The CISO's Guide to Attack Surface Management

In the era of remote work and cloud adoption, the cybersecurity landscape is rapidly transforming, and with it, the nature of attack surfaces. Traditional asset management practices need to catch up with the burgeoning complexity and the dynamic nature of these new digital environments. To achieve this level of security calls for a revolutionary approach to attack surface management—one that is automated, intelligent, and proactive.

In the past, organizations could afford to manually inventory their attack surfaces at a controlled and predictable pace. However, in today's cybersecurity landscape, traditional attack surface management practices are no longer sufficient. The complexity and dynamism of attack surfaces have increased exponentially, necessitating a shift toward modern, intelligent, and automated attack surface management (ASM) solutions.

Modern Attack Surface Management Defined

The shift toward distributed teams, the ease of provisioning new cloud services, and extensive third-party connections have redefined attack surfaces. Traditional security approaches are no longer viable in a world where a simple configuration change can inadvertently expose assets to potential threats and where new cloud assets are created on a whim. Continuous monitoring is essential for organizations to stay ahead of these risks.

Cortex Xpanse research has shown that attackers can now scan the internet for vulnerable systems in under an hour, often beginning their scans mere minutes after the public disclosure of a critical vulnerability. Attack surface management must evolve to match this speed by providing a real-time, data-rich, and complete inventory of all internet-connected assets, adopting an external perspective. Beyond that, the true measure of an advanced ASM solution is its ability to facilitate swift and effective remediation.

Challenges of Relying on Traditional Asset Inventories

Traditional asset inventories fall short as they fail to capture unknown or third-party assets, leaving them unscanned and vulnerable. Discovering an unknown asset often triggers a laborious investigative process to determine its origin, ownership, and associated risks, which significantly delays remediation efforts.

With its agentless and automated approach, Cortex Xpanse® continuously discovers, evaluates, and aids in the mitigation of attack surface risks. It scans the entire IPv4 space to identify assets requiring attention, such as those with insecure remote access, exposed databases, or other vulnerabilities. Upon detecting an unknown asset, Xpanse promptly notifies the relevant team or individual tasked with its security or immediately performs remediation tasks to remove the risk.

The Imperative of Proactive Remediation

The Cortex Xpanse ASM module streamlines the remediation process with capabilities that eliminate the cumbersome manual effort traditionally involved in vulnerability management. By employing AI-driven playbooks, organizations can swiftly identify the asset's owner and context, significantly reducing the mean time to remediate (MTTR) and effectively transitioning from detection to securing systems. This cutting-edge approach moves beyond the reactionary scramble that follows the disclosure of every new zero-day threat.

For risks that still require human response, Xpanse provides advanced assessment capabilities and adaptive risk scoring so that organizations can instantly prioritize critical issues using dynamic scores that adapt to the evolving threat landscape.

Advantages of Intelligent Prioritization and Remediation

The innovation brought by Xpanse impacts security operations profoundly, where the discovery of exposures is not only automated but also intelligently prioritized in real time. Remediation is initiated with precision and efficiency, delivering a suite of benefits:

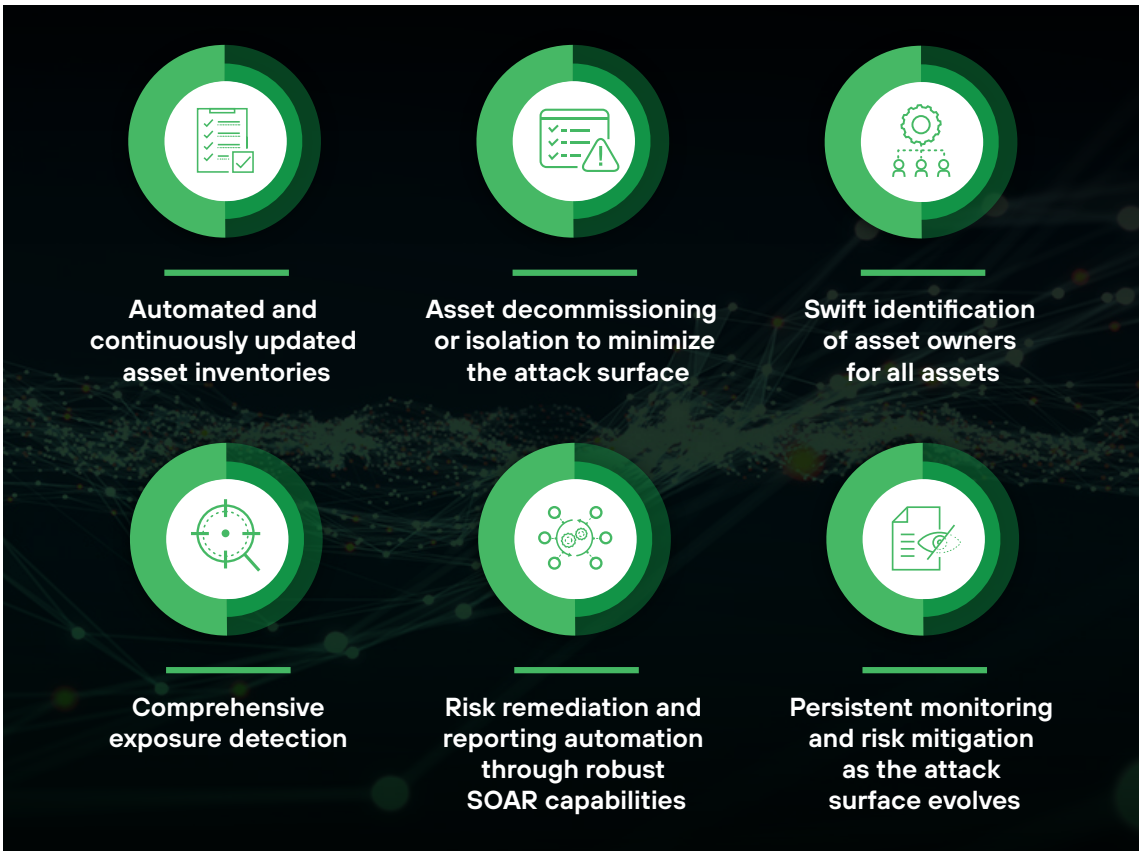
- **Continuous inventory**: Cortex Xpanse maintains a comprehensive and up-to-date inventory of all internet-connected assets, including IP addresses, domains, certificates, cloud, and physical infrastructure.
- **Dynamic scoring**: The solution adapts its scoring of exposures based on threat intelligence, enabling teams to address the most pressing risks first.
- **AI-powered remediation**: Automating the identification of asset owners and contextual information drastically cuts down the manual labor involved in vulnerability management.

Proactive Security with Cortex Xpanse

Cortex Xpanse helps transform the security operations center (SOC) from a reactive to a proactive stance. By minimizing the reliance on manual processes and promoting proactive risk management, it not only increases efficiency but also significantly reduces the costs associated with cyberthreats, such as ransomware and data breaches.

Conclusion: The Future of ASM with Xpanse

Modern attack surfaces require a modern solution. Cortex Xpanse delivers an automated, all-encompassing attack surface management platform that includes:



In addition to these core features, Cortex Xpanse offers customizable alert configurations, seamless operationalization through two-way API integrations, and enhanced asset insights through data correlation—all powered by automation capabilities in Cortex XSOAR® and the agility to rapidly adapt to the latest cybersecurity developments.

Organizations that are ready to take control of their attack surfaces in the cloud era can trust Cortex Xpanse to provide a complete, accurate, and continuously secured overview of their global internet-facing assets. Discover the definitive source of truth for your security operations and redefine your approach to attack surface management with Cortex Xpanse.

To understand how Cortex Xpanse can transform your cybersecurity posture, request a demo and witness the power of proactive attack surface management in action.

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_cisos-guide-to-attack-surface-management_060424