Secure, Manage, and Control User Access to Data

Forcepoint with Ping 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

- User behavior is analyzed and assigned a risk score by Forcepoint. If a high risk score is identified, Ping can assess the findings and enforce additional controls such as multi-factor authentication.

Outcome

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

Digital transformation can create opportunities for bad actors to prey on unsuspecting networks. Security officers are tasked with securing the many new ways of working from anywhere and safeguarding data wherever and however it's being used. It begins with identifying user risk and managing access to environments within an organization. Forcepoint has partnered with Ping to provide integrated, cloud-native, Zero Trust services that continuously provide 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 behavior are key capabilities for identifying threatening behavior before users access network data and organizational assets. Forcepoint Dynamic User Protection (DUP) and Dynamic Edge Protection (DEP) solution work together to eliminate security gaps and streamline the ability to demonstrate compliance, delivering greater productivity.

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

Forcepoint DEP solution provides controlled access to the web, cloud, and private applications—protecting against advanced threats and data loss—to all of your people, wherever they're working.

DEP Solution

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

→ Private Access (PA) provides Zero-Trust remote access to internal 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

PingFederate Single Sign On

PingFederate is a modern identity and access management (IAM) solution designed to meet complex enterprise demands. By integrating silos of identities and applications inside the enterprise, across partners, and into the cloud, PingFederate enables:

- → SSO and identity federation
- → Registration, profile management, and password reset
- → Adaptive authentication policies
- → Social login and account linking

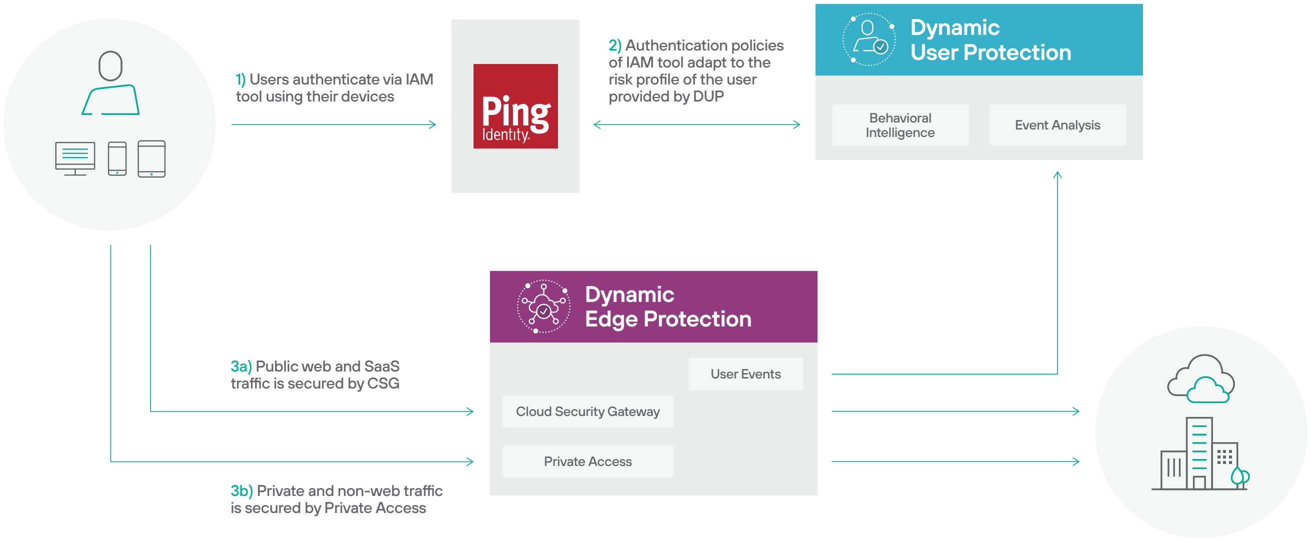
PingFederate provides easy-to-use, secure access to virtually any application, including SaaS, web, mobile, and legacy apps, and utilizes policy controls to optimize the balance of security and convenience for a wide range of use cases.

Better together: Forcepoint Zero Trust services integrated with PingFederate

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

For accounts that are assessed high risk scores, PingFederate 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.

Diagram architecture


1) Users authenticate via IAM tool using their devices
Ping Identity
2) Authentication policies of IAM tool adapt to the risk profile of the user provided by DUP
Dynamic User Protection
Behavioral Intelligence
Event Analysis
Dynamic Edge Protection
User Events
Cloud Security Gateway
Private Access
3a) Public web and SaaS traffic is secured by CSG
3b) Private and non-web traffic is secured by Private Access

forcepoint.com/contact