Solution Brief July 2025

Okta and Palo Alto Networks Cortex XDR

Eliminate user-based attacks.

Advanced attackers can infiltrate the most well-protected organizations, steal credentials, and move laterally undetected, increasing the risk of a costly attack. Okta and Palo Alto Networks have partnered to help your security analysts quickly get in front of threats as they emerge. The integration of Okta Workforce Identity and Cortex XDR allows your team to rapidly surface, prioritize, investigate, and respond to stealthy threats, including targeted attacks, insider abuse, and risky user behavior.

Cortex XDR

Cortex XDR is the industry's first extended detection and response platform that integrates endpoint, network, and cloud data to stop sophisticated attacks. With Cortex XDR, you can accurately detect threats with AI-driven analytics and cut investigation time by 88% with root cause analysis. Together with best-in-class endpoint protection, Cortex XDR provides comprehensive protection to keep your organization safe.

Okta

Okta Workforce Identity makes it easy for organizations to securely connect their users with the resources they need to do their jobs. Okta centralizes access to SaaS apps, web access management (WAM) systems and custom web apps, APIs, and infrastructure.
With one set of credentials, users can access all of the resources they need to be productive, wherever and on whatever device they choose. Administrators can assign resources relevant to a user's role as well as set access policies based on role, the resource the user is trying to access, and more. You can prompt for a second factor based on risk signals from the device, network, geography, and more. Finally, Okta can centralize user stores from on-premises systems like Active Directory® or LDAP, as well as HR systems like Workday®, and automate on/offboarding of applications, saving administrators time and reducing the risk of misconfigurations.

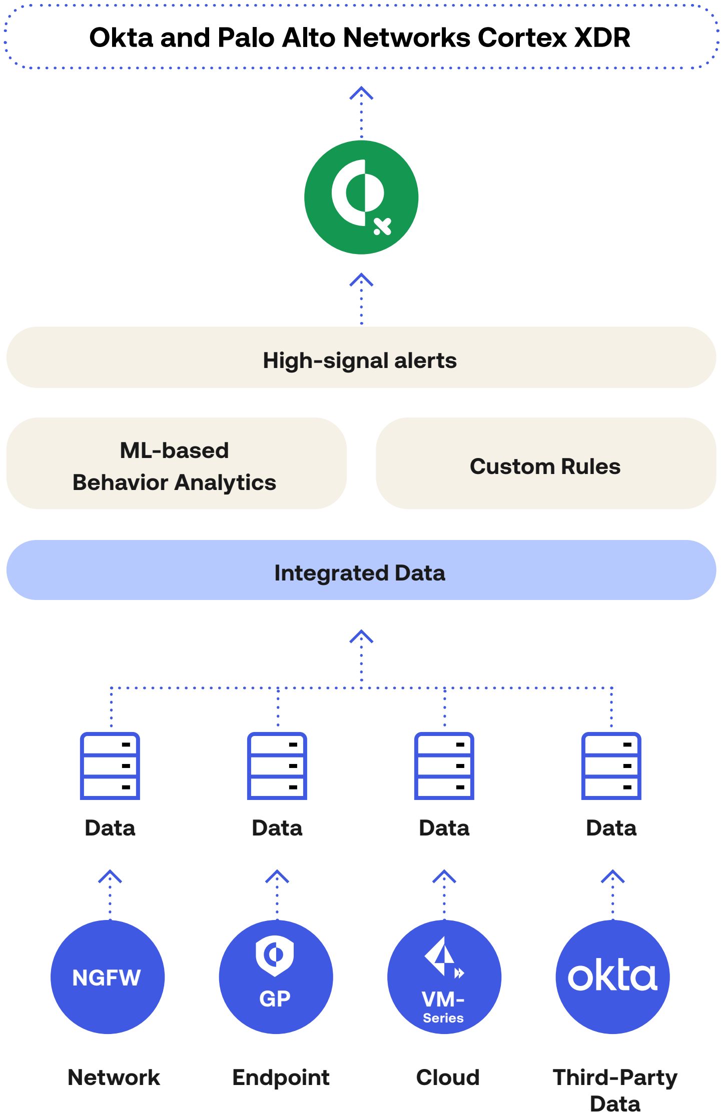
The Challenge: Keeping Up with the Speed of Threats

Security teams must adapt quickly to match the pace of threat actors and rapidly evolving enterprise ecosystems. Safely enabling remote work has suddenly become mandatory for many businesses, and they're trying to provide new tools and simplify collaboration to keep newly remote teams productive. But for enterprise security teams, millions of people using their own devices to log in to sanctioned and unsanctioned cloud and on-premises apps and data stores dramatically increases the threat level.

Meanwhile, as enterprises are suddenly forced to fully embrace cloud-based systems and "any device, anywhere" operations, IT teams are being run ragged. They have to onboard and maintain an explosion of new applications, services and platforms, and somehow find new efficiencies as well. In many cases, these teams have reduced staff and are tasked with doing more with less, or manage a variety of disparate tools that don't integrate well. Security concerns can become an unfortunate casualty...even as modern attackers increasingly target people instead of more easily-protected infrastructure, forcing security teams to scramble to spot, prioritize, and respond to threats.

Solving this unique, fast-unfolding challenge involves two basic principles. First, you have to build your strategy around identity-based security. In modern cloud and hybrid enterprise workspaces, no other solution is flexible enough or secure enough to power complex, remote teams and keep them collaborating productively and safely in today's borderless space. Second, you need new state-of-the-art tools to understand user access and activity and anticipate security compromises faster than humans can react.

Here's how Okta and Cortex XDR work together to make it happen



Okta and Palo Alto Networks Cortex XDR

High-signal alerts

ML-based Behavior Analytics

Custom Rules

Integrated Data

Data

Data

Data

Data

Network

Endpoint

Cloud

Third-Party Data

Expanded Visibility to Authentication Data with Identity Threat Protection (ITP)

Authentication logs allow you to unearth unusual user activity like credential abuse. By searching for suspicious activity, such as a user signing in from an external IP address, you can quickly zero in on user-based attacks. With Identity Threat Protection (ITP) powered by Okta AI, Cortex XDR gains access to real-time, risk-based signals that detect and assess anomalies during authentication—before a session begins. ITP enhances Cortex XDR's threat intelligence by surfacing high-risk logins using advanced behavioral analysis and dynamic risk scoring. Cortex XDR directly ingests this enriched telemetry from Okta, combining it with authentication data from other sources—whether cloud-based or on-prem—to provide a unified, extensible platform for threat hunting and investigations across all identity signals.

Powerful Threat Hunting with Okta AI-Driven Insights

Using Okta-enriched authentication stories and ITP signals, Cortex XDR allows analysts to quickly identify advanced threats by providing a platform to query and review high-risk authentication sessions. With AI-powered risk scoring from ITP, analysts can prioritize investigation of the most critical threats first. Whether using the intuitive Query Builder or leveraging powerful text-based queries, security teams can proactively hunt across a deeper, AI-informed identity dataset. Cortex XDR's management console—augmented with ITP's real-time risk signals—helps your team rapidly determine the sequence, scope, and context of an attack and initiate swift investigations.

Expanded Rapid Response with Integrated Risk Signals

Once a credible threat has been identified, Cortex XDR empowers your teams to perform a wide range of sweeping actions across your entire infrastructure. With ITP integrated, response actions can now be tied directly to risky user behaviors identified by Okta. Your team can shut down fast-spreading attacks by terminating processes, quarantining files, isolating endpoints, blocking domains—and critically, disabling high-risk user accounts in real time via ITP-driven automation. By combining Okta's identity intelligence and Cortex XDR's endpoint and network telemetry, organizations can align detection and response around user behavior and risk—accelerating remediation while reducing noise.

About Okta

Okta, Inc. is The World's Identity Company™. We secure identity, so everyone is free to safely use any technology. Our customer and workforce solutions empower businesses and developers to use the power of identity to drive security, efficiencies, and success. Learn why the world's leading brands trust Okta at **okta.com**.