Datasheet January 2026

okta

Securing Overprivileged OAuth Tokens with Okta ISPM

Gain visibility and control over the OAuth tokens that connect your critical applications.

In today's interconnected world, the applications that power your business are a double-edged sword. While they boost productivity, the OAuth tokens connecting them create a hidden, often unmonitored, attack surface. The 2025 Salesforce-Gainsight breach was a wake-up call, demonstrating how stolen OAuth tokens from one compromised vendor can be used to attack hundreds of their customers. Read on to find out how Okta Identity Security Posture Management (ISPM) can help protect OAuth tokens, service principals, and certificates that power AI Agents.

Why OAuth Token Security is Your New Priority

The Gainsight breach wasn't a failure of passwords or multi-factor authentication. It was a failure to secure application-to-application connections. Attackers exploited the inherent trust granted by OAuth tokens, turning a legitimate integration into high privileged, easy access.

Without dedicated security for these tokens, you are blind to critical risks:

- **Persistent Access:** Stolen refresh tokens can give attackers long-term, silent access to your sensitive data.
- **Excessive Permissions:** Apps often have far more access than they need, making them a prime target.
- **Third-Party Risk:** A breach in any one of your vendors can potentially lead to a breach in your own environment.

Introducing Okta ISPM with OAuth Token Security

Okta ISPM provides a comprehensive view of your identity security posture, from your security policies in Okta to downstream applications, enabling you to proactively find and fix vulnerabilities. Now, Okta is extending that visibility to workload app identities.

This new feature gives you the power to see and help secure the OAuth tokens that connect your critical SaaS applications, like Salesforce, to the rest of your technology stack.

okta

Capabilities

This new feature provides end-to-end control over your application identity landscape:

Discover Inventory: Automatically discover and catalog the OAuth tokens—both first-party and third-party—across your environment.

Identify Risk: Pinpoint risky tokens with excessive permissions, unrotated or unused tokens and secrets, or those with unexpired secrets.

Continuous Monitoring: Gain visibility and receive alerts when new tokens are created or permissions escalate, ensuring no new risks go unnoticed.

Remediation: Trigger workflows to revoke risky tokens or reduce their access to enforce the principle of least privilege.

**Features will be released on an ongoing basis throughout CY26*

Benefits: Harden Your Defenses, Build Trust

By securing your workload app identities with Okta ISPM, you can:

- **Prevent Supply Chain Attacks:** Helps eliminate the blind spots that attackers exploit to move between connected systems.
- **Reduce Your Attack Surface:** Helps ensure applications have only the minimum access required, limiting the blast radius of a potential compromise.
- **Achieve Proactive Security:** Move from a reactive to a proactive security model by continuously identifying and fixing identity risks before they can be exploited.

Ready to protect your Oauth tokens against supply chain attacks? Contact us today.

Any mention of future products, features, functionalities, or certifications in this presentation is for informational purposes only. These items are not commitments to deliver and should not be relied upon to make purchasing decisions.