Cortex XDR and Okta Identity Cloud

Give IT and Security Teams the Ability to Quickly Adapt to Rapidly Evolving Threats and IT Ecosystems

Benefits

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 Identity Cloud and Cortex XDR® provides:

- Expanded visibility into authentication data
- Powerful threat hunting capabilities
- Expanded rapid response to halt fast-spreading attacks
- Access to Identity Analytics for detecting compromised accounts and more

The Challenge

Today's advanced attackers will steal users' credentials, so they can move laterally and undetected in order to launch disruptive and costly attacks. Malicious insiders aiming to compromise or steal high-value data will also abuse user credentials—either their own or others—to achieve their goals.

Identity-based security is essential for organizations to stay on top of these threats while providing safe, reliable access to IT resources to all authorized users, no matter where they're located. It's also a must for any organization pursuing a Zero Trust approach to security, which requires continuous monitoring and validation of identity from a user's initial request for access through every transaction stage that follows.

The Solution

Focusing your organization's security posture around user identity and behavior helps you provide safe, reliable access to your users while quickly rooting out threats—now and into the future. When your security analysts have increased visibility into authentication data and access to powerful threat-hunting and expanded rapid response capabilities, they can move faster to detect unusual user activity, address instances of credential abuse, and uncover root causes. And when your IT team uses a combination of identity-based security and fast, accurate threat detection with artificial intelligence (AI) analytics, it's easier for them to keep workers collaborating productively and safely, no matter where they're located.

Okta Identity Cloud

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 software-as-a-service (SaaS) applications, web access management (WAM) systems and custom web apps, APIs, and infrastructure. With one set of credentials, users can access all the resources they need to be productive, wherever and on whatever device they choose.

Administrators can assign resources relevant to a user's role and 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 human resources (HR) systems like Workday®, and automate the onboarding and offboarding of apps, saving administrators time and reducing the risk of misconfigurations.

Palo Alto Networks 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. Through Cortex XDR, your teams 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. With Cortex XDR, you can improve your security posture and drive ROI, while lowering TCO and streamlining security by replacing siloed tools and data storage with an efficient, integrated platform.

Keep Pace with the Speed of Threats

Only identity-based security solutions are flexible enough and secure enough to support the needs of today's complex remote teams working in modern cloud and hybrid enterprise workspaces. Your organization needs state-of-the-art tools, like Cortex XDR and Okta Identity Cloud, to understand user access and activity and anticipate potential compromises faster than humans can.

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 also unite authentication logs and data regardless of the information source—including from a cloud-based authentication service—into a uniform schema, providing an extensible platform for threat hunting and investigations across all your identity data.

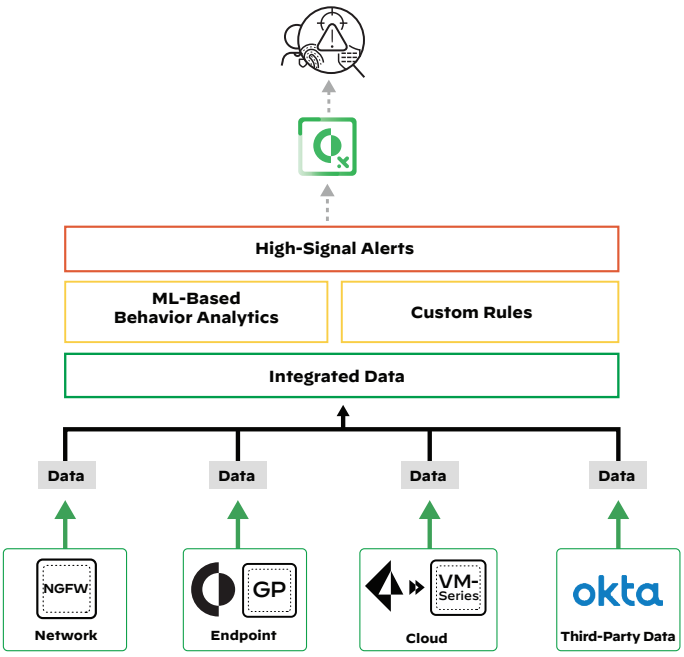

Figure 1: Overview of the Cortex XDR and Okta Identity Cloud integration

Use Case 1: Detect Compromised Accounts and Malicious Insider Activity

Challenge

Organizations need identity-related risk awareness to help prevent their exposure to attacks due to compromised users accounts and malicious insiders. They also need to quickly identify evidence of compromised credentials, especially on privileged accounts for high-level network access, so that important proprietary information isn't susceptible to security breaches.

Solution

The Identity Analytics module in Cortex XDR provides visibility into user activities such as logins, authentication, SASE gateway connections, application executions, and much more. Identity Analytics leverages user activity data from numerous sources, including the Okta authentication logs, endpoints, endpoint agents, network firewalls, Active Directory, event logs, SASE gateways, and more. Security teams can also use Identity Analytics in Cortex XDR to locate improper credential use and assess risks with AI or behavioral analytics. In addition, they can examine traffic and data from various sources to identify endpoints and users on the network.

Use Case 2: Engage in Powerful Threat Hunting

Challenge

Security analysts need to identify advanced threats quickly, determine the sequence and scope of attacks, and initiate on-the-spot investigations.

Solution

Cortex XDR uses Okta-enriched authentication to provide security teams with a platform for querying and reviewing authentication sessions. Security analysts can use Cortex XDR to hunt for and investigate threats by searching through authentication logs with the intuitive Query Builder or by using powerful text-based queries with regular expressions and wildcards. The Cortex XDR management console helps teams understand how an attack is unfolding, how widespread it is, and move fast to investigate incidents.

Use Case 3: Expand Rapid Response and Shut Down Attacks

Challenge

Once a credible threat has been identified, security teams must be able to perform a range of actions across the organization's entire infrastructure, including multiple endpoints or firewalls, simultaneously.

Solution

With the Cortex XDR and Okta Identity Cloud integration, your security team can shut down fast-spreading attacks by terminating processes, quarantining suspect files, isolating endpoints, adding domains to block lists, and more. The integration with Cortex XSOAR, the industry's first extended security orchestration, automation, and response solution, extends the capabilities of the Cortex XDR integration by letting your team disable user accounts via Okta integration, create playbooks from agent scripts, and automate response for high-risk scenarios.

Palo Alto Networks and Okta—Other Integrations

Other product integrations between Palo Alto Networks and Okta include:

- Prisma® Access and Okta SSO to secure remote access
- NGFW and Okta Identity Cloud to prevent credential theft and abuse
- Prisma Cloud and Okta SSO to seamlessly integrate Okta users and permissions into AWS®
- Cortex XSOAR and Okta Cloud-Based Identity Management Service to orchestrate and automate incident response across Identity Access Management

For more details on these integrations, visit https://technologypartners.paloaltonetworks.com/English/listing/1401394.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud lets organizations securely connect the right people to the right technologies at the right time. With over 6,500 prebuilt integrations to infrastructure providers and applications, Okta customers can easily and securely use the best technologies for their business. For more information, visit www.okta.com.

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. For more information, visit www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com