okta + splunk>

Unleash the Power of Identity for Your Security Team

Stolen credentials continue to be a major source of data breaches.[1] Security teams need clear visibility into identity data in order to identify, triage, and respond instantly to credential-based attacks. Even the critical security tools you rely on need to be protected. Okta and Splunk can help.

Quickly go from data to action

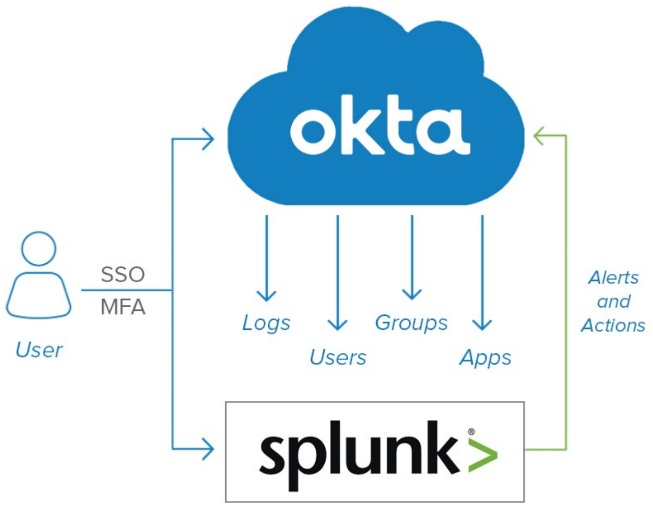
Okta, the leading independent provider of identity for the enterprise, integrates with Splunk, one of the most widely-deployed security information and event management systems (SIEMs) on the market, to enrich security data with additional identity context to make it easier to spot and act upon suspicious user activity.

Okta + Splunk work together to aggregate and correlate identity data from Okta alongside other logs from across the IT environment. Now security teams can easily see who's logging in to what apps, from what location and device, and identify unusual behavior before it becomes an issue. Once suspicious activity is identified, security analysts can work within Splunk to trigger a security action from Okta, such as move the user into a higher-security group that requires multi-factor authentication, restrict the user's access, or block the user.

Together, Okta + Splunk enable enterprises to:

- Aggregate rich identity event data from Okta and correlate it with information from other sources for advanced parsing and data modeling
- Shorten the time to detect inappropriate activity and consolidate the information to remediate issues more effectively
- Enforce security actions for containment, such as limit user access, prompt for multi-factor authentication, and more
- Perform fast and powerful ad-hoc queries of event logs, users, and groups to view trends in app usage and adoption

Integration Overview



[1] *2018 Verizon Data Breach Incident Report*

How Okta + Splunk work together

Okta provides a deep repository of identity data, while Splunk provides breadth of information from across the IT environment. Okta sends event logs and additional data from Okta's APIs to Splunk. This allows you to do more than just search the logs; you can also find users based on a variety of attributes, such as last login, status changes, profile data, group membership, and app assignment.

With this enriched Okta identity data and Splunk's powerful visualization and analysis tools, security analysts can quickly understand if a user's activity is appropriate, know who the actors are, and what targets are involved. This makes it possible to get to actionable insights more quickly, and remediate threats before they cause real damage.

The integration of Okta and Splunk enables enterprises to streamline and accelerate security actions. Once suspicious behavior is identified, security analysts can trigger Okta actions from within Splunk and quickly move suspicious users to a group that requires additional security measures, up to suspending the user account. Together, Okta and Splunk use identity to close the security loop.

Okta + Splunk also help enterprises analyze trends in business app usage and adoption. For example, an enterprise can see how many users it has on a particular app, see where they're located, and how they're using the app. This can help the enterprise make more efficient provisioning decisions about assigning and retiring licenses.

Protect Splunk with MFA and SSO from Okta

Splunk contains a vast repository of logs and data from across your business environment. Increasingly, Splunk delivers valuable information to users outside of your security team. As a result, it's critical to protect Splunk from unauthorized use while streamlining access for appropriate users.

Okta lets you improve access security for Splunk Enterprise and Splunk Cloud. Ensure strong authentication for improved identity assurance with Okta Adaptive Multi-Factor Authentication (MFA). Additionally, provide streamlined access for Splunk users through Okta Single Sign-On (SSO).

Identity-driven security for your security operations

With Okta + Splunk, enterprises can:

- Equip your security team with identity data from Okta to enhance visibility within Splunk
- Detect anomalous behavior more quickly to mitigate threats
- Execute security actions in Okta directly from Splunk, streamlining security workflows
- Uncover trends in business app usage for operational efficiency
- Protect access to Splunk with Adaptive MFA and SSO

For more information on this integration, go to **okta.com/partners/splunk**

If you have more questions, please contact our sales team at **okta.com/contact-sales**

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.

For more information, go to https://okta.com