Cloud Workshop

Simplify Your Cloud Security Roadmap

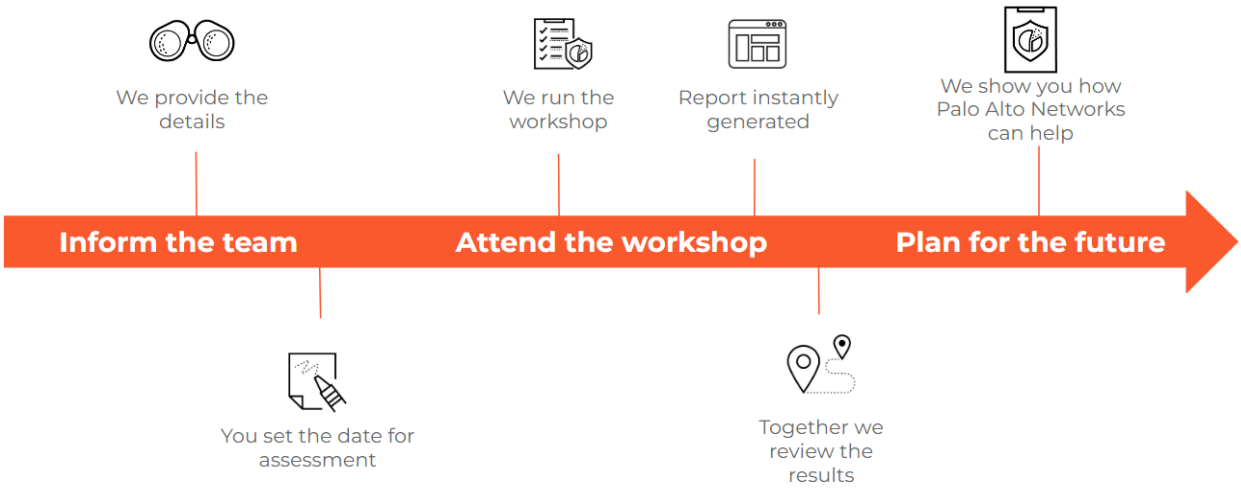
The Cloud Assessment protects you from cyberattacks by providing current state analysis and expert-level recommendations for your security environment. Simplify your road to best practice adoption to **maximize your return on investment** and **increase your cyber resiliency**.

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

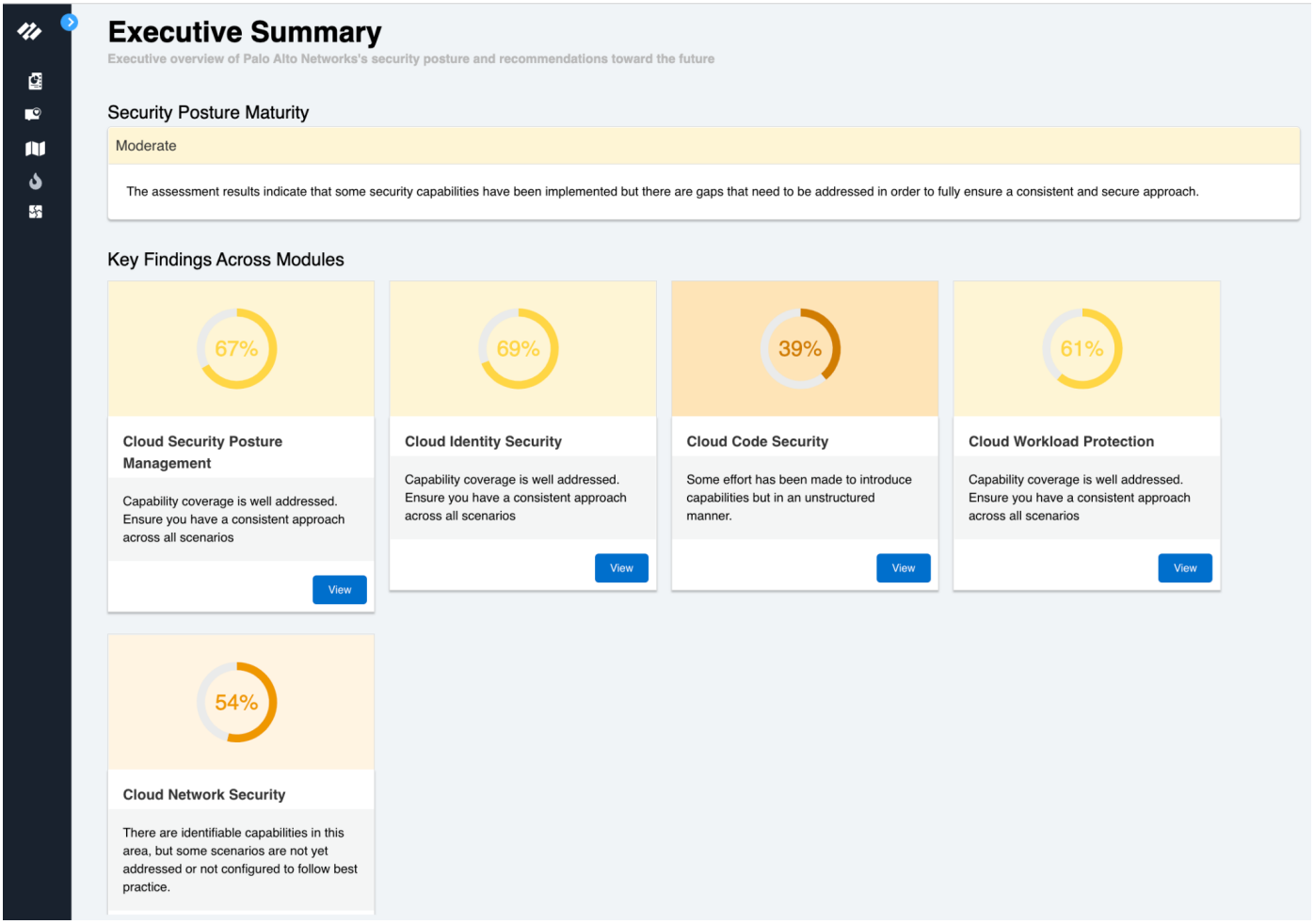
- Cloud Security Posture Management
- Identity Security
- Code Security
- Workload Protection
- Cloud Network Security



What you can Expect

- An accurate analysis of your current security posture with regards to all the components that make up Cloud 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.



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 Cloud Security Capability maturity against in the Cloud Technology Categories.

Technology Category	Security Capability	Question
Advanced Threat Prevention	Anti-Malware	How do you detect and remediate malware at-rest within your public cloud environments?
Advanced Threat Prevention	Anti-Spyware	How do you control and prevent malicious command-and-control activities?
Advanced Threat Prevention	Sandboxing	How do you ensure non-sensitive files from all traffic on all ports are sent to an automated malware analysis solution?
Advanced Threat Prevention	Content Updates	How often do you perform content updates for threat prevention capabilities (AV, IPS, C2, DNS, URL)?
Advanced Threat Prevention	Apps and API	How do you protect your web applications and application APIs against network-based attacks?
Advanced Threat Prevention	Anti-Ransomware	How do you prevent encryption of systems by ransomware attacks?
Application Control	Application Control	Is access over the network controlled via a least-privilege policy?
Application Control	Application Visibility	Can you identify applications in network traffic logs?
Application Control	Unidentified Traffic	How are unauthorized and unidentifiable applications identified and controlled at the network level? (e.g. evasive, tunneling, remote-access, unknown, ...)?

Technology Category	Security Capability	Question
Asset Management	Asset Discovery	How do you discover and manage your assets running inside your public cloud environments?
Asset Management	Asset Change History	How do you track all historical changes made to them?
Asset Management	Attack Surface Management	How do you keep track of all sanctioned and unsanctioned public-facing assets?
Automation and Integration	CI/CD Security	Do you have security embedded into the CI/CD pipeline to automate assessments and remediation?
Automation and Integration	SOC Integration	Do you have integration between your cloud security capabilities and SIEM/SOAR solutions?
Automation and Integration	Dynamic Threat Prevention Coverage	Does your cloud security infrastructure automatically scale to support increases/decreases in workloads and asset coverage?
Code Security	Cloud Infrastructure Code	How do you detect and remediate cloud infrastructure misconfiguration?
Code Security	IaC Templates	How do you detect and remediate IaC template misconfiguration?
Compliance	Assurance Monitoring	Do you have continuous compliance assurance monitoring in place for your cloud environments?
Compliance	Governance	Do you have a centralized view of risk across your cloud and microservices architectures?
Data Protection	Data Classification	How do you identify if sensitive content is being stored in your cloud environments?
Data Protection	Data Leakage Prevention	How do you identify if sensitive content is being shared publicly or inappropriately through your cloud environments?
Data Protection	Data Encryption	How do you verify and enforce encryption of sensitive data in-transit and at-rest?
DNS Security	DNS Restrictions	Do you restrict outbound DNS and DNS forwarders to an approved list?

Technology Category	Security Capability	Question
DNS Security	DNS Tunneling	How do you inspect DNS traffic for tunneling activity?
DNS Security	DNS DGAs	Are you able to detect and block malicious domains created by domain generation algorithms? (DGAs)
DNS Security	DNS Sinkhole	Do you sinkhole suspicious DNS queries to validate the internal source IP?
Logging	Centralised Logging	Are logs forwarded to a central logging repository for security monitoring purposes?
Logging	Log Retention	What is your log retention period for proactive monitoring and behavioral analysis purposes?
Logging	Log Storage	Do you backup logs to internal/external storage to meet compliance requirements around long-term log retention?
Compliance	Multi Cloud Management	How do you manage resources across public cloud providers?
Segmentation	Segmentation	How do you segment your network environment up to layer 7 to prevent lateral threat movement?
Segmentation	Micro Segmentation	Have you implemented microsegmentation in any network segments?
User Control	MFA	Is Multi-Factor Authentication in place to control access to critical systems, applications and data?
User Control	User Control	How do you control user access and monitor activity towards internal and external systems and applications?
User Control	User Privilege	How do you maintain visibility and control over the effective user privileges across your cloud environments?
User Control	Behavioral Analytics	Do you leverage behavioral analysis to detect advanced attacks?
Vulnerability Management	Vulnerability Discovery	Do you leverage behavioral analysis to detect advanced attacks?

Technology Category	Security Capability	Question
Vulnerability Management	Pen Testing	Do you conduct regular pentesting of your environment?
Vulnerability Management	Vulnerability Remediation	How fast are you able to remediate discovered vulnerabilities?
Web Content Filtering	URL Filtering	Do you inspect URLs and web traffic for content, malware, corporate usage reasons?
Web Content Filtering	URL Logging	Do you alert, log and correlate on known-bad, unknown and IP-based URLs?