SECURONIX Security Analytics. Delivered. | okta

SOLUTION BRIEF

Risk-Based Authentication and Monitoring with Securonix and Okta Integration

Securonix Security Analytics Platform enables you to detect, investigate, and respond to cybersecurity threats in real time. Okta Identity Cloud provides secure connections between people and technology to enable any user to access any technology on any device. When integrated together, Okta and Securonix allow you to aggregate user activity, detect suspicious activity, and prompt immediate response against malicious actors.

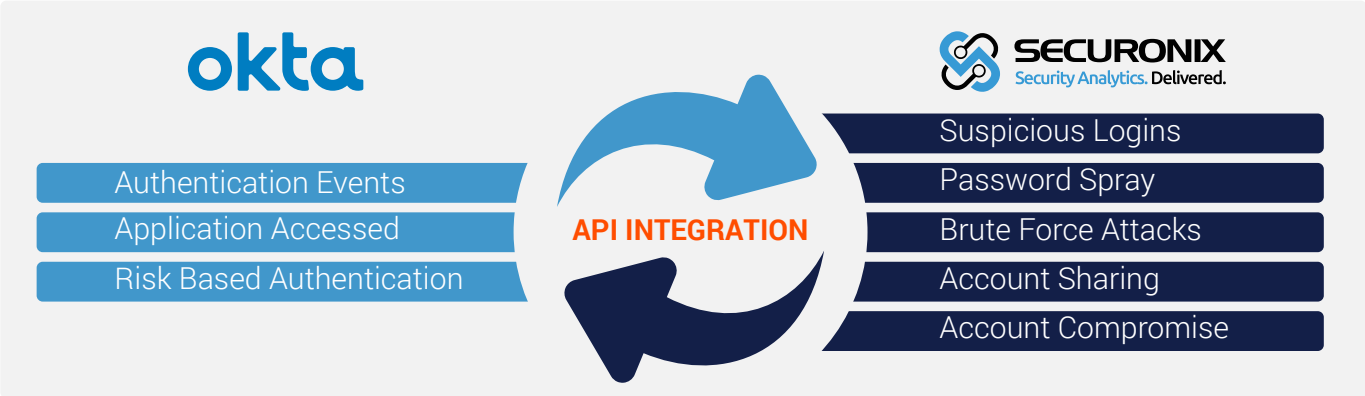
The Challenge and Solution

When your applications and data reside in the cloud and your users access critical data worldwide, managing and monitoring user access across your hybrid IT environment is a critical security concern. Okta provides the ability to enforce strong authentication requirements for all users across your entire environment. Acting both as a security watch tower and control point, Okta captures valuable information including user location, time, device, and the number of attempts.

Securonix uses an API integration to collect security events from Okta in real time and monitors the authentication logs for suspicious login activities and locations, brute force attacks, password spray attacks, credential sharing, and account compromise. Securonix applies advanced security analytics and machine learning to detect threats in real time. Automated workflows allow you to take immediate action based upon risk scores. This may require high-risk users to perform step-up authentication or deny authentication attempts. Together, Securonix and Okta provide complete visibility and response to mitigate risks related to insider threats and data breaches.

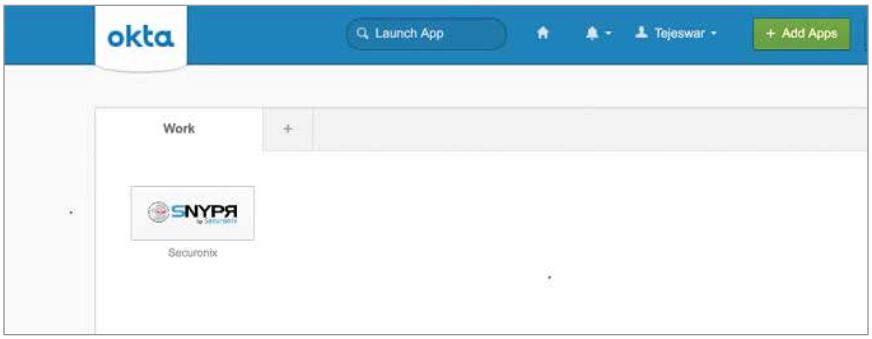
Integration Benefits

- Gain visibility and insight into user activity across your environment.
- Detect authentication attempts and password attacks.
- Pinpoint suspicious users and compromised accounts.
- Take immediate action against user accounts. For example, by requiring step-up authentication.
- Mitigate the risk of insider threats and data breach.



Securonix consumes user and event logs from Okta and monitors for suspicious activites. Okta can take action based on threats discovered by Securonix, including prompting for multi-factor authentication (MFA) or even suspending a suspicious user.

Securonix behavior analytics detects that a user's activity deviates from typical behavior, like anomalous logins from disparate geographical locations. The user's risk score is elevated to trigger an automatic response through Okta to mitigate the threat.



Single sign-on (SSO) from the Okta dashboard into Securonix to further enhance and enrich your security analytics.

How it Works

- Securonix uses an API connection to fetch authentication and application access events from Okta.
- Okta provides valuable identity context, including user location, time, device, and number of attempts.
- Securonix creates data insights to visualize authentication patterns, provide risk scores, and detect anomalous activity.
- Threats with an elevated risk score trigger immediate or partially automated workflows through Okta.
- Okta responds by moving the user into a different group, while prompting for step-up authentication or even account suspension.

About Securonix

Securonix transforms enterprise security with actionable intelligence. Using a purpose-built security analytics platform Securonix quickly and accurately detects high-risk threats to your organization. For more information visit www.securonix.com.

About Okta

As the leading provider of identity for the enterprise, 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 visit www.okta.com.

SECURONIX
Security Analytics. Delivered.

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000

14665 Midway Rd. Suite #100, Addison, TX 75001 |