SASE Workshop

Simplify Your SASE Security Roadmap

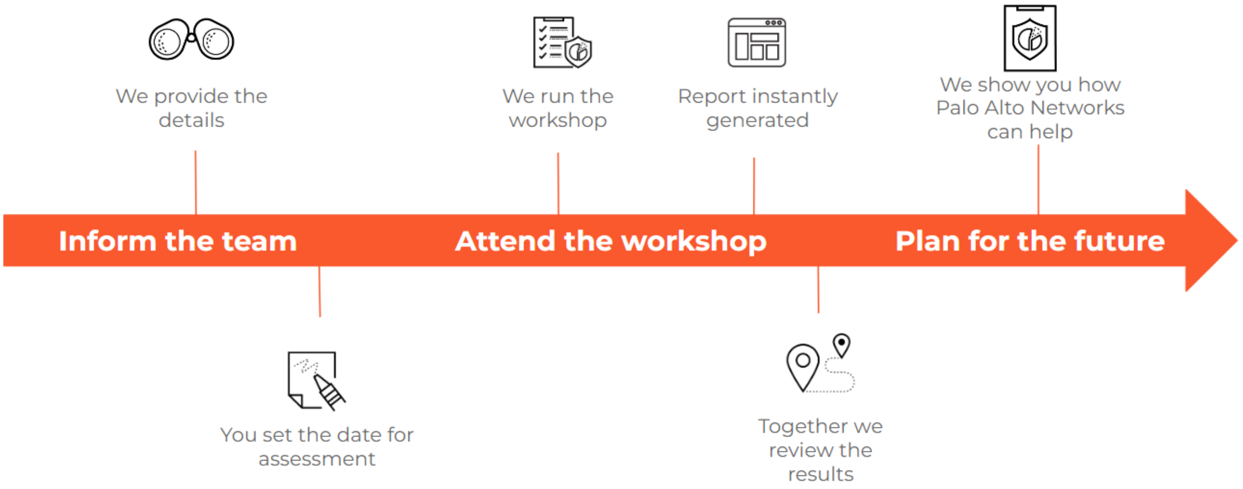
The SASE Assessment protects you from cyberattacks by providing current state analysis and expert-level recommendations for your security environment. Simplify your road to best practice adoption to **maximize your return on investment** and **increase your cyber resiliency**.

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 SASE Assessment can help you reduce risk and improve operational resilience, so you can embrace digital with confidence. We offer a complimentary SASE 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 SASE Assessment covers the following technology areas and takes approximately one hour to complete.

- Zero Trust Network Access (ZTNA 2.0)
- Autonomous Digital Experience Management (ADEM)
- Secure Web Gateway (SWG)
- Cloud Access Security Broker (CASB)
- Data Loss Prevention (DLP)
- Software Defined Networking (SD-WAN)
- Internet of Things device security (IoT)



We provide the details

We run the workshop

Report instantly generated

We show you how Palo Alto Networks can help

Inform the team

Attend the workshop

Plan for the future

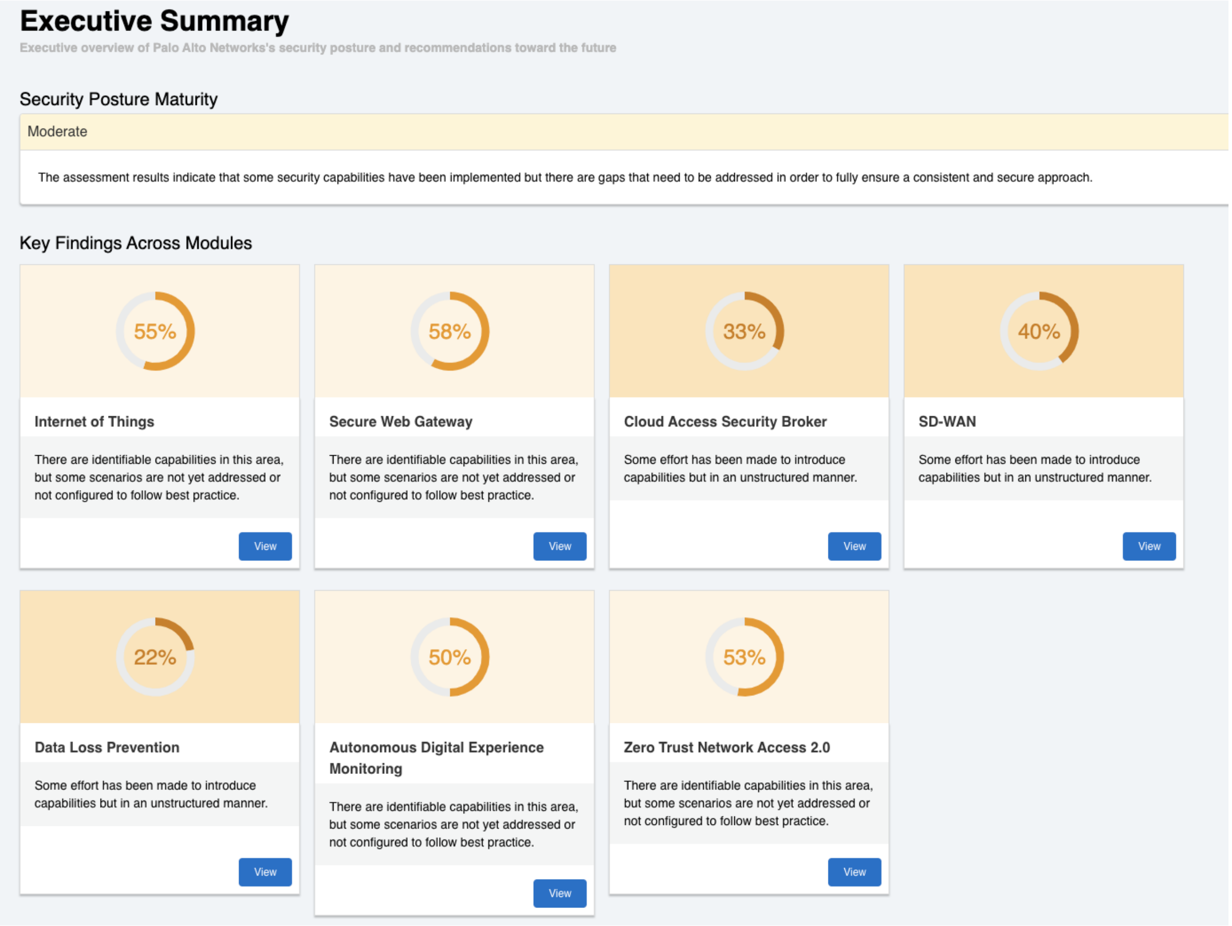
You set the date for assessment

Together we review the results

What you can Expect

- An accurate analysis of your current security posture with regards to all the components that make up SASE - Secure Access Service Edge.
- 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

55%

Internet of Things

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

58%

Secure Web Gateway

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

33%

Cloud Access Security Broker

Some effort has been made to introduce capabilities but in an unstructured manner.

40%

SD-WAN

Some effort has been made to introduce capabilities but in an unstructured manner.

22%

Data Loss Prevention

Some effort has been made to introduce capabilities but in an unstructured manner.

50%

Autonomous Digital Experience Monitoring

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

53%

Zero Trust Network Access 2.0

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

Who should attend the workshop

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

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

The workshop comprises the following Security capabilities and questions:

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

Technology Category	Security Capability	Question	Question Background
ZTNA 2.0	Remote User Access	How do you control and manage Remote User Access?	VPN is the traditional method of remote user access but is typically configured separately to other controls and often bypasses security checkpoints in favor of resource access.
ZTNA 2.0	Remote User Control	Do remote users have the same security controls as on-premise users?	Users and data are now located in many different places and often users are transitioning between an office based location and home or remote. It's important to recognize that the security capability set remains consistent regardless of a users location.
ZTNA 2.0	Device and User Management	Can you provide different security access levels based on User and Device?	Device inspection is increasingly important as an additional point of reference for access control. Ensure inspection of all available credentials when permitting access to protected resources.
ZTNA 2.0	3rd Party Access	How do you manage 3rd party user access?	3rd party users should have a tighter set of security controls, given a general lack of oversight into their behavior on other systems outside your control.
ZTNA 2.0	Supply Chain	Do you secure supply chain connectivity to your organisation?	Supply chain breaches are increasing so it's vital that supply chain security is understood and any B2B connections are monitored for threat activity.

ZTNA 2.0	Application Control	Is application access controlled in network security policies?	Application enforcement removes the reliance on port and protocol based restriction and only allows the specific applications chosen. Defining a set of allowed applications has a number of benefits for network speed and simplicity beyond the security functions
ZTNA 2.0	User Control	Is access to systems based on user identity controlled by a firewall or other network device?	While most applications have some form of user control, network level user access control creates a consistent environment and removes the complexity of managing multiple user authentication sources
ZTNA 2.0	Centralised Logging	Are logs forwarded to a central logging repository for security monitoring purposes?	Audit logging should be consistent and centralised across cloud platforms to provide an efficient and comprehensive audit trail when required
ZTNA 2.0	Integration	Do your current security controls work together and with other business systems?	Having a cohesive set of security controls is not only easier to manage, but generally more effective than a disparate set of tools.
ZTNA 2.0	Automation	What level of automation exists in your security operations?	Any repetitive tasks that can be automated - should be. This allows skilled workers to focus on more complex tasks like threat hunting.
SWG	URL Filtering	How do you inspecting web traffic, URLs and other internet traffic flows?	URL filtering limits access by comparing web traffic against a database to prevent employees from accessing unproductive, harmful sites such as phishing pages.
SWG	DNS Protection	How do you inspect DNS traffic for tunneling and threat activity?	As a common internet service, DNS is often used to hide malicious traffic as the likelihood of access is high. Visibility into DNS traffic flows therefore become critical in identifying incoming or present threats.
SWG	DNS DGAs	Are you able to detect and block malicious domains created by domain generation algorithms? (DGAs)	Domain generation algorithms (DGA) are algorithms seen in various families of malware that are used to periodically generate a large number of domain names that can be used as rendezvous points with their command and control servers.
SWG	Credential Theft Prevention	How do you prevent Credential Phishing attempts?	Corporate credentials are often the weakest link in the security portfolio so it's important to know where they are being used outside of the organisation. In addition, some phishing campaigns are incredibly complex so have an automated system to alert on and restrict credential use is important

SWG	Anti-Malware	Is a network level Anti-Malware solution in-line for all traffic?	By addressing malware at the application and network level, you restrict the threat closer to the source and provide full network coverage regardless of endpoint.
SWG	Anti-Spyware	How do you control and prevent malicious command-and-control activities?	DNS sinkholing and URL filtering capabilities are an effective method for preventing C&C flows from leaving your network if a device is compromised
SWG	Vulnerability Management	Is a network-level Vulnerability protection solution in line for all traffic?	In addition to host based vulnerability protection, network VP provides a safeguard for IOT devices, and other network connected assets that do not have endpoint coverage
SWG	Decryption	Is SSL decryption available in-line with all network traffic flows?	The majority of traffic to and from the internet is now encrypted and attackers are utilising SSL connections to bypass security layers unable to inspect
CASB	User Activity Reporting	How do you report on and control user activity within SaaS applications?	With more and more data stored in SaaS applications it's important to maintain the same visibility and control as internally hosted applications. The responsibility for securing this data is unchanged, despite a change in location.
CASB	Anti-Malware	How do you protect from malware and threats within SaaS applications?	Threat prevention capabilities must extend across all corporate resources.
CASB	Sanctioned and Unsanctioned Access	How is access to sanctioned, tolerated and unsanctioned SaaS applications monitored and controlled?	Is it good practice to create and enforce applications lists to safeguard your organisation from unauthorised data access.
CASB	Content Storage Control	How do you identify if sensitive content is being stored in your sanctioned SaaS applications?	With sensitive data, it's important to identify as much context as possible. ie Who, What, Why, When in order for the correct decision to be made. SSL Decryption and data inspection drive this capability
CASB	Data Leakage Prevention	How do you control transfer of data into and out of key SaaS applications?	Data exfiltration can occur through legitimate paths or through compromise so it's important to be able to track the flow of data and prevent critical data from leaving the network
SD-WAN	Consistency and Convergence	How are you managing consistent performance and security across a diverse workforce?	With remote work, shift to cloud for resources and other business initiatives that are changing the corporate perimeter, it's important to maintain a consistent security set and user experience across all applications and services.

SD-WAN	Application Optimisation	Is your WAN application aware? Can you measure and adjust application performance?	Critical applications are often unique across different businesses and teams so having the ability to prioritize applications based on their importance to your users allows for improved experience and provides operational benefits.
SD-WAN	New Site Deployment	How easy is it to deploy a new site or service?	Reducing the overall time in deploying a new site, or migrating services from one location to another quickly creates more opportunity for growth and lowers cost and operational overhead.
SD-WAN	Connectivity	Is there resiliency and redundancy in your network connectivity?	Having multiple WAN connections ensures business applications are always available but it's also important to maintain value from this architecture. Active/Passive redundancy is ok, but active/active provides better value and dynamically assigning applications across links to ensure application performance adds an additional set of benefits.
SD-WAN	Troubleshooting	How hard is it to troubleshooting WAN connectivity issues?	With MPLS, managed WAN or internet based VPNs - most of the network path is hidden from operational view. With a SASE architecture, that visibility is returned so that an operations team can easily see where a performance issue is across the entire WAN infrastructure.
ADEM	User Visibility	How do you track user activity at the network level?	Monitoring user access to resources is the first step to identifying normal and abnormal behaviours. In some areas of the network, user enforcement may not be necessary however for forensic purposes, having the ability to show user activity is vital to understanding the chain of events
ADEM	Troubleshooting	How do you troubleshoot application and network performance issues for your employees that are working from home?	Local networks not under management can often be the cause of a performance issue when working remotely. Having visibility into the entire network flow allows for fast and effective support.
DLP	Sensitive Data Visibility	Do you identify sensitive content in network traffic?	With sensitive data, it's important to identify as much context as possible. ie Who, What, Why, When in order for the correct decision to be made. SSL Decryption and data inspection drive this capability

DLP	Sensitive Data Control	Do you prevent sensitive content from leaving the network?	Data exfiltration can occur through legitimate paths or through compromise so it's important to be able to track the flow of data and prevent critical data from leaving the network
DLP	Data Transfer	How is the transfer of files controlled in both download and upload direction?	When you understand the flow of files between network segments, and the applications delivering them, you can make policy decisions that enhance your overall security posture
IoT	IoT Visibility	Do you have a comprehensive catalog of your OT/IOT assets? Is this dynamic or static?	Knowing what devices are connected to your networks is the first point in understanding the risks they may pose to neighboring devices.
IoT	IoT Control	Do you enforce any protections of IoT devices? Segmentation or traffic inspection?	As IoT devices typically have no endpoint protection software - the network is where enforcement of security must take place.
IoT	Vulnerability Management	Is a network-level Vulnerability protection solution in line for IoT Devices?	In addition to host based vulnerability protection, network VP provides a safeguard for IOT devices, and other network connected assets that do not have endpoint coverage