

# Secure Okta with Comprehensive SaaS Security

## The Challenge

With sensitive data increasingly moving to the cloud to enhance productivity, organizations extend their security perimeters beyond traditional boundaries. Okta administrators and security teams must securely manage access and understand both user and non-human activities across this expanded digital landscape. Staying on top of policies, configurations, and detecting third-party SaaS connections and threats is critical. Without comprehensive visibility, third-party apps can introduce hidden vulnerabilities that may lead to data breaches.

## The Solution

Integrating Okta with AppOmni enhances visibility and control across Okta Classic or Okta Identity Engine (OIE) and your SaaS landscape, allowing comprehensive management of multiple tenants for improved access, configuration, and policy control. AppOmni enhances security by applying over 60 baseline threat detection rules and scrutinizing numerous Okta-specific configurations, significantly mitigating data breach risks. The platform offers proactive management tools to mitigate third-party and compliance risks, safeguarding sensitive data by monitoring unauthorized connections to Okta and other SaaS applications. AppOmni promotes an integrated security approach that fosters collaboration across teams and facilitates a unified security monitoring and response platform. Such an approach streamlines decision-making and bolsters your organization's overall security posture.



### THE CHALLENGE

- Limited SaaS visibility
- Unmonitored access risks and third-party connections
- Inefficient remediation workflows
- Policy enforcement challenges lead to non-compliance



### THE BENEFITS

- Enhance visibility and control
- Proactive third-party and compliance risk management
- Efficient threat detection and incident response
- Strengthened policy enforcement and compliance










### KEY CAPABILITIES

- Support for OIE and Okta Classic
- Connectivity Visualization
- Threat Detection and Response
- Policy Enforcement & Compliance
- Drift Detection
- Extend Identity Awareness

## Effortlessly Monitor and Manage Policy Issues

Assess Policy Issues in AppOmni to identify misconfigurations and security within Okta. Address these policy violations efficiently with integrated remediation tools to ensure your environment remains secure and compliant.

| <input type="checkbox"/> Risk ▾   | Service & Type  | Environment | Rule Description  |
|-----------------------------------|---|-------------|---|
| <input type="checkbox"/> Critical |  Okta Identity Engine<br>Okta  | Production  | Alert me when new Authentication Policy rules are created and not listed as allowed |
| <input type="checkbox"/> Critical |  Okta Identity Engine<br>Okta  | Production  | All Authentication Policy Rules' setting '[OIE] Factor Mode Type' must be TwoFactor |
| <input type="checkbox"/> Critical |  Okta - Prod<br>Okta           | Production  | Alert me when new MFA Policy rules are created and not listed as allowed            |
| <input type="checkbox"/> Critical |  Okta Identity Engine<br>Okta  | Production  | Alert me when new Sign On Policy rules are created and not listed as allowed        |
| <input type="checkbox"/> High     |  Okta Identity Engine<br>Okta  | Production  | All MFA Policies' setting '[OIE] Security Question MFA' must be Not Allowed         |
| <input type="checkbox"/> High     |  Okta - Prod<br>Okta           | Production  | All Sign On Policy Rules' setting 'Maximum Session Idle Time' must be less than 3   |
| <input type="checkbox"/> High     |  Okta Identity Engine<br>Okta | Production  | Alert me when new Groups are created and not listed as an exception                 |

## Key Capabilities

| Capability                       | Description   | Use Case  |
|----------------------------------|---|---|
| Support for OIE and Okta Classic | Comprehensive support for both OIE and Okta Classic ensures seamless integration and enhanced security features across all Okta environments.             | Enterprises migrate to OIE benefitting from the advanced security features OIE enables in AppOmni.  |
| Policy Enforcement & Compliance  | Advanced scanning and monitoring capabilities enforce security policies and detect policy violations within Okta, reducing the risk of compliance issues. | A retail organization continuously monitors to enforce security policies, flagging and correcting unauthorized changes to user access permissions, ensuring ongoing compliance with PCI requirements. |

| Capability                    | Description  | Use Case   |
|-------------------------------|--|--|
| Threat Detection and Response | Continuously monitors Okta for suspicious activities, such as unauthorized access attempts and data exfiltration, providing timely detection and mitigation of threats.            | A financial services company using Okta can quickly detect and respond to a brute force attack on user accounts, preventing unauthorized access to sensitive data.                                       |
| Extend Identity Awareness     | Manage and secure identities by providing visibility into user activities and attributes within SaaS applications, helping to enforce dynamic and context-aware security policies. | A global technology company uses AppOmni Identities to detect and respond to unusual user activities, such as unexpectedly large data access, ensuring robust identity governance and enhanced security. |
| Connected App Management      | Approve trusted apps and monitor unapproved apps connected to Okta, reducing risks of compromised credentials and unauthorized access.   | An organization using Okta can see all connected SaaS applications in a single dashboard, identifying and managing any unauthorized applications to prevent potential security risks.                    |

## About AppOmni

AppOmni is a leader in SaaS Security and enables customers to achieve secure productivity with their SaaS applications. With AppOmni, security teams and SaaS application owners quickly secure their mission-critical and sensitive data from attackers and insider threats. The AppOmni Platform continuously scans SaaS APIs, configurations, and ingested audit logs to deliver complete data access visibility, secure identities and SaaS-to-SaaS connections, detect threats, prioritize insights, and simplify compliance reporting. 25% of the Fortune 100 and global enterprises across industries trust AppOmni to secure their SaaS applications.

© 2024 All Rights Reserved

[Request a demo](#) to see how you can use AppOmni with OIE to secure your SaaS environment.