Palo Alto Networks Xpanse Active Attack Surface Management Automatically Remediates Cyber Risks Before They Lead to Cyberattacks

December 12, 2022

New Cortex Xpanse features give organizations complete visibility and effortless control of their attack surfaces to discover, evaluate and address cyber risks

SANTA CLARA, Calif., Dec. 12, 2022 /PRNewswire/ -- Cyberattackers today use highly automated methods to quickly find and exploit weaknesses in target organizations — sometimes within minutes of a new vulnerability being disclosed. Most security teams try to find these weaknesses, but because they are doing this with manual tools they quickly fall behind. Palo Alto Networks (NASDAQ: PANW), the global cybersecurity leader, introduced a new Cortex® capability: Xpanse Active Attack Surface Management, or Xpanse Active ASM. This helps security teams not just actively find but also proactively fix their known and unknown internet-connected risks. Xpanse Active ASM equips organizations with automation to give them the edge over attackers.

"While the fundamental need for attack surface management hasn't changed, the threat landscape today is much different. Organizations need an active defense system that operates faster than attackers can," said Matt Kraning, chief technology officer of Cortex for Palo Alto Networks. "As the leader and pioneer in the ASM market, we realize that customers need complete, accurate, and timely discovery and remediation of risky exposures in their internet-connected systems. With Xpanse Active ASM, we give defenders the ability not only to see their exposures instantly but also to shut them down automatically with no human labor required."

Available today, Xpanse Active ASM gives organizations the following tools and capabilities:

- **Active Discovery**: Attackers use frequent, automated probes to find vulnerable and/or exposed assets, and organizations need tools that allow them to have the same visibility. Active Discovery refreshes its internet-scale database several times a day and uses supervised machine learning to accurately map these vulnerabilities back to an organization. This helps them get an outside-in view of their network — the same view attackers have.

- **Active Learning**: Xpanse continuously processes discovery data, mapping new systems to the people responsible for each system. Active Learning continuously analyzes and maps the streamed discovery data to understand and prioritize top risks in real time. As a result, customers can stay ahead of attackers by closing down the riskiest exposures quickly.

- **Active Response**: While instant discovery of vulnerabilities and/or exposures can give security teams a realistic risk picture, merely finding issues isn't enough. Automated remediation is key to staying ahead of attackers, saving response time in the SOC by eliminating the manual step of merely creating a ticket for analysts who then must spend multiple hours of manual effort actually tracking down the owner of the affected system and resolving the vulnerability. True automation is completely solving the end-to-end remediation process without human intervention. A critical new capability for security teams, Active Response includes native embedded automatic remediation capabilities that make use of active discovery data and active learning analysis to automatically shut down exposures before they allow threats into a network. It executes ASM-specific playbooks to triage, deactivate and repair vulnerabilities automatically.

  The Xpanse Active Response module includes built-in end-to-end remediation playbooks. These playbooks automatically eliminate critical risks such as exposed Remote Desktop Protocol (RDP) servers and insecure OpenSSH instances without any manual labor.

  Following remediation, Active Response automatically validates that remediation was successful by scanning assets, compiling audited actions and placing investigation details into clear dashboards and reports.

Cortex Xpanse is used today by some of the most complex and demanding organizations in the world. Palo Alto Networks recently announced a multiyear deal for Cortex Xpanse to equip the Department of Defense with Internet Operations Management capabilities.

Availability
Cortex Xpanse Active ASM is now available globally with full support.

Additional Resources

- Learn more about Xpanse Active ASM.
- Register for the Xpanse Active ASM online event.
- Follow Palo Alto Networks on Twitter, LinkedIn, Facebook and Instagram.

About Palo Alto Networks
Palo Alto Networks is the world's cybersecurity leader. We innovate to outpace cyberthreats, so organizations can embrace technology with confidence. We provide next-gen cybersecurity to thousands of customers globally, across all sectors. Our best-in-class cybersecurity platforms and services are backed by industry-leading threat intelligence and strengthened by state-of-the-art automation. Whether deploying our products to enable the Zero Trust Enterprise, responding to a security incident, or partnering to deliver better security outcomes through a world-class partner ecosystem, we're committed to helping ensure each day is safer than the one before. It's what makes us the cybersecurity partner of choice.

At Palo Alto Networks, we're committed to bringing together the very best people in service of our mission, so we're also proud to be the cybersecurity workplace of choice, recognized among Newsweek's Most Loved Workplaces (2021), Comparably Best Companies for Diversity (2021), and HRC Best Places for LGBTQ Equality (2022). For more information, visit www.paloaltonetworks.com.

View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-xpanse-active-attack-surface-management-automatically-remediates-cyber-risks-before-they-lead-to-cyberattacks-301699989.html

SOURCE Palo Alto Networks, Inc.

mmanturi@paloaltonetworks.com