Okta + Cisco + Exabeam: Comprehensive Visibility, Security and Response

SecOps teams face a never-ending barrage of individual security events, and remediating each of these threats is exhausting and fraught with risk. The challenge is to strengthen defense: by aggregating alerts for visibility across users and network, by building sophisticated, data-driven incident timelines, by conducting deep security analysis to identify real threats, with the goal of orchestrating swift remediation.

Okta, Cisco and Exabeam have joined forces to offer that complete solution, to help you quickly and decisively identify and block threats wherever and whenever they occur.

Okta, the leading independent provider of identity for enterprises, together with Cisco, the market leader in network security, and with Exabeam, the next-generation SIEM, now integrate in a single solution designed to help enterprises safeguard their users, networks, and data from cloud to ground against a broad range of sophisticated threats. Okta provides rich identity context, Cisco offers complete network data, and Exabeam delivers advanced security intelligence. Any malicious threats detected by Exabeam are remediated by Cisco for the network and Okta for the user for complete enterprise security.

Together, Okta + Cisco + Exabeam let you:

- Detect potential threats for all user activity and network threats across the attack lifecycle
- Aggregate security data from across your enterprise into one intelligent framework
- Analyze the aggregated security data to pinpoint suspicious user or entity behavior
- Remediate compromised credentials and insider threats across both users and your network

Security Triple Play

Okta provides:

- Streamlined access across hybrid IT via Okta single sign-on (SSO)
- Advanced security and user remediation via adaptive multi-factor authentication (MFA)

Cisco provides:

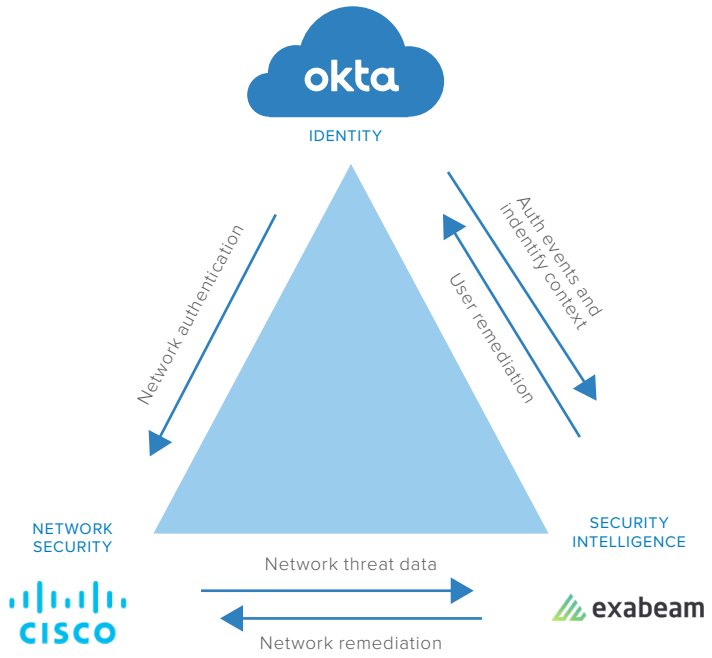
- Comprehensive threat protection across your network, email, web and DNS
- Centralized control enforcement point via Cisco Umbrella, ASA, AnyConnect, Threat Grid, ISE, WSA, AMP, ESA, Stealthwatch, and PxGrid

Exabeam provides:

- Aggregation of disparate security logs into a consolidated Data Lake informed by Advanced and Entity Analytics intelligence
- Advanced analytics engine via Exabeam Incident Responder for security orchestration and remediation

Solution Scenario

Example: Despite your best efforts, imagine your CEO falls victim to a phishing attack. This would be a nightmare for most, but thankfully you're covered because you've already deployed this security triple play. When the threat actor uses those stolen credentials to try accessing a sensitive internal financial application, you can stop him in his tracks. You've set up Okta MFA for your Cisco AnyConnect VPN, and the threat actor fails repeated MFA prompts. Okta provides the auth data showing failed log-in attempts on the Cisco VPN to Exabeam. Exabeam obtains additional context from Cisco IronPort, an email and web gateway solution, for Exabeam to build an incident timeline, and Exabeam adjusts the risk scores from data via Cisco Umbrella. Exabeam remediates against the user by kicking off a playbook to suspend their account in Okta until IT can reauthorize your grateful CEO with clean credentials.



Enhanced Visibility and Orchestrated Response

Okta takes user logs and authentication data and adds incident enrichment through user and identity context, while Cisco provides the breadth and depth with network, web and device data. Exabeam takes all of these inputs and applies advanced analytics and machine learning to quickly spot suspicious user behavior and network threats. The result is a consolidated view of security incidents, and dramatically improved visibility across your security environment.

Once a threat is detected, Exabeam's deep security analytics work with Cisco and Okta's control policies to support automated investigation and response, build incident timelines, adjust risk scores, and automatically trigger or elevate actions from either Cisco or Okta. Cisco enforces threat responses across the network, while Okta takes action against the user by applying policy enforcement to move suspicious users into higher risk groups, step up auth, or suspend their accounts.

Strengthen your security and stop data breaches in their tracks.

With Okta + Cisco + Exabeam integrated together, enterprises can:

- Protect the enterprise from risky behavior and malicious threats
- Detect complex and developing threats by intelligently analyzing data and event logs
- Automatically trigger quick, informed responses to threats from any source

Okta + Cisco + Exabeam combine the industry's best security expertise to provide a comprehensive and modern security fabric for defending corporate networks and cloud deployments with an integration that lets enterprises protect their resources, detect threats from outside and within, and respond decisively.

For more information on this integration, go to okta.com/integrations/MFA-for-VPN/cisco/ or okta.com/partners/exabeam. If you have more questions, please contact our sales team at okta.com/contact-sales.

*According to Verizon's 2018 Data Breach Investigations Report

About Okta

Okta is the leading provider of identity for the enterprise. The Okta Identity Cloud connects and protects employees of many of the world's largest enterprises. It also securely connects enterprises to their partners, suppliers and customers. With deep integrations to over 5,000 apps, the Okta Identity Cloud enables simple and secure access from any device.

Thousands of customers, including Experian, 20th Century Fox, LinkedIn, Flex, News Corp, Dish Networks and Adobe trust Okta to work faster, boost revenue and stay secure. Okta helps customers fulfill their missions faster by making it safe and easy to use the technologies they need to do their most significant work.

https://okta.com