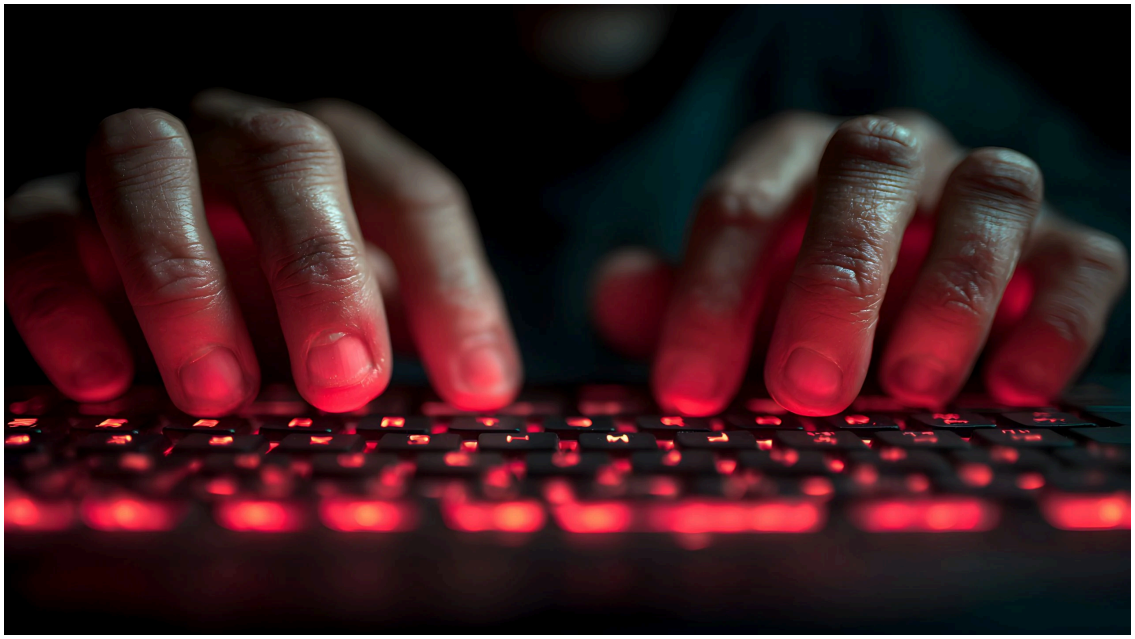
Cloud Security - Palo Alto Networks Blog

By Mar 24, 2026 By Asaf Henig and Cameron Hyde

Archived: 2026-04-05 13:11:31 UTC



When Security Scanners Become the Weapon: Breaking Down the Trivy Supply Chain Attack

The Trivy Supply Chain Attack shows how security tools can be weaponized. Learn how this 2026 breach unfolded and how Cortex Cloud blocks the threat.

AppSec

Cloud Security

Threat Prevention

Unit 42

Vulnerability Exposed

Mar 24, 2026

By Asaf Henig and Cameron Hyde

Cloud Security

Application Security

Cloud Posture Security

Cloud Runtime Security

AI Security Posture Management

Cloud Native Application Protection Platform

Announcement, Cloud Native Application Protection Platform, Cloud Security, CNAPP, Reports

Where Cloud Security Stands Today and Where AI Breaks It

Cloud security trends reveal where teams gain ground and fragmentation breaks defense. Explore insights from 2,800 leaders and how cloud, identity and AI risks converge.

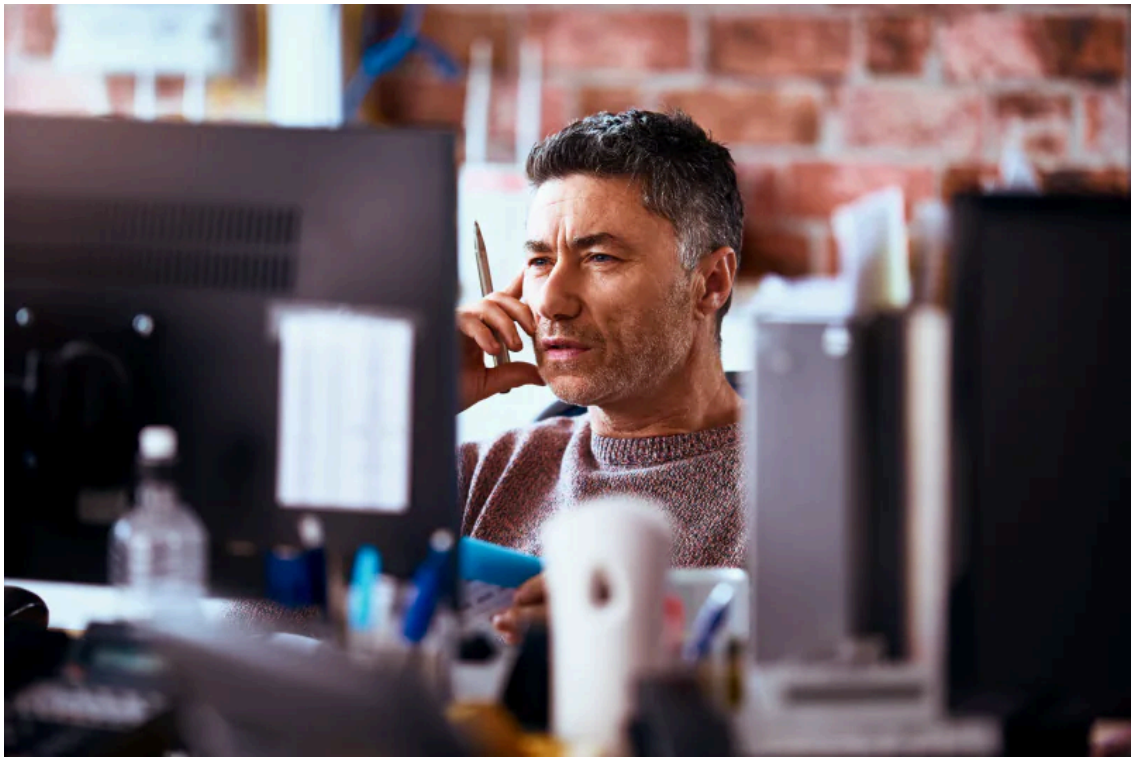
Dec 16, 2025

By Cody Queen

Application Security, AppSec, ASPM, Cloud Security, DevSecOps

Mar 12, 2026

By Cameron Hyde



Cloud Infrastructure Entitlement Management, Cloud Security, IAM, Identity Security

Cortex Cloud Named Leader and Outperformer in the 2026 GigaOm Radar for CIE...

Cloud infrastructure entitlement management is foundational to CNAPP. See why Cortex Cloud was named a Leader in the 2026 GigaOm CIEM Radar.

Mar 05, 2026

By David Trigano and Andrea Halsted

ASPM, Cloud Runtime Security, Cloud Security, CNAPP, Containers

Container Security: A Layer-by-Layer Guide for Security Engineers

Container security demands more than shift left. Learn how to build defense in depth across IDE, CI, registry, admission control and runtime without a...

Mar 03, 2026

By Bruno Almeida and Avishai Moshka

More Blogs

Displaying 1—16 of

481 results

Sort By:

Announcement, Cloud Security, Cloud Security Platform, CNAPP, Code to Cloud to SOC

Why the Future of Cloud Security Is Agentic

Agentic cloud security marks the shift from dashboards to autonomous action. Learn why AI agents are redefining cloud defense and closing the speed gap.

Feb 25, 2026

By Jonathan Bregman

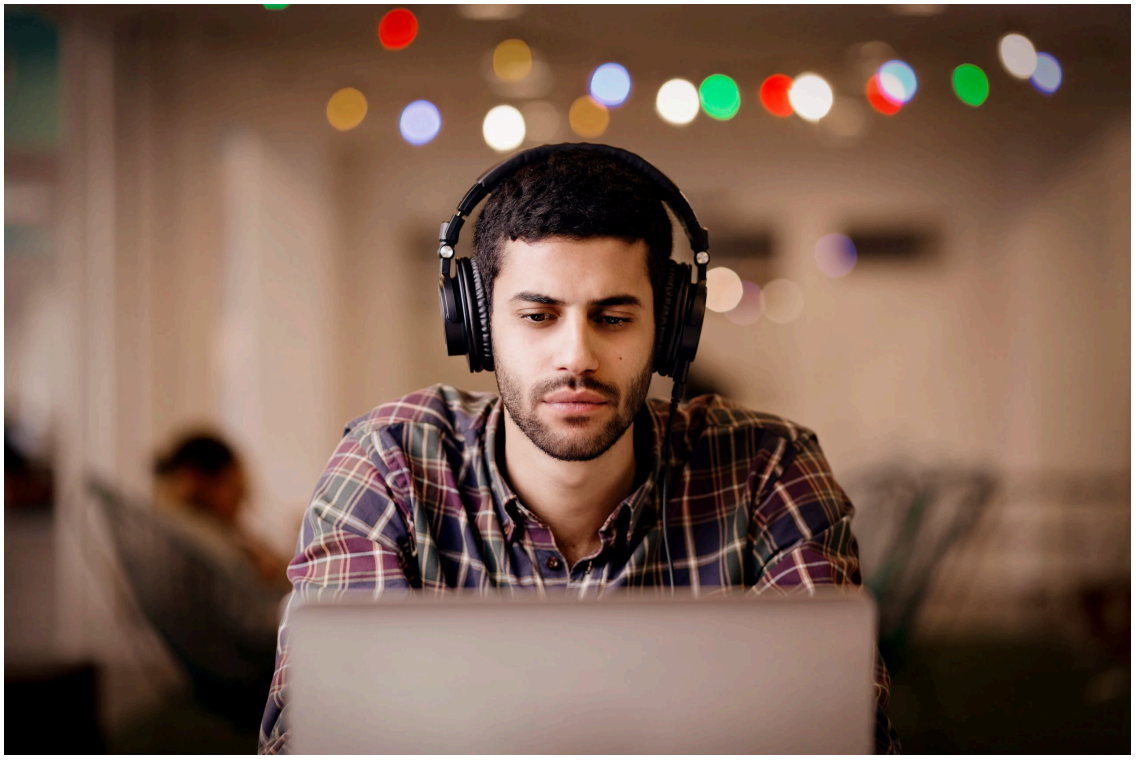
Announcement, Cloud Security, Cloud Security Platform, CNAPP

Closing the Gap Between Cloud Visibility and Network Security

Cloud visibility improves risk prioritization by adding network security context, revealing protected paths, reducing false positives, and focusing te...

Feb 17, 2026

By Alexandre Cezar and Mohit Bhasin



AppSec, ASPM, Cloud Security, Code Security, DevSecOps, Research

An Inside Look into ASPM: Five Findings from New Industry Research

ASPM is emerging as the orchestration layer for AppSec. Explore key findings in new research from Omdia on risk reduction, automation, and tool conver...

Feb 09, 2026

By Cameron Hyde

Application Security, AppSec, ASPM, Cloud Security, Partners

Palo Alto Networks and Veracode: Unifying Application Security from Code to...

Secure your software supply chain with the Cortex Cloud and Veracode integration. Correlate code vulnerabilities with cloud context to prioritize and ...

Jan 20, 2026

By Cameron Hyde

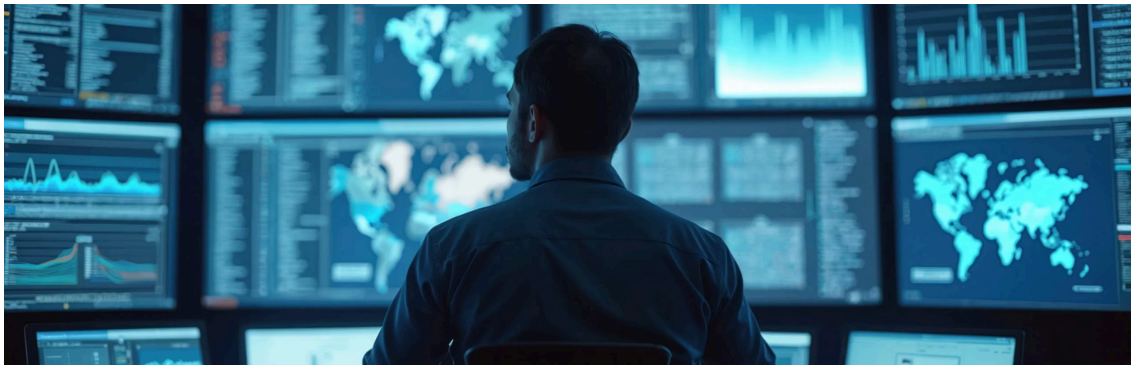
AI Security, AI-SPM, CIEM, Cloud Security, DSPM, Identity Security

Is AI a New Challenge for Cloud Security? Yes and No.

AI security challenges are accelerating as models and agents reshape cloud risk. Learn where traditional controls break down and how to close the AI security gap.

Jan 15, 2026

By Sharon Farber



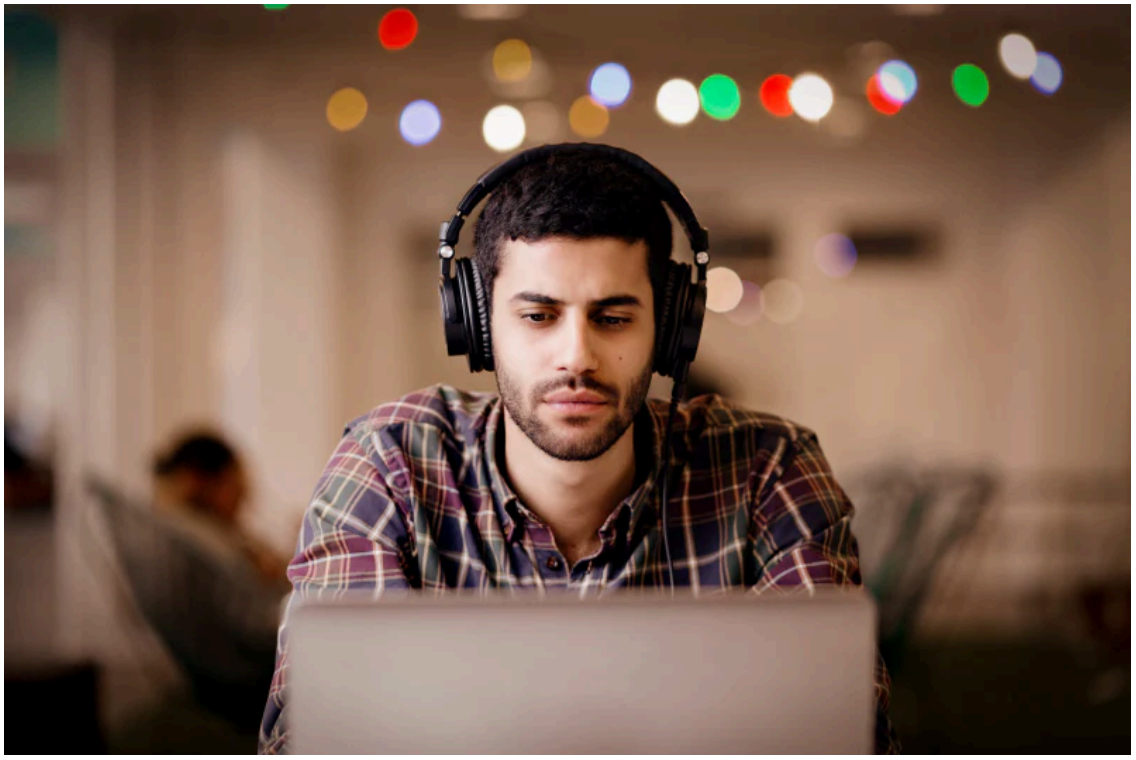
AppSec, ASPM, Cloud Security, CNAPP, Code to Cloud to SOC

AI-Powered Cloud Security That Sees Everything and Fixes It Faster

AI-powered cloud security unifies posture, runtime and AppSec with autonomous investigation, guardrails and real-time protection to reduce risk faster...

Jan 06, 2026

By Cody Queen



AI Security, Cloud Security, Cloud Workload Protection

Understanding API Risk in the Age of AI

API security now sits at the center of AI risk. Learn how AI-driven traffic expands exposure and how Cortex Cloud delivers discovery, prioritization and real-time protection.

Dec 18, 2025

By Andrea Halsted and Amit Biton

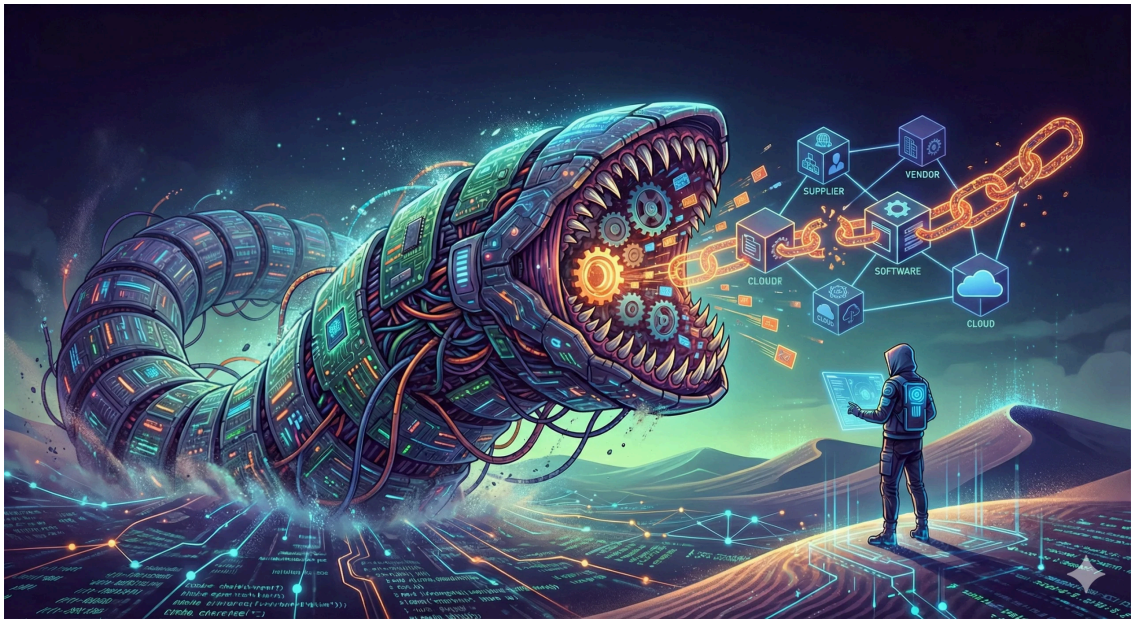
AI Security, Cloud Security

OWASP Top 10 for Agentic Applications 2026 Is Here – Why It Matters and How...

Agentic AI introduces new risks across tools, identities, supply chains and memory. Learn what the OWASP Top 10 for Agentic AI means and how to secure autonomous systems.

Dec 10, 2025

By Jaimin Patel and Elad Koren



AppSec, Cloud Detection and Response, Cloud Runtime Security, Cloud Security, Supply Chain Security

Shai-Hulud 2.0: How Cortex Helps Protect Against the Resurgent npm Worm

Shai-Hulud 2.0 exposes the fragility of software supply chains. Learn how the npm worm spreads through developer ecosyst...

Nov 26, 2025

By Cameron Hyde and Yitzy Tannenbaum

CIEM, Cloud Security, IAM, Identity Security, KSPM

Turning Kubernetes Last Access to Kubernetes Least Access Using KIEMPossibl...

Kubernetes identity security demands clarity. Learn how KIEMPossible uncovers entities, permissions and usage to help you reduce identity attack surfa...

Nov 25, 2025

By Golan Myers

Data Security, Data Security Posture Management

Is Your Snowflake Data at Risk? Find and Protect Sensitive Data with DSPM

Cloud data security is critical. Learn how Snowflake users can mitigate risks with effective data security posture management (DSPM) and enhanced secu...

Nov 21, 2025

By Sharon Farber

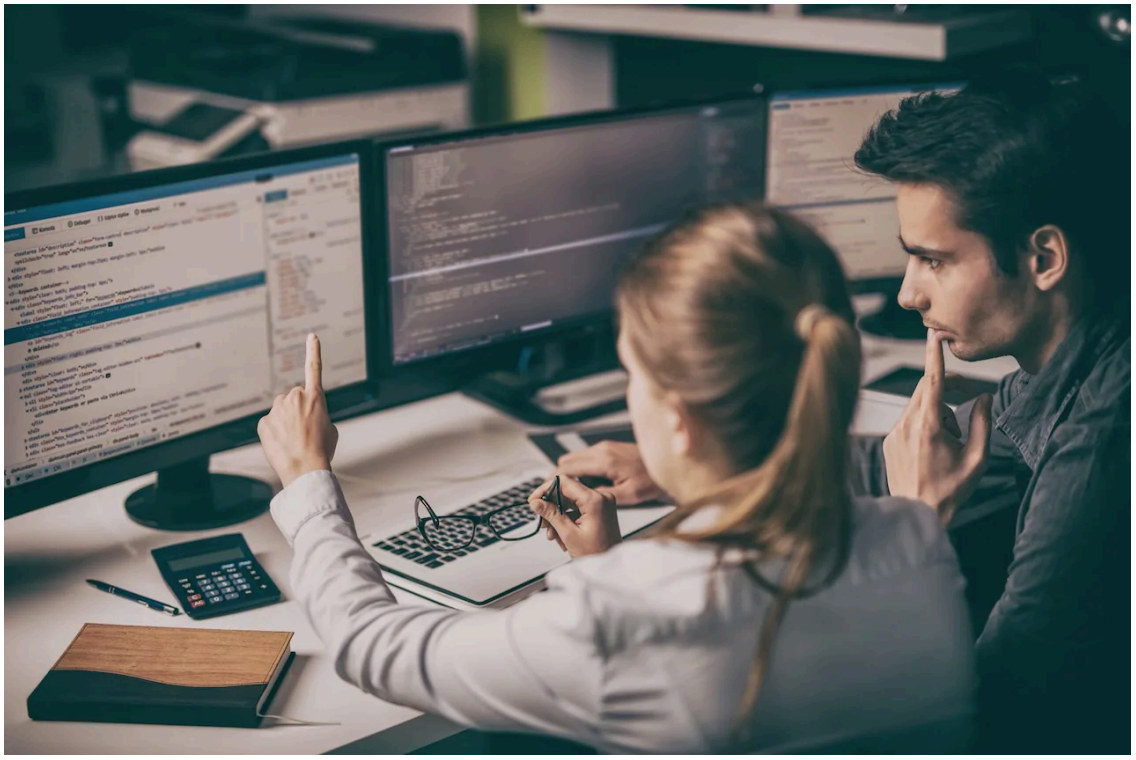
AI Security, AI-SPM, Cloud Security

Explore the OWASP Top 10 for LLMs: A New Interactive Guide

AI security starts with the OWASP Top 10 for LLMs. Explore our interactive guide to uncover and mitigate the biggest risks across your AI pipelines.

Nov 20, 2025

By Sharon Farber



CIEM, Cloud Security, DSPM, IAM

All Paths Lead to Your Cloud: A Mapping of Initial Access Vectors to Your A...

Initial-access risks in AWS demand clarity. Uncover how service exposure and access-by-design flaws open cloud perimeters and learn how to secure them...

Nov 18, 2025

By Golan Myers and Ofir Balassiano

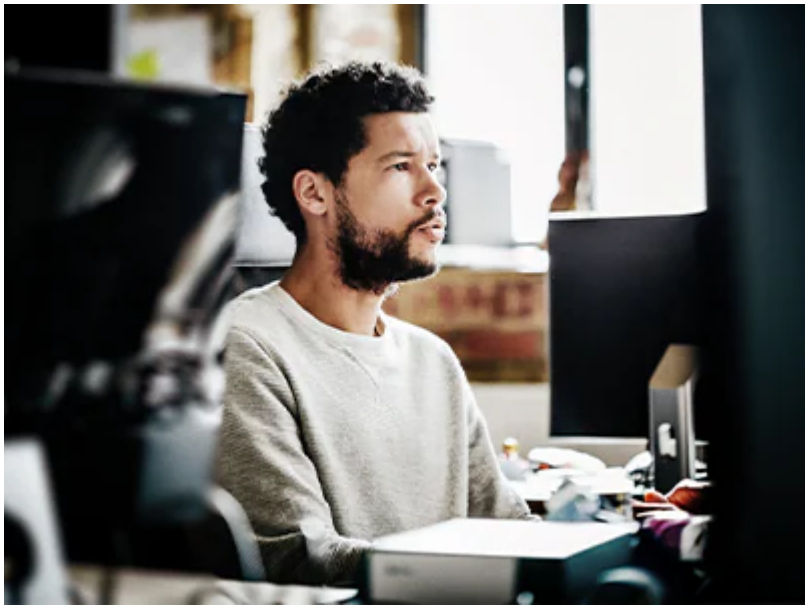
Cloud Runtime Security, Cloud Security, Cloud Workload Protection, CWPP

Agentless Vs. Agent-Based Scanning in Kubernetes: A Deep Dive

Kubernetes security depends on smart scanning. Compare agentless and agent-based approaches to find the right balance between coverage and runtime def...

Nov 13, 2025

By Bruno Almeida



CIEM, Cloud Security, IAM

Regaining Control Over Identity and Access

Cloud permissions outpace control. Learn how CIEM restores visibility, enforces least privilege, and secures every identity in dynamic cloud environments.

Nov 12, 2025

By Shahar Livschitz

CDR, Cloud Detection and Response, Cloud Runtime Security, Cloud Security

Lessons Ted Lasso Can Teach You About CDR

Ted Lasso’s lessons inspire a smarter, faster, more collaborative approach to cloud detection and response. Learn to turn chaos into confidence.

Nov 11, 2025

By Mohit Bhasin and Emily Rodenhuis

Load more blogs

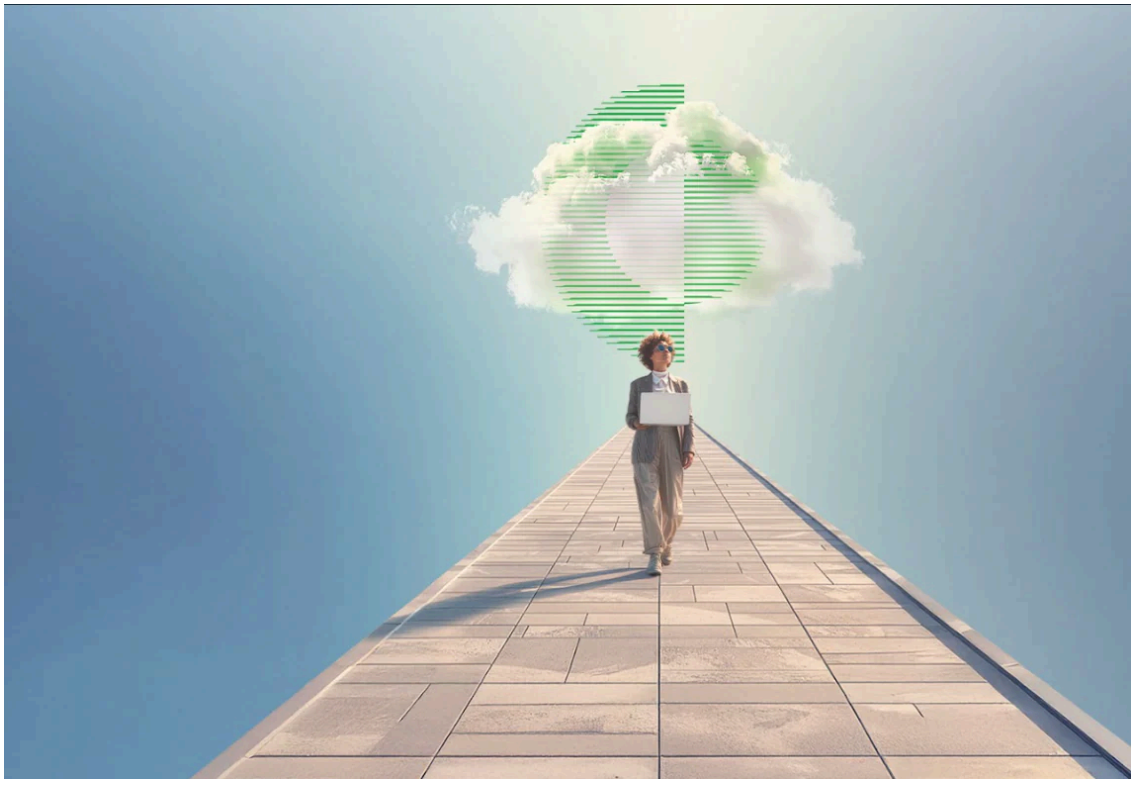
Load more blogs

More Blogs

Displaying 1—16 of

481 results

Sort By:



Announcement, Cloud Security, CNAPP, Code to Cloud to SOC

Introducing Cortex Cloud 2.0: Smarter Cloud Security for an AI-Driven World

Cortex Cloud 2.0 delivers unified protection from code to cloud to SOC, turning complexity into clarity with AI-driven prevention and response.

Oct 28, 2025

By Elad Koren

AppSec, ASPM, Cloud Security

Breakdown: Widespread npm Supply Chain Attack Puts Billions of Weekly Downl...

npm supply chain attack exposed billions of downloads to risk. Learn how malicious packages spread and how to prevent threats with Cortex Cloud.

Sep 10, 2025

By Asaf Henig and Cameron Hyde

AI Security, AI Security Posture Management, DSPM

Model Context Protocol (MCP): A Security Overview

Model Context Protocol (MCP) introduces new AI integration risks. Learn how to manage threats like prompt injection, credential leaks, and toolchain abuse.

Jun 06, 2025

By Sharon Farber

AI Security, Cloud Security

OWASP Top 10 for Agentic Applications 2026 Is Here – Why It Matters and How...

Agentic AI introduces new risks across tools, identities, supply chains and memory. Learn what the OWASP Top 10 for Agentic AI means and how to secure autonomous systems.

Dec 10, 2025

By Jaimin Patel and Elad Koren

Introducing Cortex Cloud ASPM

Cortex Cloud ASPM redefines application security with context-aware prevention, unified policy and runtime insight across the full software lifecycle.

Aug 05, 2025

By Cameron Hyde and Sarit Tager

Announcement, Application Security, Cloud Security, CNAPP, News and Events, Product Features, Products and Services

Introducing Cortex Cloud — The Future of Real-Time Cloud Security

Cortex Cloud brings the world's leading CNAPP onto the #1 SecOps platform, delivering real-time protection — for the fir...

Feb 13, 2025

By Elad Koren

AI Security Posture Management, Announcement, Data Security Posture Management

AI-SPM Now Generally Available: Enhancing AI Security and Compliance with P...

Learn how AI Security Posture Management (AI-SPM) addresses new cloud security challenges, including model risk, data exposure, and misuse in AI envir...

Aug 06, 2024

By Amol Mathur

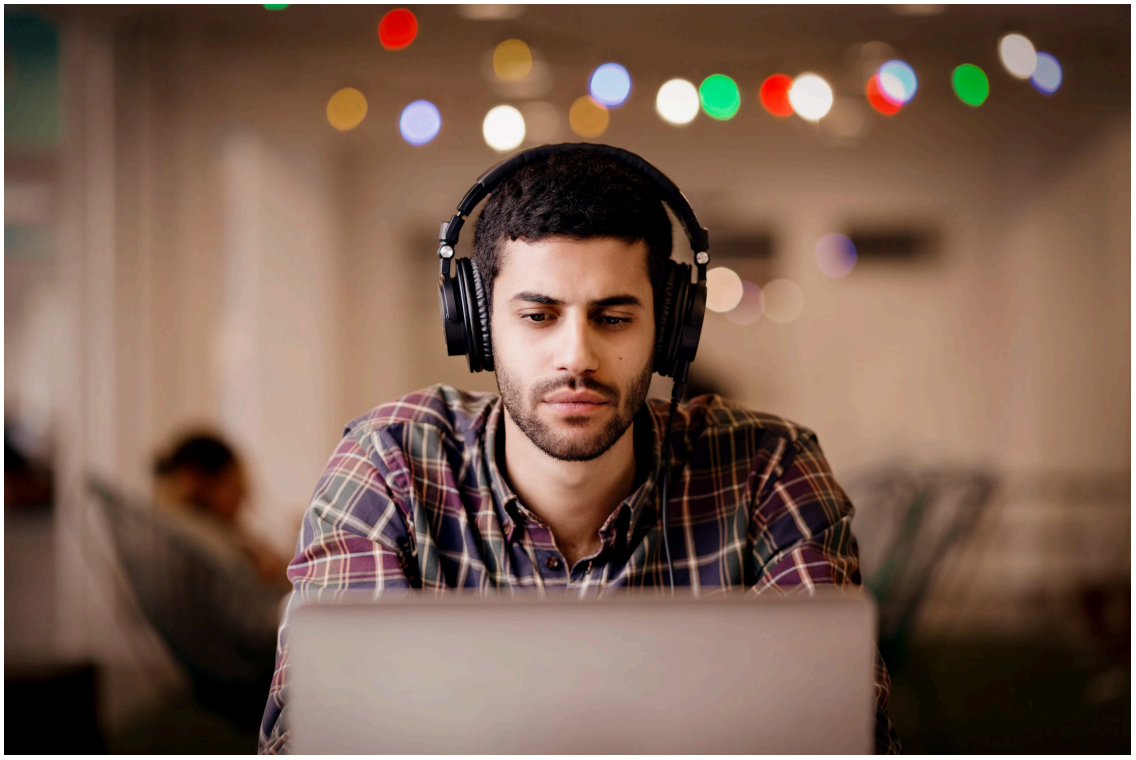
Announcement, Cloud Security, Cloud Security Platform, CNAPP, Code to Cloud to SOC

Why the Future of Cloud Security Is Agentic

Agentic cloud security marks the shift from dashboards to autonomous action. Learn why AI agents are redefining cloud defense and closing the speed gap.

Feb 25, 2026

By Jonathan Bregman



AppSec, ASPM, Cloud Security, Code Security, DevSecOps, Research

An Inside Look into ASPM: Five Findings from New Industry Research

ASPM is emerging as the orchestration layer for AppSec. Explore key findings in new research from Omdia on risk reduction, automation, and tool conver...

Feb 09, 2026

By Cameron Hyde

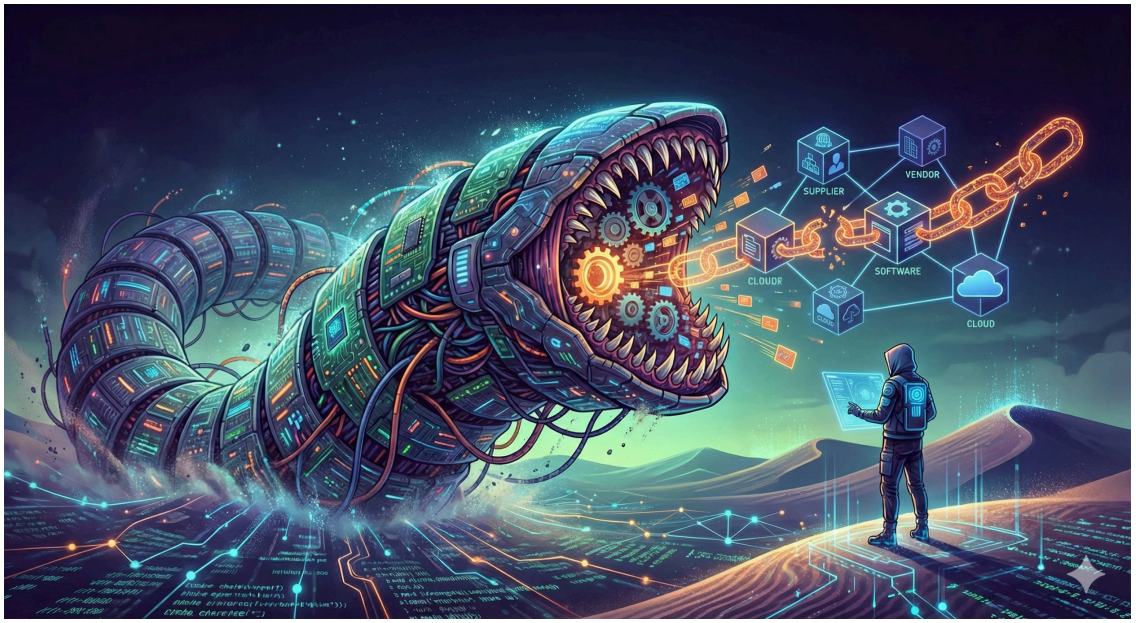
Application Security, AppSec, ASPM, Cloud Security, Partners

Palo Alto Networks and Veracode: Unifying Application Security from Code to...

Secure your software supply chain with the Cortex Cloud and Veracode integration. Correlate code vulnerabilities with cloud context to prioritize and ...

Jan 20, 2026

By Cameron Hyde



AppSec, Cloud Detection and Response, Cloud Runtime Security, Cloud Security, Supply Chain Security

Shai-Hulud 2.0: How Cortex Helps Protect Against the Resurgent npm Worm

Shai-Hulud 2.0 exposes the fragility of software supply chains. Learn how the npm worm spreads through developer ecosyst...

Nov 26, 2025

By Cameron Hyde and Yitzy Tannenbaum

Cloud Workload Protection Platform, DevSecOps

Announcing Checkov 2.0: Deepening Open Source IaC Security

Checkov 2.0 is a graph-based, open source IaC security tool for environments with complex dependencies across resources and modules.

Apr 08, 2021

By Matt Johnson

Announcement, Cloud Security, Cloud Security Platform, CNAPP

Closing the Gap Between Cloud Visibility and Network Security

Cloud visibility improves risk prioritization by adding network security context, revealing protected paths, reducing false positives, and focusing te...

Feb 17, 2026

By Alexandre Cezar and Mohit Bhasin

Cloud Workload Protection, Cloud Workload Protection Platform

Agentless vs. Agent-Based Security: How to Use Them to Stay Secure

The cloud computing industry will see a staggering compound annual growth rate of over 15% through 2028 when its market cap is expected to exceed $1 T...

Feb 09, 2023

By Aqsa Taylor

Cloud Native Application Protection Platform, CNAPP

Code to Cloud Vulnerability Management

Innovative vulnerability management dashboard streamlines discovery, prioritization and remediation of vulns, ensuring robust security from code to cloud.

Oct 26, 2023

By Alon Ben Porath and Alexandre Cezar

Platform, Research, Threat Research

Understanding Three Real Threats of Generative AI

Understand the real threats generative AI poses to your organization, including KYC verification bypass and image generators, deepface generation, and malicious LLMs.

May 23, 2024

By Kyle Wilhoit

Load more blogs

Load more blogs
