Zscaler and ForgeRock

Deliver seamless authentication and security to applications — anywhere, anytime, on any device

Challenges

Today's diverse and distributed workforce must connect to more business resources and devices, posing significant challenges to enterprises. Massive volumes of new identities, roles, entitlements, and applications need to be securely managed, often remotely. This situation can be overwhelming for risk professionals and requires a new security approach based on zero trust.

Zero trust is a framework to secure modern organizations based on least–privileged access and the principle that no user or application should be inherently trusted. Connections are authorized based on validation of the user's identity, risk–based context, and business policy.

ForgeRock Workforce IAM helps address these challenges by converging identity management, access management, and identity governance. It provides greater efficiencies, security, and cost savings with the ability to manage, secure, and govern identities throughout their entire lifecycle — all within a single platform.

ForgeRock Access Management determines which applications (modern and legacy) users are authenticated for and authorized to access while delivering a seamless user experience. With self–service registration, single sign–on (SSO), federation, and multifactor authentication (MFA) capabilities, the platform provides both security and convenience.

SSO makes it easy for users to login into multiple resources (applications, services, and systems) with one set of credentials. It also allows users to securely federate one authentication session across multiple applications. In sum, SSO improves the user experience, enhances security, and boosts productivity by eliminating the frustration with password management.

Zscaler is a pioneer in zero trust, enabling customers to accelerate their secure digital transformation journey. The cloud–delivered Zero Trust Exchange platform acts like an intelligent switchboard that securely connects users and applications. All communication goes through the Zero Trust Exchange, and nothing reaches applications without the platform allowing it. Applications become invisible to unauthorized users, so your resources can't be discovered and exploited on the internet

Solution

ForgeRock and Zscaler deliver an integrated zero trust solution that simplifies deployment, improves the user experience, and enables fast, direct, and secure access to applications anytime, anywhere, and on any device. The integration is delivered via Security Assertion Markup Language (SAML) v2.O, an open standard authentication protocol that enables federation, identity management, and SSO.

> ForgeRock and Zscaler simplify deployment, improve the user experience, and enable fast, direct, and secure access to applications.

How it works

ForgeRock's AM utilizes the concept of the "Circle of Trust" to manage the relationship between Identity Providers (IDPs) and Service Providers (SPs).

When configuring AM to provide SSO using SAML v2.0, organizations can map user and group accounts at the identity provider (i.e., ForgeRock) to accounts at the service provider (i.e., Zscaler), including mapping to an anonymous user and/or an OT/IoT device. ForgeRock communicates with Zscaler using SAML assertions, which Zscaler uses to make authorization decisions for access to applications.

ForgeRock AM allows administrators to tailor access for the unique needs of users, design user access journeys with a drag-and-drop interface, add new capabilities (on a moment's notice), and integrate pre-tested and pre-coded technology.

ForgeRock integrates with Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) to enable secure access to SaaS, internet, and private applications.

ZIA includes a comprehensive suite of AI-powered security and data protection services to help stop cyberattacks and prevent data loss with a comprehensive zero trust approach. As a fully cloud-delivered SaaS solution, new capabilities can be added without any additional hardware or lengthy deployment cycles.

ZPA applies the principles of least privilege access to give users secure, direct connectivity to private applications running on-prem or in the public cloud while eliminating unauthorized access and lateral movement. Authorized users can only connect to approved resources, not the network, which is impossible with legacy VPNs.
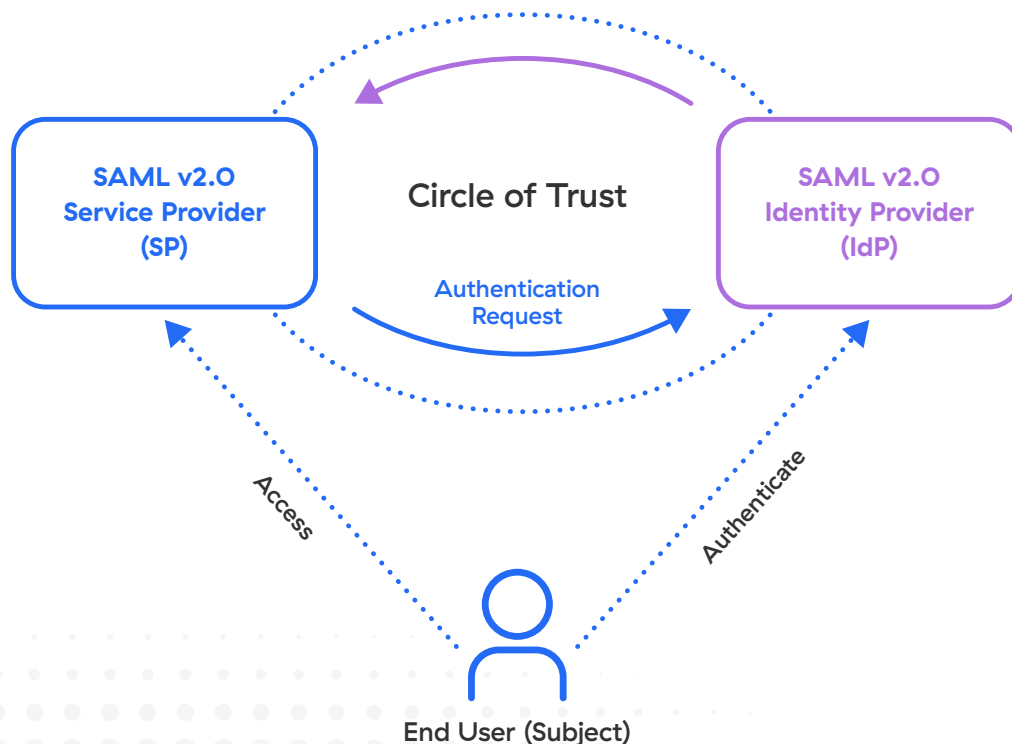

Figure 1. ForgeRock Access Management

Key Benefits

The ForgeRock and Zscaler integration provides the following key benefits:

- Frictionless user experience via Single Sign-on (SSO), delivering a 'log in once, access everything' environment for all users to gain access to all their applications.

- Intelligence-based login decisions, turning user devices and locations into analytics to make real-time, policy-based decisions on user access.

- Reduced attack surface with risk-based authentication that securely connects users directly to authorized apps without accessing the network to prevent lateral movement.

- Secure remote access to internal, SaaS, and internet applications running in the cloud or in data centers using a zero trust framework.

About ForgeRock
ForgeRock® (NYSE: FORG) is a global digital identity leader helping people simply and safely access the connected world. The ForgeRock Identity Platform delivers enterprise-grade identity solutions at scale for customers, employees, and connected devices. More than 1,300 organizations depend on ForgeRock's comprehensive platform to manage and secure identities with identity orchestration, dynamic access controls, governance, and APIs in any cloud or hybrid environment. For more information, visit www.forgerock.com or follow ForgeRock on social media: Facebook ForgeRock | Twitter @ForgeRock | LinkedIn ForgeRock.

ForgeRock®

zscaler | Experience your world, secured.™