Endpoint Workshop

Simplify Your Endpoint Security Roadmap

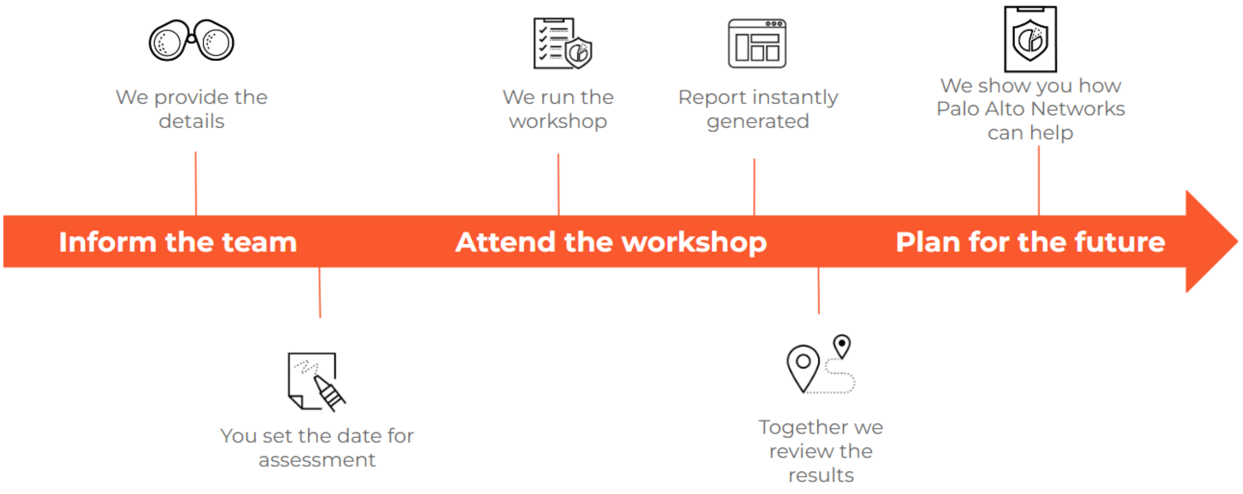
The Endpoint Assessment protects you from cyberattacks by providing current state analysis and expert-level recommendations for your security environment. Simplify your road to best practice adoption to **maximize your return on investment** and **increase your cyber resiliency**.

Overview

Reducing cyber risk and costs can't come at the expense of building a business that is equipped to meet new challenges and opportunities. Our Endpoint Assessment can help you reduce risk and improve operational resilience, so you can embrace digital with confidence. We offer a complimentary Endpoint assessment that is tailored to your organisation's cyber maturity objectives. By understanding your current security posture, we design a roadmap that's right for you.

The Endpoint Assessment covers the following technology areas and takes approximately one hour to complete.

- Asset Management
- Endpoint Protection
- Detection and Response
- Ransomware Protection
- Application Control
- User Control
- Device Control
- Data Protection



Inform the team

We provide the details

You set the date for assessment

Attend the workshop

We run the workshop

Report instantly generated

Together we review the results

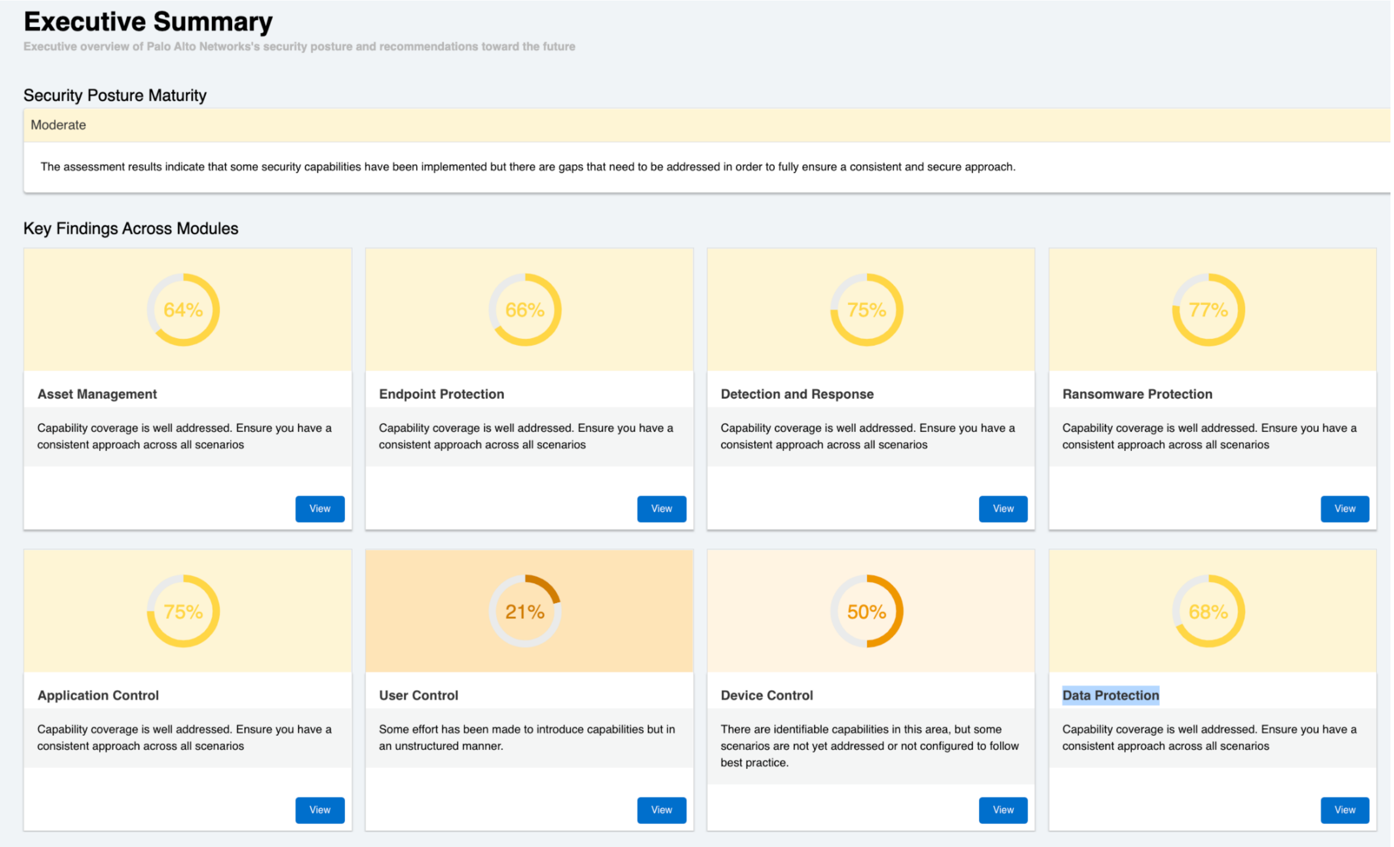
Plan for the future

We show you how Palo Alto Networks can help

What you can Expect

- An accurate analysis of your current security posture with regards to all the components that make up Endpoint security..
- Enablement of security teams so you may best optimize existing technologies
- Reduction in overall business risk by incorporating new technologies and security controls

Fig 1: Executive Summary - aggregate, non-technical view of significant overall findings.



Executive Summary

Executive overview of Palo Alto Networks's security posture and recommendations toward the future

Security Posture Maturity

Moderate

The assessment results indicate that some security capabilities have been implemented but there are gaps that need to be addressed in order to fully ensure a consistent and secure approach.

Key Findings Across Modules

64%
Asset Management
Capability coverage is well addressed. Ensure you have a consistent approach across all scenarios

66%
Endpoint Protection
Capability coverage is well addressed. Ensure you have a consistent approach across all scenarios

75%
Detection and Response
Capability coverage is well addressed. Ensure you have a consistent approach across all scenarios

77%
Ransomware Protection
Capability coverage is well addressed. Ensure you have a consistent approach across all scenarios

75%
Application Control
Capability coverage is well addressed. Ensure you have a consistent approach across all scenarios

21%
User Control
Some effort has been made to introduce capabilities but in an unstructured manner.

50%
Device Control
There are identifiable capabilities in this area, but some scenarios are not yet addressed or not configured to follow best practice.

68%
Data Protection
Capability coverage is well addressed. Ensure you have a consistent approach across all scenarios

Who should attend the workshop

The following roles at your organisation should be invited to attend the session:

- Security Architects
- Network and Infrastructure Operations
- Endpoint Dev SecOps
- Helpdesk
- Data Privacy Officer or Cyber Risk Analyst

The workshop comprises the following Security capabilities and questions:

We assess your organisation's Endpoint Security Capability maturity against in the Endpoint Technology Categories.

Technology Category	Security Capability	Question
Asset Management	Asset Discovery	How do you discover and manage endpoints across the organisation?
Asset Management	Critical Asset Policy	Do you apply stronger policy to critical systems?
Asset Management	Asset Inventory	How do you discover and manage installed applications for all workstation and server endpoints?
Asset Management	Asset Management	How do you track asset configuration changes?
Asset Management	Endpoint Security Automation	How do you maintain your endpoint security updates?
Asset Management	OS patching	How do you roll out OS level patches and hotfixes?
Endpoint Protection	Vulnerability Discovery	Do you conduct regular pentesting of your environment?
Endpoint Protection	Vulnerability Protection	How do you discover and manage vulnerabilities on endpoints?
Endpoint Protection	Automated Malware Analysis	Are new Indicators of Compromise (IOCs) found in malicious files automatically turned into network and endpoint prevention updates?
Endpoint Protection	Endpoint Detect and Response	Are you able to prevent unauthorized agent interactions like shutdown or telemetry interference?
Endpoint Protection	Legacy System Control	How do you monitor and protect unsupported or legacy OS versions?
Detection and Response	Exploit Prevention	How do you detect and prevent exploits on physical and virtual Windows, Linux and MacOS systems?

Technology Category	Security Capability	Question
Detection and Response	Automated Malware Analysis	Do you use static and dynamic analysis (sandbox) to detect and block malicious files?
Detection and Response	Endpoint Detect and Response	Do you perform periodic scanning of workstations and servers?
Detection and Response	Endpoint Detect and Response	How do you detect and prevent corporate policy violations?
Detection and Response	Endpoint Detect and Response	How do you create and deploy custom detection policies to the endpoints and servers?
Detection and Response	Log Retention / Log Quality	How do you collect and store data from the endpoints and servers? Particularly for forensic analysis
Detection and Response	Log Consolidation	Are logs forwarded to a central logging repository for security monitoring purposes?
Detection and Response	Log Analysis	Are you performing log stitching for incident analysis with network and other log sources?
Ransomware Protection	Anti-Malware	How to do you detect and prevent malware presence and execution on physical and virtual systems?
Ransomware Protection	Ransomware Protection	How do you prevent lateral movement of ransomware attacks?
Ransomware Protection	Data Loss Prevention	Can you identify or prevent (via network or endpoint logs) data exfiltration events?
Ransomware Protection	Ransomware Protection	How do you prevent encryption of systems by ransomware attacks?
Application Control	Unsanctioned Application Control	Do you have the ability to limit execution of unwanted or unsanctioned applications?
Application Control	SaaS Visibility	Can you identify user/device access to corporate SaaS applications
Application Control	Application Restriction (Exploit Prevention)	How do you control and restrict operations on endpoints? (command line execution, processes, activities from logical drives, activities from hardware locations, etc.?

Technology Category	Security Capability	Question
Application Control	Privileged Process Protection (process spawning protection)	How do you prevent unwanted process spawning activities? (powershell launching command)
User Control	Privileged User Management	How do you control privilege account access on endpoints?
User Control	Behavioral Analytics	Do you leverage behavioral analysis to detect advanced attacks?
Device Control	BYOD	Do you have a policy for BYOD device access and privilege?
Device Control	Remote Access	Do you allow split tunnel from remote devices?
Device Control	Host Inspection	Do you apply any security posture assessment of devices either on-premise or remote?
Device Control	External Device Management	Do you scan, inspect or prevent the use of removable devices?
Device Control	Host Based Firewall	Do you leverage a host-based firewall to control network access to and from endpoints?
Device Control	Host Hardening	Do you have a host hardening process or solution to limit attack surface
Data Protection	Data Management	Do you have a data management strategy?
Data Protection	Data Classification	Have you implemented a data classification methodology?
Data Protection	Data Encryption	How do you verify and enforce encryption of sensitive data in-transit and at-rest?
Data Protection	Disk Encryption	Do you apply disk encryption on your endpoints?
Data Protection	Search and Destroy	How do you eradicate malicious or suspicious files from endpoints as part of a breach mitigation workflow?