Palo Alto Networks Launches Cortex XDR for Cloud: XDR 3.0 Expands Industry-Leading Extended Detection and Response Platform to Cloud and Identity to Detect and Stop Cyberattacks

August 23, 2021

Third-generation XDR automates threat detection and investigation across endpoint, network, cloud and identity, from a single console

SANTA CLARA, Calif., Aug. 23, 2021 /PRNewswire/ -- Palo Alto Networks (NYSE: PANW) today announced Cortex® XDR™ 3.0, expanding its pioneering extended detection and response (XDR) solution to cloud- and identity-based threats to give organizations the holistic analytics needed to protect against increasingly sophisticated cyberattacks.



The third generation of Cortex XDR — already delivering top performance in the MITRE ATT&CK® evaluation — now offers security operations center (SOC) teams even broader protections across their attack surface. By extending detection, monitoring and investigation into cloud environments, and detecting malicious user activities and insider threats through analysis of identity data, SOC teams benefit from security analytics across endpoint, network, cloud and identity for organization-wide detection and response — critical in an era of increasingly interrelated attacks.

In addition, Cortex XDR 3.0 offers security teams forensic investigation features based on the advanced proprietary tools of Palo Alto Networks' world-class Unit 42 Security Consulting group, and supports ingestion and custom correlations for virtually all third-party data sources.

"Palo Alto Networks created the extended detection and response (XDR) category in 2019 — understanding that only by integrating data from across all security sources can we detect complex threats accurately, prevent attacks automatically, and investigate them much faster. We've been innovating against that mission ever since," said Tim Junio, senior vice president of products, Cortex at Palo Alto Networks. "With our third-generation XDR solution expanding to cloud and identity analytics, Cortex XDR 3.0 has taken a large step towards being the most comprehensive platform for the SOC to protect endpoints, entities, assets, workloads, and critical data."

Cortex XDR has delivered top performance for three years running in the MITRE ATT&CK evaluation and achieved the highest overall combined detection and protection rate. As cybersecurity threat actors get faster, more organized and more sophisticated in their tactics, techniques and procedures, the new features of Cortex XDR 3.0 prepare SOC teams to know and stop attacks:

- **Cortex XDR for cloud** allows SOC teams to extend detection, monitoring and investigation into cloud environments. XDR 3.0 brings together and integrates cloud host data, traffic logs, audit logs, data from Palo Alto Networks' industry-leading Prisma® Cloud product, and third-party cloud security data with non-cloud endpoint and network data sources. This provides the best coverage for SOC teams to span on-premises and multicloud environments.
- **Cortex XDR Identity Analytics** further enhances the user behavior analytics capabilities of XDR to detect malicious activities and insider threats by collecting and analyzing an extensive set of identity data.
- **Cortex XDR Forensics** module delivers the advanced forensic investigation tool used by the Palo Alto Networks Unit 42 Security Consulting group directly to Cortex XDR customers. The XDR Forensics module provides the ability to gather historical evidence such as user, file, application, browser and other activities from compromised systems to bring the full analytic potential of XDR to bear during incident response.
- **Cortex XDR Incident Management Interface** provides security analysts with a comprehensive story of an incident in one place, including related malicious artifacts, hosts, users and correlated alerts mapped to the MITRE ATT&CK framework. This helps analysts handle incidents more quickly and completely.
- **Cortex XDR Third-Party Data Engine** offers customers the ability to ingest, normalize, correlate, query and analyze data from virtually any source. This third-party data can be correlated with threat activity and tagged with MITRE ATT&CK tactics, techniques and procedures to help provide a more detailed picture of adversarial movement. This also allows SOC teams to understand the full scope of an incident and respond more completely.

More Information

More information on Cortex XDR 3.0 is available here and in our blog, or learn more at our events on September 14 and 15.

Availability

Cortex XDR 3.0 will become available globally over the next week.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For

more information, visit www.paloaltonetworks.com.

Palo Alto Networks, Cortex, Prisma, Unit 42 and the Palo Alto Networks logo are trademarks of Palo Alto Networks, Inc. in the United States and in jurisdictions throughout the world. All other trademarks, trade names, or service marks used or mentioned herein belong to their respective owners.



View original content to download multimedia:https://www.prnewswire.com/news-releases/palo-alto-networks-launches-cortex-xdr-for-cloud-xdr-3-0-expands-industry-leading-extended-detection-and-response-platform-to-cloud-and-identity-to-detect-and-stop-cyberattacks-301360315.html

SOURCE Palo Alto Networks, Inc.