Guide to Cybersecurity in the Age of Dynamic Attack Surfaces

In an era where the boundaries of networks are fluid and ever-expanding, securing the multitude of access points—from in-house infrastructure to cloud-based services and from supply chain partners to remote employee devices—demands unprecedented visibility and control.

What Is Attack Surface Management?

As we transition from static to dynamic networks encompassing multicloud, private, and public clouds, the concept of an attack surface has evolved. When an organization grows, especially through mergers and acquisitions, it inherits new vectors for cyberthreats. A comprehensive attack surface management (ASM) strategy isn't just about maintaining an asset inventory; it's about actively mitigating and prioritizing threats to ensure the security of an organization's expanding digital perimeter.

Cortex Xpanse: Revolutionizing ASM

Cortex Xpanse® empowers security teams to proactively manage and protect their digital terrain by:

- Detecting asset sprawl across a myriad of platforms
- Identifying stale IP records and asset expirations
- Recognizing a multitude of device types vulnerable to exploitation
- Uncovering certificate misconfigurations
- Pinpointing potential domain takeover risks
- Highlighting shadow IT and remote access protocols
- Addressing risks associated with employee assets in consumer ISP spaces

How Cortex Xpanse Delivers

The automated Cortex Xpanse platform transforms ASM by offering comprehensive processes for discovery, evaluation, and mitigation.

Discover

With precision and scale, Cortex Xpanse indexes the internet to detect assets, omitting the noise associated with scanning only open ports. Whether your organization is a burgeoning enterprise or a multinational conglomerate, Cortex Xpanse scales to meet your needs.

Assess

Beyond asset identification, Cortex Xpanse contextualizes each asset, aligning it with specific business units and stakeholders, and evaluates risks for prioritized mitigation and compliance adherence.

Remediate

Real-time policy violation alerts and integrations with platforms like ServiceNow and Splunk streamline the workflow for exposure remediation, enhancing your security team's capacity to swiftly detect and act. Automatically remediate common exposure risks, including open Remote Desktop Protocol (RDP) ports, which are a main vector for ransomware attacks.

Shortcomings of Traditional Solutions

Legacy asset inventory methods like configuration management databases (CMDBs) fall short due to manual entries and an insular focus on internal assets, missing the full scope of a modern attack surface. Risk scores provide only a temporal view, failing to track assets or mitigate risks dynamically. Even established vulnerability management tools are limited to known assets, while Cortex Xpanse extends protection to the unknown, integrating with these tools to maximize coverage and ROI.

Cortex Xpanse Use Cases in Action

From asset discovery to incident response, Cortex Xpanse offers a myriad of applications:

- Pinpoint and monitor unknown assets, integrating seamlessly with current security and IT systems.
- Enhance asset management with automated labeling and categorization, speeding up the response during security incidents.
- Navigate M&A and supply chain security with comprehensive cybersecurity audits and IT integration monitoring.
- Secure cloud environments by discovering all cloud instances and transitioning assets between sanctioned and unsanctioned environments with automated alerts.
- Strengthen security across federated ecosystems by identifying internet-based assets and misconfigurations in third-party networks.
- Streamline governance, risk, and compliance with auditable inventories and global visibility into attack surfaces and remediation efforts.
- Accelerate vulnerability management with daily updates to scan targets and alerts on new or repeating exposures.

The Impact of Cortex Xpanse on Business

Cortex Xpanse isn't just a tool; it's a transformative force for your cybersecurity operations:

- Achieve a complete, continuously updated inventory of your organization's assets.
- Slash mean time to detect (MTTD) and respond (MTTR), streamlining operational efficiency.
- Reduce costs by replacing outdated and manual processes with a singular, accurate asset repository.
- Enhance M&A visibility for strategic planning and network integration.
- Drive ecosystem-wide automation, ensuring thorough due diligence on prospective partnerships and historical acquisitions.

In summary, Cortex Xpanse equips organizations with the capability to navigate the complexities of modern attack surfaces with clarity and confidence. As the landscape evolves, so too must our approach to cybersecurity. Cortex Xpanse represents the next step in that evolution, offering a proactive, comprehensive solution to secure the digital assets of today and tomorrow.

Read the Cortex Xpanse datasheet to learn the full potential of Cortex Xpanse for your organization.

paloalto NETWORKS

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

cortex_guide-to-cybersecurity-in-the-age_070824