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 Network have partnered to help your security analysts quickly get in front of threats as they emerge. The integration of Okta Identity Cloud 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 for Complete Prevention, Detection and Response

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

The Okta Identity Cloud 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.

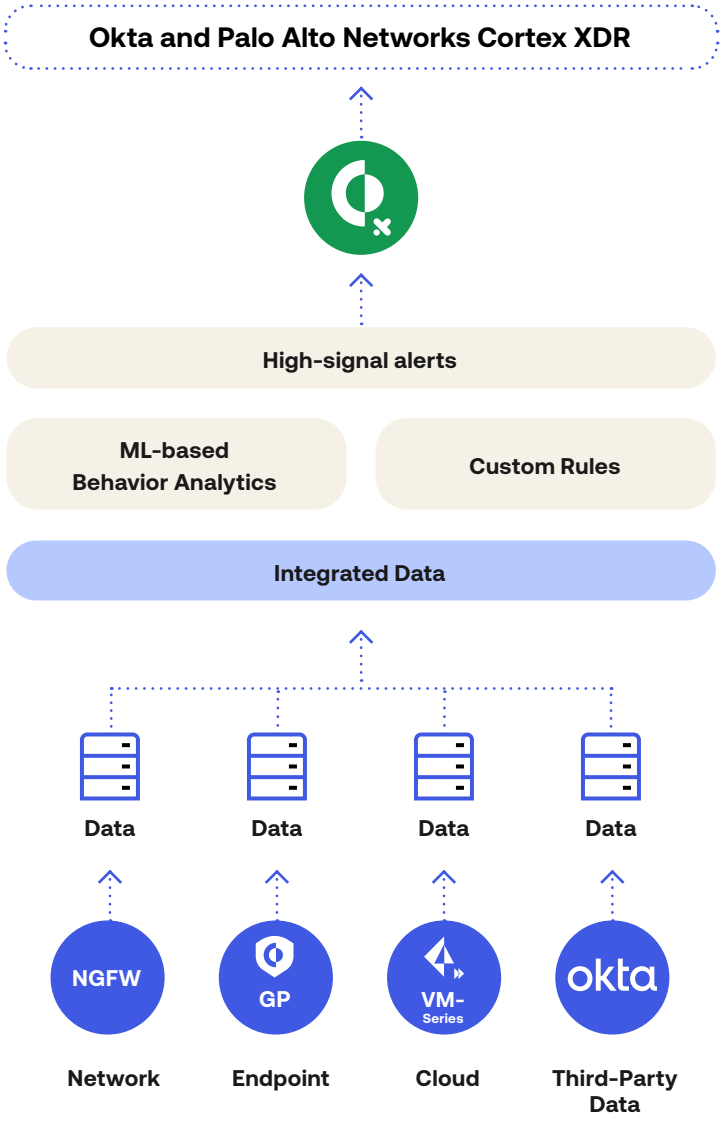
The Challenge: Keeping Up with the Speed of Threats

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



Expanded Visibility to Authentication Data

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. Cortex XDR directly ingests rich data from Okta's user authentication logs to deepen its understanding of access activity across your extended enterprise network. Cortex XDR can unite authentication logs and data regardless of the information source, including from a cloud-based authentication service or an on-premise key distribution center, into a uniform schema, providing an extensible platform for threat hunting and investigations across all your identity data.

Powerful Threat Hunting

Using Okta-enriched authentication stories, Cortex XDR allows analysts to quickly identify advanced threats by providing a platform to query and review authentication sessions. You can hunt for and investigate threats by searching through authentication logs with the intuitive Query Builder or using powerful text-based queries with regular expressions and wildcards. Cortex XDR's management console can help your team rapidly determine the sequence and scope of an attack and initiate on-the-spot investigations.

Expanded Rapid Response

Once a credible threat has been identified, Cortex XDR empowers your teams to perform a wide range of sweeping actions across your entire infrastructure, including multiple endpoints or firewalls simultaneously. Your team can shut down fast-spreading attacks by terminating processes, quarantining suspect files, isolating endpoints, adding domains to blocklists, and more. Integration with Cortex XSOAR, the industry's first extended security orchestration, automation and response solution, adds additional capabilities, including letting your team disable user accounts via integration with Okta, create playbooks from agent scripts, and automate response for high-risk scenarios. This integration combines Okta and Cortex XDR's considerable powers to help your organization focus its security posture around user identity and behavior, so you can provide safe, reliable access to your users while quickly rooting out threats— now and into the future.