeter	11	8	3	100.0	100.0	0.0	100.0	100.0	100.0	100.0	0.0	100.0	90.9	100.0	100.0
East-West	5	4	1	50.0	50.0	0.0	50.0	100.0	0.0	50.0	0.0	0.0	80.0	100.0	100.0
HQ	5	5	0	60.0	40.0	0.0	80.0	80.0	0.0	20.0	0.0	20.0	100.0	100.0	100.0
Branch Offices	3	2	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
Internal Core	3	2	1	100.0	100.0	100.0	100.0	100.0	0.0	100.0	0.0	0.0	0.0	0.0	100.0
North-South	3	3	0	0.0	0.0	0.0	66.7	100.0	0.0	66.7	0.0	100.0	100.0	100.0	100.0
shared	3	2	1	0.0	100.0	0.0	0.0	100.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0
Cloud	2	2	0	50.0	0.0	0.0	50.0	100.0	0.0	50.0	0.0	0.0	100.0	100.0	100.0
Grand Total:	349	342	7	75.4	75.4	0.6	76.3	78.1	2.3	75.4	0.0	31.8	7.7	100.0	100.0

Figure 5: Example of prevention capability adoption by device group

Figure 6 shows a much more granular heatmap of specific zones in the platform configuration. This is an example of a notable pattern we have observed. Most organizations intend to provide full protection and control for internet access points but do not consider enabling protection on internal traffic.

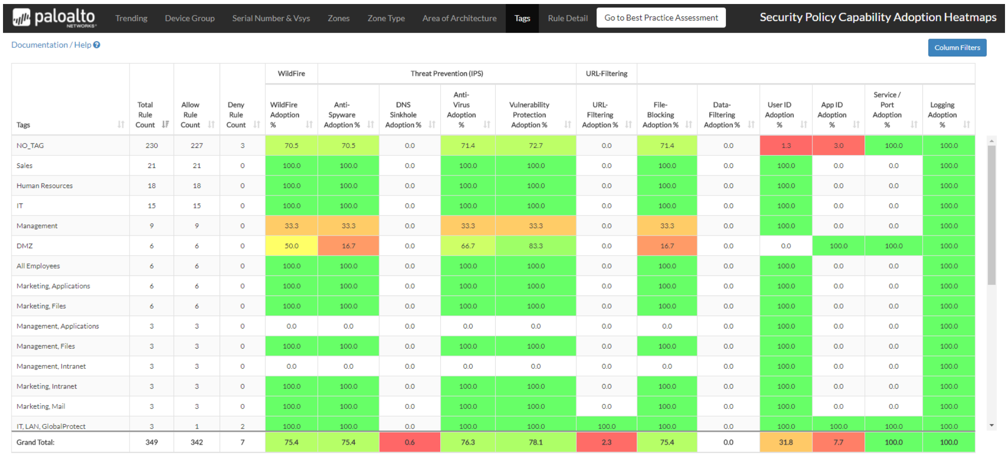


					WildFire	Threat Prevention (IPS)				URL-Filtering						
Source Zone	Destination Zone	Total Rule Count	Allow Rule Count	Deny Rule Count	WildFire Adoption %	Anti-Spyware Adoption %	DNS Sinkhole Adoption %	Anti-Virus Adoption %	Vulnerability Protection Adoption %	URL-Filtering Adoption %	File-Blocking Adoption %	Data-Filtering Adoption %	User ID Adoption %	App ID Adoption %	Service / Port Adoption %	Logging Adoption %
LAN	DataCenter	317	317	0	76.7	76.7	0.0	77.3	77.3	0.0	77.3	0.0	31.2	0.9	100.0	100.0
GlobalProtect, LAN	untrust	9	7	2	100.0	100.0	0.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0
any	any	6	3	3	0.0	0.0	0.0	0.0	66.7	0.0	0.0	0.0	0.0	33.3	100.0	100.0
untrust	DMZ	4	4	0	50.0	0.0	0.0	50.0	100.0	0.0	25.0	0.0	0.0	100.0	100.0	100.0
DMZ	untrust	2	2	0	50.0	50.0	0.0	100.0	50.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0
LAN	untrust	2	1	1	100.0	100.0	0.0	100.0	100.0	100.0	100.0	0.0	100.0	50.0	100.0	100.0
HQ-LSVPN	VLAN-ATM	1	1	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0
DataCenterApp	DataCenterDB	1	1	0	100.0	100.0	0.0	100.0	100.0	0.0	100.0	0.0	0.0	100.0	100.0	100.0
DataCenterWeb	DataCenterApp	1	1	0	100.0	100.0	0.0	100.0	100.0	0.0	100.0	0.0	0.0	100.0	100.0	100.0
MPLS	LAN	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	0.0	0.0	0.0	0.0	100.0
LAN	MPLS	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	0.0	0.0	0.0	0.0	100.0
Management	DataCenter	1	1	0	0.0	0.0	0.0	0.0	100.0	0.0	0.0	0.0	100.0	100.0	100.0	100.0
any	untrust	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0
LAN	ITServices	1	1	0	0.0	100.0	0.0	0.0	100.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0
Grand Total:		349	342	7	75.4	75.4	0.6	76.3	78.1	2.3	75.4	0.0	31.8	7.7	100.0	100.0

Figure 6: Prevention capability adoption by zone example

From a prevention-readiness perspective, it is not enough to protect only the perimeter. Going through the capabilities using this view, we can manage customer expectations and confirm that the platform is configured and operating as intended for all zones. This gives customers confidence that they can get the best possible prevention from their investment, and it ensures we build continuous operational rigor around reporting customers' prevention readiness.

Our third heatmap, in Figure 7, is based on tagging. Organizations that use tagging well ought to appreciate this view as a complement to the other heatmaps. If you don't use tagging, reach out to a Palo Alto Networks representative for help with building and implementing a tagging strategy. It will be well worth your time to make sure you're taking full advantage of the platform's prevention capabilities.



				WildFire	Threat Prevention (IPS)				URL-Filtering						
Tags	Total Rule Count	Allow Rule Count	Deny Rule Count	WildFire Adoption %	Anti-Spyware Adoption %	DNS Sinkhole Adoption %	Anti-Virus Adoption %	Vulnerability Protection Adoption %	URL-Filtering Adoption %	File-Blocking Adoption %	Data-Filtering Adoption %	User ID Adoption %	App ID Adoption %	Service / Port Adoption %	Logging Adoption %
NO_TAG	230	227	3	70.5	70.5	0.0	71.4	72.7	0.0	71.4	0.0	1.3	3.0	100.0	100.0
Sales	21	21	0	100.0	100.0	0.0	100.0	100.0	0.0	100.0	0.0	100.0	0.0	0.0	100.0
Human Resources	18	18	0	100.0	100.0	0.0	100.0	100.0	0.0	100.0	0.0	100.0	0.0	0.0	100.0
IT	15	15	0	100.0	100.0	0.0	100.0	100.0	0.0	100.0	0.0	100.0	0.0	0.0	100.0
Management	9	9	0	33.3	33.3	0.0	33.3	33.3	0.0	33.3	0.0	100.0	0.0	0.0	100.0
DMZ	6	6	0	50.0	16.7	0.0	66.7	83.3	0.0	16.7	0.0	0.0	100.0	100.0	100.0
All Employees	6	6	0	100.0	100.0	0.0	100.0	100.0	0.0	100.0	0.0	100.0	0.0	0.0	100.0
Marketing, Applications	6	6	0	100.0	100.0	0.0	100.0	100.0	0.0	100.0	0.0	100.0	0.0	0.0	100.0
Marketing, Files	6	6	0	100.0	100.0	0.0	100.0	100.0	0.0	100.0	0.0	100.0	0.0	0.0	100.0
Management, Applications	3	3	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0	100.0
Management, Files	3	3	0	100.0	100.0	0.0	100.0	100.0	0.0	100.0	0.0	100.0	0.0	0.0	100.0
Management, Intranet	3	3	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0	100.0
Marketing, Intranet	3	3	0	100.0	100.0	0.0	100.0	100.0	0.0	100.0	0.0	100.0	0.0	0.0	100.0
Marketing, Mail	3	3	0	100.0	100.0	0.0	100.0	100.0	0.0	100.0	0.0	100.0	0.0	0.0	100.0
IT, LAN, GlobalProtect	3	1	2	100.0	100.0	0.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0
Grand Total:	349	342	7	75.4	75.4	0.6	76.3	78.1	2.3	75.4	0.0	31.8	7.7	100.0	100.0

Figure 7: Prevention capability adoption by tagging

The configuration heatmaps are intended to provide consistent, simple, nontechnical feedback on your prevention readiness. We want to build confidence that we're doing everything we can to take away an attacker's ability to use known vectors, techniques and tools.

Metrics to Build IT and Security Leadership Confidence

Our passion and dedication to prevention innovation is paramount at Palo Alto Networks. As such, we know it is important to build IT and security leaders' confidence that their enterprises are operating as intended and protected as much as possible. Certain metrics are especially relevant here, as shown in Figure 8.

Leveraging KPIs to Get Customers Thinking From the Inside Out, Instead of the Outside In

Data center and cloud

- Amount of unknown TCP – Goal: 0
- Amount of unknown UDP – Goal: 0
- Amount of unexpected traffic – Goal: 0
- Rules without application and user policies – Goal: 0
- Internet access rules without full IPS, sandboxing and file blocking – Goal: 0

Sanctioned SaaS

- Number of sanctioned SaaS apps without user control – Goal: 0
- Number of sanctioned SaaS apps without deployed policies – Goal: 0
- Number of sanctioned SaaS apps without discovery and analysis reporting – Goal: 0
- Documented list of sanctioned SaaS – yes/no
- Amount of public-facing content from SaaS – Goal: 0

Unsanctioned SaaS

- Number of unsanctioned SaaS apps with "customer" name
- Number of unsanctioned SaaS apps without full user and policy usage control – Goal: 0
- Unsanctioned SaaS usage policy – yes/no

Figure 8: **Building IT and security leadership confidence**

All these indicators focus on the data center, cloud and SaaS areas of architecture because:

- They help reinforce an attitude of thinking and prioritizing from the inside out.
- Every goal achieved here is extensible to other areas of the architecture.
- These areas typically appear on short lists of customer priorities.
- It keeps things simple and prioritizes efforts with IT and security teams.

All metrics in Figure 8 are easy to consistently measure. In practice, it's often best not to do everything at once. We usually focus on unknown UDP, unknown TCP and unexpected traffic (i.e., known applications operating on nonstandard ports). In addition, we compile a list of all SaaS applications and check them against your existing governance policy for SaaS. If you don't have a governance policy, we will work with you to establish one.

Wrapping Things Up

Our representatives and partners are here to make prevention a reality across your architecture. Our advisors have the tools to get you to the best prevention readiness possible, and we will continue to innovate and iterate on these tools in the future. These are complimentary, added-value items – part of our commitment to prevent successful cyberattacks and protect our digital way of life. For this reason, we created the Best Practice Assessment, or BPA, and the Prevention Posture Assessment, or PPA.

For more information, please visit paloaltonetworks.com/preventionarchitecture.

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