Connect Tamnoon with Cortex

Transform CNAPP Alerts to Targeted Remediation Tasks

The Challenge

Organizations often cannot optimally staff and operationalize their security tools due to budget or skill gaps. To bridge these gaps, organizations need adaptable solutions they can customize to their specific architecture and business priorities, ensuring the remediation effectively addresses critical infrastructure.

Our Integrated Solution

With Cortex Cloud and Tamnoon, security teams can rely on the trusted security capabilities of Palo Alto Networks combined with the modern managed detection and response (MDR) approach Tamnoon delivers.

Organizations can confidently address their most critical cloud vulnerabilities by combining the visibility that cloud-native application protection platforms (CNAPPs) provide with context-rich alerts and expert-guided remediation. This further enhances the CNAPP's powerful detection capabilities, surfacing risks across multicloud environments while ensuring these alerts are prioritized and resolved with precision.

Managed cloud remediation enables companies to bridge the gap between detection and action while enabling security and engineering teams to collaborate effectively in any environment. Contextual insights and developer-friendly playbooks further support these initiatives, empowering teams to focus on critical risks without disrupting production environments.

Tamnoon Managed Cloud Remediation

Tamnoon combines real-time cloud security with AI-powered technology and context from a cloud professional to prioritize and contextualize CNAPP alerts at scale—transforming remediation planning and execution within an organization.

The Tamnoon service offloads alert triaging and prioritization, saving security and engineering teams countless hours every week while enabling organizations on the journey to zero critical alerts. Organizations overcome alert fatigue by ensuring every alert is enriched with context, deduplicated, and prioritized.

This service also simplifies remediation planning with AI-driven automation and human cloud security experts who show the root cause of an alert, complete with detailed impact analysis and tailored remediation playbooks. With Tamnoon, recommendations are turned into verified engineering tasks without impacting production to help ensure

Palo Alto Networks Cortex Cloud

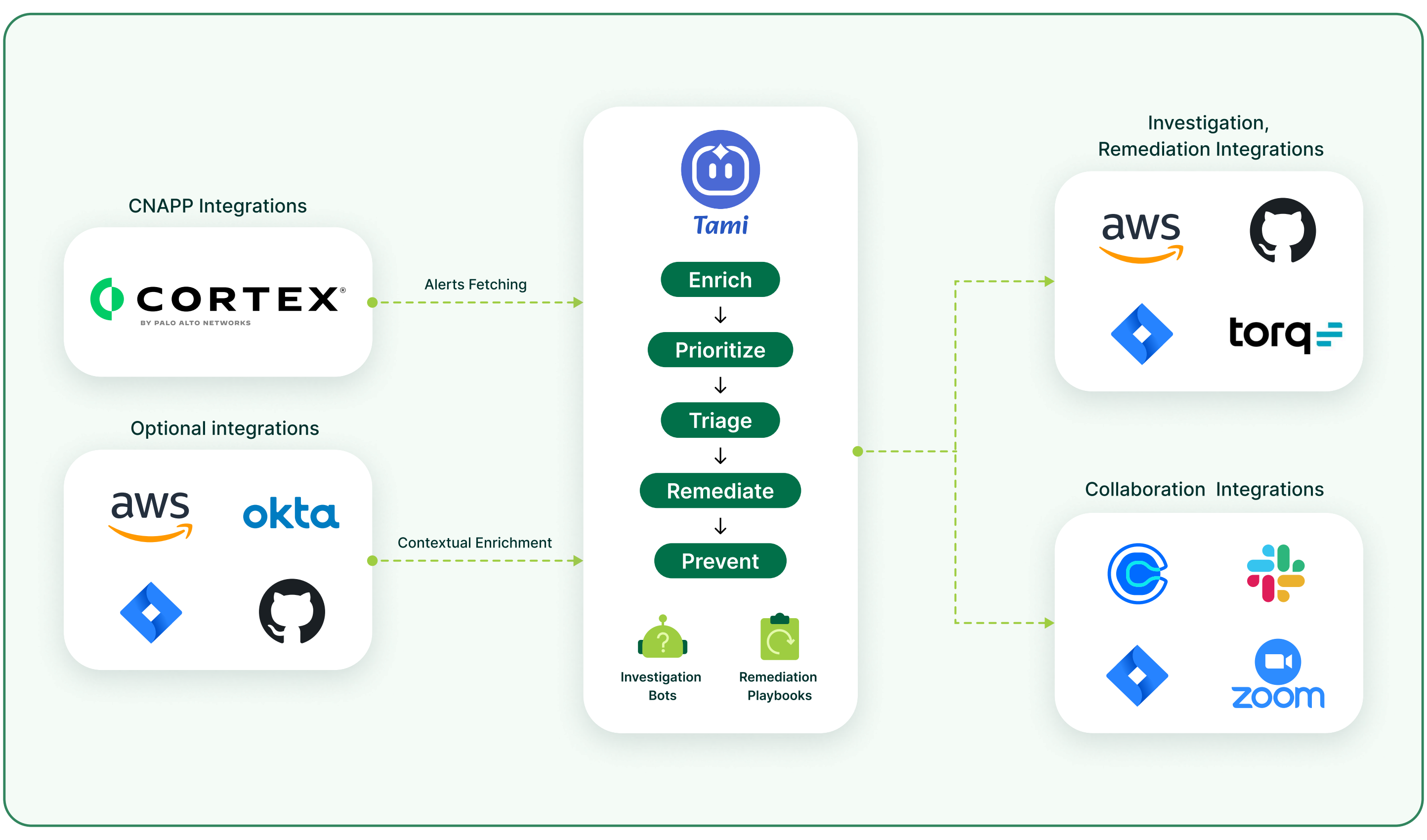
Cortex Cloud, the next-generation Prisma® Cloud, unifies cloud detection and response (CDR) with leading CNAPP for real-time security. It integrates with engineering ecosystems to prevent risks and secure apps by design. By combining AppSec tools with full code and runtime context, it helps prevent and prioritize risks. Cortex Cloud enhances multicloud risk management with AI-driven prioritization, guided fixes, and automated remediation. It correlates risks—misconfigurations, vulnerabilities, IAM issues, and data exposures—to identify attack paths. AI-powered Action Plans group related risks, enabling scalable remediation.

Cortex Cloud also stops known and unknown threats in real time across VMs, containers, Kubernetes, and serverless environments. A single agent provides unified runtime security, enabling proactive defense across cloud workloads.

Palo Alto + Tamnoon Managed Cloud Remediation

Tamnoon integrates seamlessly with Palo Alto Networks Cortex Cloud, combining posture management with the context, expert remediation advice, and proactive protection against cloud vulnerabilities that Tamnoon provides. The Cortex Cloud security posture provides teams with immediate visibility into all workloads and cloud services, identifying vulnerabilities and misconfigurations across cloud environments.

The cloud security experts and AI from Tamnoon enhance Cortex Cloud insights with context—resource type, environment, exposure, encryption, criticality, and ownership— helping teams prioritize and remediate the most critical misconfigurations and risks first. Tamnoon offers simple, easy-to-follow remediation advice and playbooks to block major, recurring misconfigurations from happening again. This hybrid approach bridges the gap between detection and action, enabling teams to prioritize and remediate cloud security risks efficiently and effectively.



Use Cases

Prioritizing Exposed Sensitive Blob Storage

CHALLENGE

Organizations often struggle to manage the flood of alerts that misconfigured storage buckets generate when these alerts lack context. Even after identifying a potentially exposed AWS S3 bucket, security teams lack clarity on the bucket's true level of risk. Without clear prioritization or actionable steps, critical misconfigurations can go unnoticed, prolonging exposure and increasing the likelihood of data breaches or compliance violations.

SOLUTION

Cortex Cloud identifies misconfigured AWS S3 buckets, generating alerts to highlight potential risks. It automatically prioritizes resources identified as high risk. Tamnoon then increases the severity level of the most at-risk storage buckets. Next, our team researches and analyzes the potential impact, suggests concrete remediation guidance, and provides tailored playbooks to the development team, helping ensure a swift and effective remediation.

About Tamnoon

Tamnoon finishes what CNAPPs start. Our platform delivers battle-tested remediation at machine speed, safely resolving vulnerabilities and misconfigurations while dramatically reducing friction between cloud security and development teams.

About Palo Alto Networks Cortex Cloud

As the global cybersecurity leader, Palo Alto Networks (NASDAQ: PANW) is dedicated to protecting our digital way of life via continuous innovation. Trusted by more than 70,000 organizations worldwide, we provide comprehensive AIpowered security solutions across network, cloud, security operations and AI, enhanced by the expertise and threat intelligence of Unit 42®. Our focus on platformization allows enterprises to streamline security at scale, ensuring protection fuels innovation. Discover more at www.paloaltonetworks.com.

tamnoon

Cloud SecOps that Feels Like Magic

tamnoon.io