Security Posture Assessment

Simplify Your Security Roadmap

The Security Posture Assessment (SPA) supports your cybersecurity planning and strategy by providing in-depth, current state analysis and expert-level recommendations for your security environment.

Simplify your road to best practice adoption to **maximize your return on investment** and **increase your cyber resilience**.

What Is the Secure Posture Assessment

The SPA is a powerful, highly flexible consultative assessment tool that helps you achieve a broad spectrum of outcomes from your security architecture and covers all deployment scenarios that Palo Alto Networks supports. It uses data gathered via an interview to autonomously generate next steps and future state recommendations.

The SPA customizes recommendations based on your deployment scenario, relevant applications, and many other security capabilities. It then creates a security roadmap that can be displayed in various formats designed for multiple decision-makers ranging from executive leadership to highly technical security engineers.

Why Use the SPA?

With a highly flexible modular structure, fully automated recommendations, and customizable reporting ability, the SPA is the most advanced tool of its kind from Palo Alto Networks.

It provides audience-specific recommendations ready to share within minutes of completing the interview. Through the wealth of embedded security knowledge, the SPA can contextualize even the most complex environments with accuracy and speed.

Despite its highly technical backend, this tool is extremely approachable and intuitive, making it accessible to anyone looking to improve their security posture.

How Does It Benefit Me?

The SPA can build a security roadmap designed specifically for your organization, taking you from your current state of cyber resilience to any security outcome you need. This includes:

- A suite of views to better understand your current state.
- A definition of the future state we recommend.
- A roadmap for your security teams.
- An executive summary to gain support from your organization's leadership.

We ensure that you have everything you need to successfully adopt Palo Alto Networks solutions and achieve greater value on your investment—all while helping you earn your position as a trusted expert security advisor to your organization.
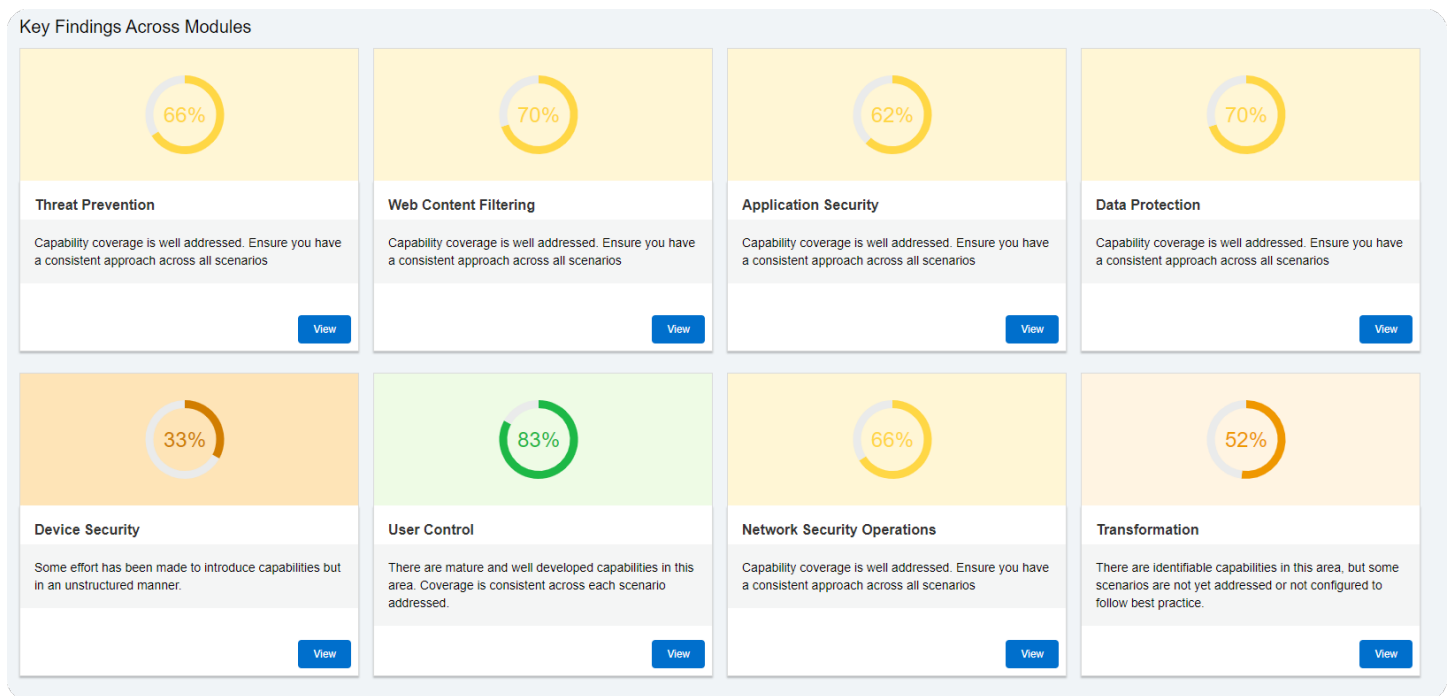

Key Findings Across Modules

66%	70%	62%	70%
Threat Prevention	**Web Content Filtering**	**Application Security**	**Data Protection**
Capability coverage is well addressed. Ensure you have a consistent approach across all scenarios	Capability coverage is well addressed. Ensure you have a consistent approach across all scenarios	Capability coverage is well addressed. Ensure you have a consistent approach across all scenarios	Capability coverage is well addressed. Ensure you have a consistent approach across all scenarios
View	View	View	View

33%	83%	66%	52%
Device Security	**User Control**	**Network Security Operations**	**Transformation**
Some effort has been made to introduce capabilities but in an unstructured manner.	There are mature and well developed capabilities in this area. Coverage is consistent across each scenario addressed.	Capability coverage is well addressed. Ensure you have a consistent approach across all scenarios	There are identifiable capabilities in this area, but some scenarios are not yet addressed or not configured to follow best practice.
View	View	View	View

Figure 1: Executive summary provides a nontechnical view of your current security posture

Network Security Capabilities				
Network Traffic		Network Locations		
Internal Users	Remote Users	Branch Office	Headquarters	Data Center
Threat Prevention	Threat Prevention	Threat Prevention	Threat Prevention	Threat Prevention
Decryption	Decryption	Decryption	Decryption	Decryption
DNS Security	DNS Security	DNS Security	DNS Security	DNS Security
Application Protection	Application Protection	Application Protection	Application Protection	Application Protection
Data Protection	Data Protection	Data Protection	Data Protection	Data Protection
User Control	User Control	Asset Discovery	Asset Discovery	Asset Discovery
Web Access Control	Web Access Control	Iot Protection	Iot Protection	Iot Protection
		DoS and Recon Protection	DoS and Recon Protection	DoS and Recon Protection
		Network Segmentation	Network Segmentation	Network Segmentation
		Automation	Automation	Automation
		Logging and Monitoring	Logging and Monitoring	Logging and Monitoring

Figure 2: Customizable heatmap provides a quick health check on entire areas of your architecture

Who Is It Designed For?

The SPA is designed for anyone seeking expert advice on how to improve their security posture. It serves a variety of roles, falling into two general categories:

Nontechnical

This role answers questions such as: "How do I implement Zero Trust architecture across my cloud applications?"

Technical (Engineers)

This role answers questions such as: "How can I construct my network so it's compliant with endpoint microsegmentation?"

What You Can Expect

· An accurate analysis of your current security posture.
· Enablement of security teams to help you best optimize existing technologies.
· Reduction in overall business risk by incorporating new technologies and security controls.

What Assessments Are Available?

· **SASE/ZTNA 2.0 Deployments**
· **Network Security Refresh/Improvement**
· **SOC Modernization**
· **Operational Technology (OT) Security**
· **Cloud and Cloud Code Security**
· **Endpoint Security Controls**
· **Enterprise Cybersecurity—In-Depth**
· **Enterprise Cybersecurity—Concise**
· **5G Capability and Readiness (Telco)**

Get an assessment →