Secure, Manage, and Control User Access to Data

Forcepoint with Okta Identity Access Management integration

Challenge

- Gain visibility into user behavior of people within an organization who log in from different places or from various devices.

Solution

- Forcepoint DUP uses behavioral intelligence to streamline risk.
- Forcepoint DEP enables secure access to cloud and on-premises environments.
- Okta Identity Cloud enforces password security and authenticates and secures application logins with SSO within cloud environments.

Outcome

- Gain the ability to leverage your existing investment with Forcepoint to identify, manage, and remediate against compromised access incidents.

Digital transformation that outpaces cybersecurity creates opportunities for bad actors to prey on unprotected networks. A strong cybersecurity approach begins with identifying every user, no matter where they are working, and continuously assessing the risk they pose in order to safely manage access. Forcepoint has partnered with Okta to provide integrated, cloud-native, Zero Trust-modeled Identity Access Management (IAM) services that provide dynamic, continuous security through an understanding of user identity and application and user security risk protection.

Forcepoint Dynamic User Protection (DUP) and Forcepoint Dynamic Edge Protection (DEP)

Understanding human identity and understanding user behavior are two keys to stopping high-risk users from accessing network data and organizational assets. Forcepoint DUP and Forcepoint DEP solutions work together to eliminate security gaps and streamline compliance, delivering greater productivity for both security analysts, by eliminating false positives, and users, by providing faster access to cloud apps.

Forcepoint DEP provides web, cloud, and private application management and protection

DEP safely provides controlled access to web, cloud, and private applications—protected against advanced threats and data loss—to all of your people wherever they're working: at home, in the office, or on the road.

DEP Solution

→ Cloud Security Gateway (CSG) secures user access to SaaS apps and public internet

→ Private Access (PA) provides Zero-Trust remote access to private apps without the pain of VPNs

Business Outcomes

→ **Lower costs:** Cut CAPEX and OPEX by not having to buy, deploy, and manage patchworks of security hardware and software

→ **Reduced risk:** Deliver strong, extensible security against advanced threats and data loss without gaps or redundancies

→ **Greater productivity:** Give remote users faster access to cloud apps without putting your business at risk

Forcepoint DUP insider risk prioritization and analysis

Solution

- → Streamlines risk management and reduces the threat of data loss
- → Enforces data protection policies based on each employee's unique risk level
- → Democratized user activity monitoring via a lightweight, cloud-based solution

Business Outcomes

- → **Meaningful visibility:** Understand user behaviors with real-time risk calculations
- → **Immediate TTV:** Frictionless deployment and policy management
- → **Enhanced productivity:** Increase analyst capacity to investigate users through the elimination of false positives

Okta Identity Cloud Platform

The Okta Platform provides a complete identity layer for any application and is the foundation for secure connections between people and technology. By harnessing the power of the cloud, Okta allows people to access applications on any device at any time, while still enforcing strong security protections.

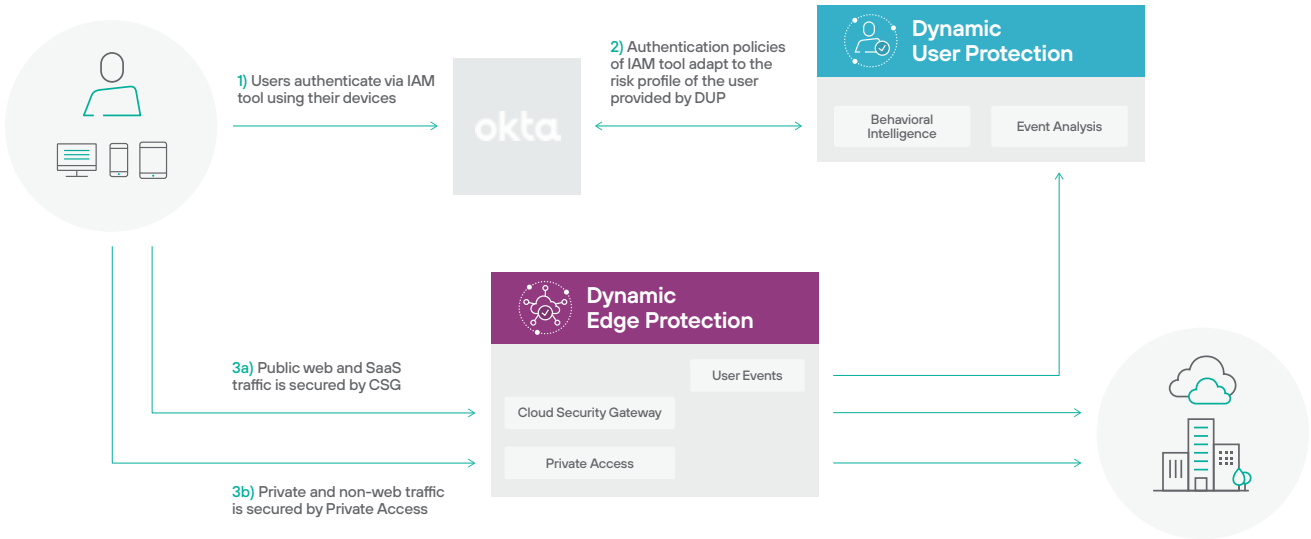
Okta's suite of products include the base products Okta Single Sign-On (SSO) and Okta Adaptive Single Sign-On, with a variety of available add-ons—including Universal Director, Adaptive Multi-Factor Authentication, and API Access Management—that provide extensive adaptive and contextual authentication.

Better together: Forcepoint Zero Trust services integrated with Okta Identity Cloud

Forcepoint Behavioral Analytics works with the Okta platform to provide a complete identity, security, and risk protection solution. Users can engage with Okta's contextual and adaptive authentication on their own devices or company-issued equipment. System logs are created by Okta that are ingested by Forcepoint DUP and DEP to analyze event and user behavior, then assigned a risk score that is stored using the Okta user and group ID.

For accounts that are assessed high risk scores, Okta can change the membership to terminate an active session, denying SSO, and forcing a new log-in. Each new login attempt goes through the same process to analyze access based on user risk. Users who are granted access are then allowed to safely and securely access web traffic that is secured by Forcepoint DEP Zero Trust services.

IAM Integration Diagram



forcepoint.com/contact