

The Power of an Integrated Approach to Zero Trust Cybersecurity

edgile.com



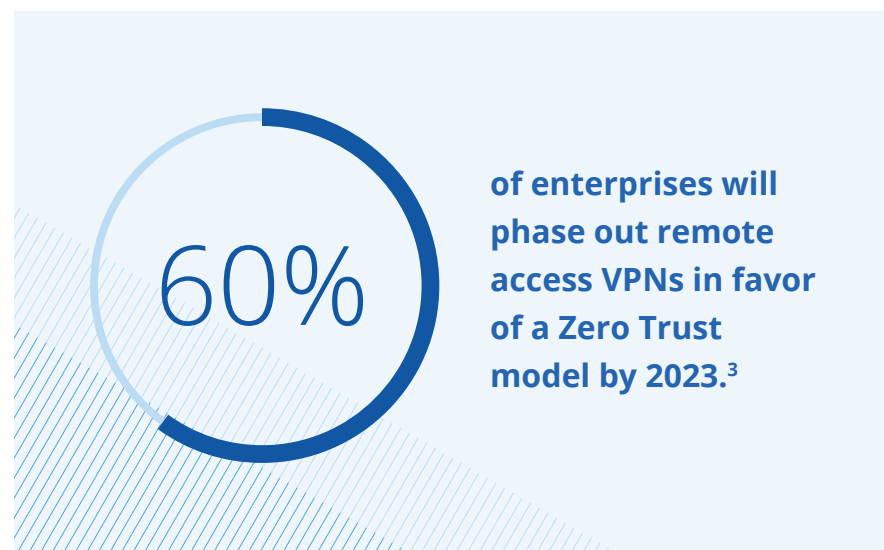
Cloud-based infrastructure is the foundation for digital transformation and is quickly becoming a must-have for modern organizations. In fact, 92% of the world's businesses have already adopted at least some level of cloud computing.¹ With this migration outside the traditional network perimeter, the right level of security can no longer be achieved with firewalls, intrusion detection systems, VPNs, and other network devices. And with cybercrime increasing a staggering 630% in the first quarter of 2020,² one thing is clear: A new approach is needed.

The Zero Trust model

As its name implies, the Zero Trust model assumes that no identity — be it an employee, a service provider, or a connected device — is inherently trustworthy. Every access request must be fully authenticated, authorized, and encrypted before access is granted, regardless of origination inside or outside the network or which resource is being requested.

Zero Trust is based on three guiding principles:

1. **Always verify** – Require authentication for every access request, every time, based on all available data points (e.g., user identity, location, device health, anomalies).
2. **Limit privilege** – Implement just-in-time and just-enough-access (JIT/JEA) policies to ensure each user is restricted to only the access they need to do their jobs.
3. **Assume breach** – Treat all access requests as malicious until proven otherwise.



¹ 2020 IDG Cloud Computing Study. IDG.

² Lance Whitney. "Cybercriminals targeting cloud services amid shift to remote working." TechRepublic. May 2020.

³ Avast Blog. "What Is Zero Trust Network Access?" Security Boulevard. May 2021.

An integrated approach to securing the modern enterprise

Edgile's information and cloud security approach shifts an organization's viewpoint from a purely risk-centric function to a hybrid risk and business-aligned capability, turning security into a strategic business enabler for the enterprise. Accordingly, we've developed a comprehensive and holistic approach for organizations looking to move from a perimeter-based security concept to a Zero Trust framework.

Our integrated solution leverages strengths from two principal leaders in our partner network: Microsoft and SailPoint. SailPoint is a leader in Identity Security and Microsoft is a leader in Access Management, according to Gartner MQ.



Founded in 2001, Edgile is a strategy-first risk and security advisory services firm offering a full suite of consulting services - including strategy, implementation, training, and managed support - to help large organizations in a variety of industries solve complex security challenges.

Gold Microsoft Partner



We partner with Microsoft to offer a low-risk, low-cost rapid implementation service that can leverage your existing investments in Microsoft 365 Azure Active Directory (AD) and a proxy server to modernize cloud and legacy on-premises applications and achieve Zero Trust. Our strategy goes beyond technology product deployment by using a comprehensive method that also manages people, processes, threat signals, and data across your enterprise. This enables your stakeholders to understand the “why” of security and compliance and how it relates to the risk framework, which can ease some of the burden on your IT operations.



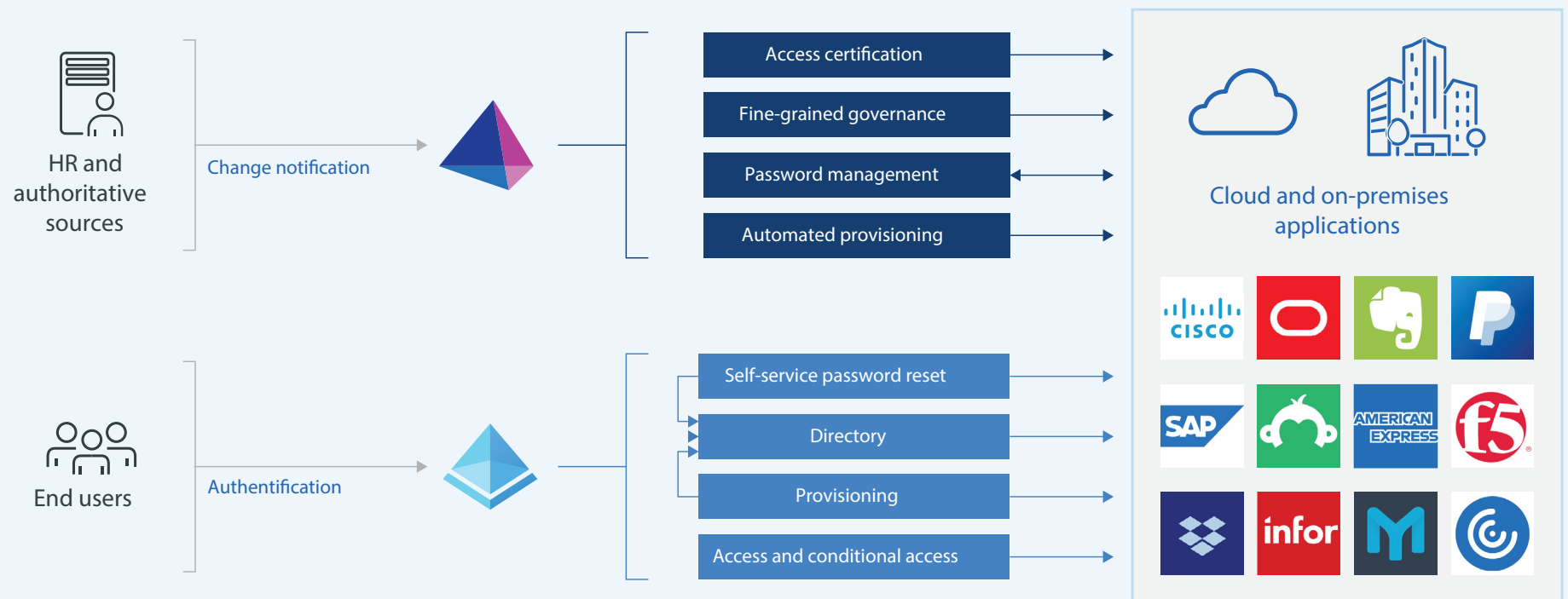
Identity security is at the core of Zero Trust and identity governance. As the fastest-growing, independent identity security provider, SailPoint helps global organizations securely and effectively deliver and manage user access to data and applications residing in the datacenter, on-premises, on mobile devices, and in the cloud. We work with SailPoint to help you integrate core services including identity governance, provisioning, and access management, on-premises and from the cloud.

Blueprint for Zero-Trust success

Our unified approach brings together SailPoint's identity security capabilities and Microsoft's Azure AD identity and access

management services to bridge the gap among cloud, external identities, and critical systems.

Microsoft + SailPoint best practices architecture



This high-level blueprint provides an overview of the solution architecture for a typical implementation.

Process overview

1

SailPoint provides the identity security and governance foundation, tapping into your organization's source of identity data and governance policies (often human resources). SailPoint automates lifecycle management processes (joiner/mover/leaver) and enables the ability to report and certify who has access to what.

2

Leveraging the power of artificial intelligence and machine learning, automation is applied to ensure people have the appropriate access based on their roles and that any changes in privilege are immediately detected and addressed. This fine-grained governance helps drive the Zero Trust model.

3

SailPoint synchronizes passwords for non-federated applications, giving users frictionless access from the beginning.

4

SailPoint's provisioning integrates with Microsoft's Azure AD to provide an intuitive dashboard interface for seamless sign-in, password reset, and access to approved applications and use of the Microsoft Portal for single sign-onv (SSO).

5



Microsoft controls the authentication process and either grants access or triggers conditional access based on several parameters such as type of identity, threat, application to access, network to access, threat and security vectors, and type of data to be accessed.

6

End users can also be invited and authenticated by Microsoft for self-service password reset and immediate access to approved applications.

Any business, any industry, any goal

Our integrated solution can be customized to suit your unique needs and supports a variety of B2B and B2C scenarios.

Goal:	Approach:			
Provide simple, secure, SSO access to customer-facing apps with social or business IDs	 Azure AD integration	 Connect with existing systems	 Connect to a store	 Migrate existing users
Customize the user journey with data exchange among various systems, identity proofing, etc.	 SSO to customer apps	 Social accounts	 Use your own branding	 Open standards
Allow apps to be securely accessed by customers, partners, and employees	 Native sign-in experience	 Workflows	 Enrich user journeys	 Customize with HTML and CSS
Migrate existing customer accounts to a new cloud-based solution and provide a seamless user experience	 Conditional branching	 B2B collaboration	 Compliance	 Security
Protect access to apps from advanced threats	 Identity experience framework	 Smart lockout protection	 Multi-factor authentication	 Security reporting
Comply with industry regulations and national data protection laws	 Self-service capabilities	 Audit and login reports	 Custom attributes addition	 Scale to millions of users

Customer story: Multilateral development bank

The bank is a source of international development financing, supporting economic development, social development, and regional integration by lending to governments and government agencies, including state corporations.

The need

Upon modernizing and moving critical processes to the cloud, the organization recognized the need for more robust, sophisticated identity governance and access management. They sought a simple yet secure solution that would meet this need while providing a seamless experience for internal and external users — in a single, unified platform.

The solution

Already a Microsoft Azure AD customer, the bank partnered with Edgile to take advantage of our integrated framework to better manage and protect several critical applications. These included partner, vendor, and ex-employee portals that handle sensitive banking transactions, as well as an event management website serving financial leaders from 48 countries.

Solutions applied:



**Azure
External Identities**



**Azure AD for
Access Management**



**SailPoint Identity Security
Platform for identity
governance and control**

The results



• Cost savings

- Implemented cost takeout from another product
- Moved into true customer identity and access management (CIAM) as a service, resulting in minimal cost and time required to manage infrastructure



• Identity transformation

- Created holistic platform for identities
- Provided immediate productivity for customers
- Delivered seamless end-user experience



• Enhanced security

- Mitigated the risk of external identities in internal systems
- Eliminated the need to manage external users' passwords and identities

Trust is a vulnerability

Zero Trust flips traditional cybersecurity approaches upside down. Rather than establishing trust and protecting the perimeter from outside threats, trust is completely eliminated, and protection is ubiquitous.

Edgile's integrated approach to Zero Trust can help you:

- Secure workforce access to cloud and on-premises applications in minutes instead of weeks
- Ensure that only the right users have access to the right applications
- Mitigate internal and external risk of threats



See how our integrated approach to Zero Trust
cybersecurity can help secure your enterprise.