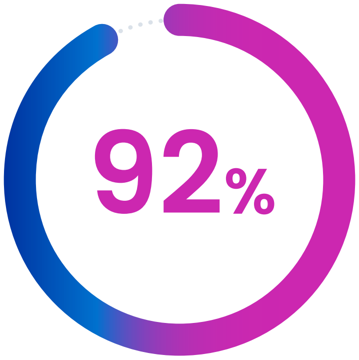
eBook

Identity Security: An Essential Piece of Your Zero Trust Strategy

There has never been a more challenging time to manage cyber risk and respond to the challenges of an ever-changing business landscape. Some of the challenges include:

- A sharp increase in the number of remote workers and non-employee workers
- More types of users, non-human entities, devices, and data sources to manage and protect than ever before
- The steady migration of applications and workloads to diverse cloud and hybrid infrastructures
- Cloud services with different identity models (e.g. more inherited roles and permissions)

This explosion of cloud computing, mobile, IoT, DevOps, bring-your-own-devices (BYOD), and work-from-home initiatives have led to the de-centralization of IT. Increased adoption of mobile and cloud technologies means that more business operations are now conducted outside the corporate network. An increasing number of users are accessing resources such as applications and business systems from a wide range of devices and locations. With cybercriminals relentlessly attempting to compromise user accounts in order to gain entry, organizations have shifted their security perimeters to focus on workers – including employees, contractors, partners, vendors, suppliers, and non-human bots. This is the basis of identity security: Enabling the right access while continually protecting the business. And this is why many organizations are employing identity security as the foundational component to their Zero Trust Security program.



companies are planning on implementing a Zero Trust security model.[1]

[1] Zero Trust Adoption Accelerates to Manage work from Home Risks, August 2021

Zero Trust is More than a Security Solution. It's a Strategy.

Zero Trust is a security framework that aims to enable an organization's digital business while ensuring data security integrity by providing exactly the right access to the right individuals through the right authority. For this reason, identity security is an essential piece of an effective Zero Trust strategy. In fact, the vitality of a Zero Trust architecture relies on the integrity of identities, the effectiveness and strength of access control policies, and the continuity of governance over identities and access across a hybrid IT environment.

Zero Trust Security Starts with Identity Security

Zero Trust Security is based on the notion of "never trust, always verify" and "assume the breach." What this means in practice is that no one should automatically be trusted to access resources, whether inside or outside of an organization. Essentially, every user is considered suspect until proven safe. When all network traffic by default is untrusted, the only viable security strategy is one built on identity.

A successful identity-centric Zero Trust model relies on the principle of least privilege, ensuring that all users have the least amount of access to do their job successfully — no more, no less. This requires not just knowing who has access to what, but more importantly who should have access and under what circumstances.

According to a recent IDSA report, nearly all (97%) IT security experts agree identity is a foundational component of a Zero Trust security model.[2]

So identity security plays a critical role in the success of any Zero Trust program. Identity security means having technologies in place that automate the identity lifecycle; manage the integrity of identity attributes; enforce least privilege through dynamic access controls, role-based polices, and Separation of Duties (SoD); and continuously assess a range of signals to govern and respond to access risks using advanced technologies such as AI/ML.

[2] 2021 Trends in Securing Digital Identities.

Implementing a strong and comprehensive identity security program enables organizations to manage and govern access for all types of digital identities so you can establish a Zero Trust framework that is able to systematically adapt and respond to the ongoing changes across the organization and threat landscape. Key principles include:

- **Never Trust, Always Verify:** Enable accurate access decisions to be driven with contextual, up-to-date identity data.
- **Deliver Just Enough, Timely Access:** Enforce least privilege using roles and complex policy logic.
- **Continuously Monitor, Analyze and Adapt:** Keep security up-to-date and dynamically respond as changes happen and threats are detected.

Finally, Zero Trust is a holistic security solution. This means your Zero Trust architecture should include Zero Trust Network Control (ZTNC), Privilege Access Management (PAM), and Access Management, as well as identity security – all communicating and working together to secure your complex hybrid environment.

Never Trust - Always Verify

Historically, organizations only had to manage closed and relatively static environments. Anyone on a network was deemed safe once proper login procedures authenticated the user; trust would then automatically be granted. But as network perimeters dissolved and cloud resources began to be adopted, a slew of new identity types (such as contractors and partners) became increasingly important. And this meant IT and Security teams had to fundamentally rethink the way they protected the business.

Thus, the first tenant of a Zero Trust strategy – Never Trust. But this begs the question: How can companies operate if they never trust their users accessing company resources? The answer is that they must verify the user is who they say they are. For most organizations, this means having a strong access management strategy and solution. Single sign-on (SSO) and multi-factor authentication (MFA), of course, are critical security components but they don't fully authenticate a user — they don't verify that a user is who they say they are. To do that (and therefore allow the user into your circle of trust), it's essential to consider all attributes, specifically contextual and up-to-date identity data.

To generate the identity visibility needed to drive accurate access decisions; organizations should have the following:

- **Complete Visibility:** Build a 360-degree view of all user types and their related access – including all permissions, entitlements, attributes, and roles.
- **Single Source-of-Truth:** Create clean, accurate identity records that all access decisions are based on.
- **Data Integrity:** Continuously keep identity data fresh and up-to-date with automated identity lifecycle management.

It is one thing to say “Never Trust,” but in order for organizations to operate, trust is not optional. By going beyond simple authentication decisions and using a complete identity record for each user — including permissions, entitlements, attributes and roles – organizations can confidently grant access when needed.

Deliver Just Enough, Timely Access Through Least Privilege

If the first tenant of Zero Trust is never to trust automatically, the second is to always default access granted to the lowest amount — known as “Least Privilege.” While this concept is easy to understand, implementing it at scale in a growing and ever-changing business environment is extremely difficult and very complex.

This is where roles and role-based access controls (RBAC) play a critical part in always ensuring that users have the access they need without imposing undue risk on the organization. Organizations that have clearly defined and detailed roles for access are able to easily assign, adjust, and remove access without the risk of one-off access assignments that are often missed, and most times never removed. In addition to roles, a dynamic access policy logic is required in order to avoid toxic access combinations that can lead to over-provisioning and even fraud or theft. For example, ensuring users who have access to procurement systems do not also have permissions within adjacent accounts receivable systems that could result in unscrupulous employees siphoning off corporate funds via fraudulent purchase orders.

of companies still rely on manual processes to adjust access.[1]

So how do organizations deliver just enough, timely access while maintaining least privilege?

- **Secure Access Controls:** Grant just-enough access using roles, fine-grained entitlements, permissions, and dynamic rules.
- **Access Automation:** As new users are created or roles change, access is automatically granted and updated based on access policies. To reduce risk exposure, unused access, and dormant accounts are automatically de-provisioned.
- **Ongoing Safeguards & Separation-of-Duties:** Detect and prevent toxic access combinations to avoid potential fraud or theft.

Continuously Monitor, Analyze, and Adapt

While many organizations have been able to successfully adopt the principles of Never Trust and Least Privilege, the challenge is making sure their Zero Trust model stays relevant and can accommodate all changes occurring inside and outside of the network. All too often, organizations fall into the trap of “set it and forget it” instead of actively monitoring, governing, and adapting their access policies and controls. This often happens because organizations are overwhelmed with the amount of identity data generated and lack the internal expertise needed to properly maintain their Zero Trust strategy.

Identity data plays a crucial role in Zero Trust as it contains important information, such as identity attributes, access rights, access entitlements, behavioral data, and role and group memberships. But because of the volume of identity data available, it is beyond the scope of human ability to sort through all of this information manually. Analyzing vast amounts of identity-related data in order to adapt to changes in the organization and make correct access decisions requires the use of tools that leverage artificial intelligence and machine learning, as well as integrations with additional security systems that support their Zero Trust strategy.
By making use of identity data, organizations can then employ powerful strategies to keep security up-to-date and dynamically respond as changes happen and threats are detected:

- **Ongoing Access Monitoring:** Through AI-driven insights, organizations can get deep visibility and understanding of all user access, including trends, roles, outliers, and relationships.
- **Consistent Governance:** Measuring the efficacy of access controls for apps, data, and cloud resources ensures that permissions comply with policies.
- **Orchestration:** Constantly monitoring risk signals from the digital ecosystem and communicating with the Zero Trust gateway ensures real-time enforcement of security policies.
- **Extensibility:** By taking advantage of custom workflows, APIs, and event-triggers, organizations can automate their identity security program across other cybersecurity and access systems.

67% of respondents believe the use of automation and advanced technologies would increase their organizations’ ability to prevent cyberattacks.[3]

[3] Ponemon Institute: The Economic Value of Prevention in the Cybersecurity Lifecycle.

Zero Trust Requires a Holistic Approach

In previous sections we discussed ways that a Zero Trust strategy relies on different systems working together. This holistic security approach is critical to all Zero Trust deployments.

The Identity Defined Security Alliance (IDSA), a consortium of identity and security vendors, has developed a reference architecture (Figure 1) that provides a framework for understanding the different components for identity defined security.

The various types of "users" (at left) are seeking access to target resources, (data, at right). Different identity and security controls beyond identity management and governance (shown as discrete building blocks, center) all play a part in securing user access across devices, networks, infrastructure, applications, and data.

Identity Security solutions need to inform and integrate with complementary identity and security technologies to provide a complete Zero Trust security solution.

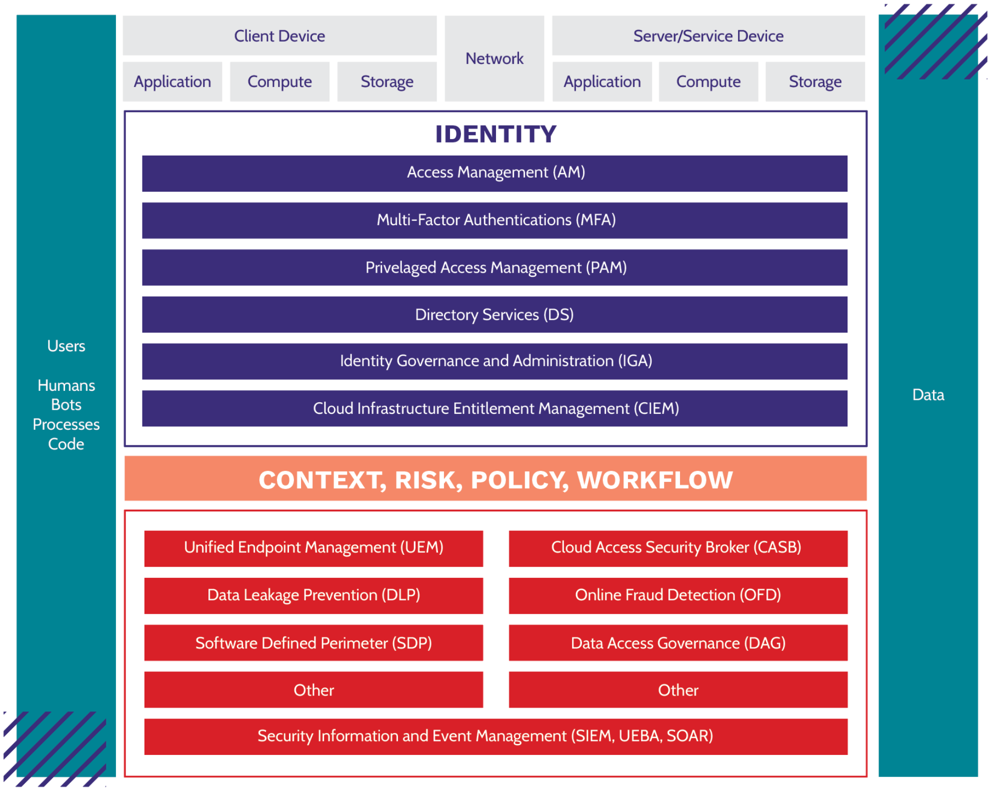

Client Device
Application
Compute
Storage
Network
Server/Service Device
Application
Compute
Storage
Users
Humans
Bots
Processes
Code
IDENTITY
Access Management (AM)
Multi-Factor Authentications (MFA)
Privelaged Access Management (PAM)
Directory Services (DS)
Identity Governance and Administration (IGA)
Cloud Infrastructure Entitlement Management (CIEM)
CONTEXT, RISK, POLICY, WORKFLOW
Unified Endpoint Management (UEM)
Cloud Access Security Broker (CASB)
Data Leakage Prevention (DLP)
Online Fraud Detection (OFD)
Software Defined Perimeter (SDP)
Data Access Governance (DAG)
Other
Other
Security Information and Event Management (SIEM, UEBA, SOAR)
Data

Figure 1. Identity Defined Security Reference Architecture[1]

[1] IDSA: The Guide to Identity Defined Security

Is Your Zero Trust Strategy Aligned with an Identity Security Approach?

This checklist can help ensure your Zero Trust strategy is aligned with an Identity Security strategy that will grow and adapt as your business and security needs change.

□ **Deploy an identity warehouse:** Create a centralized repository of identity data that provides full access visibility into and understanding of the identities of each of your users, non-human entities, devices, and data sources (including shadow IT).

□ **Implement strong access controls:** Use roles and access policy management to assign access to data and application resources only where it is needed and set SoD policies to avoid potential toxic access combinations.

□ **Follow the principle of Least Privilege:** Continuously review and adjust your users' identity entitlements and roles to ensure they have exactly the right amount of access to the right resources at exactly the right time.

□ **Monitor activity data:** Log what your users are doing with their access to your organization's resources and monitor those logs for suspicious behavior.

□ **Alert on activity data:** Flag suspicious access activity or changes to entitlements and alert the appropriate administrators.

□ **Remove unused access:** Automatically deprovision access that is no longer needed.

□ **Automate incident response:** Automatically modify or terminate access based on changes to a user's attributes or location.

□ **Orchestrate incident response:** Integrate your security and identity systems for a holistic view of security events that could indicate a potential compromise. Automatically perform remediation actions when risky activity is detected.

Take the Next Step

SailPoint Identity Security is the cornerstone of an effective Zero Trust strategy. The vitality of a Zero Trust architecture relies on the integrity of identities, the effectiveness and strength of access control policies, and the continuity of governance over identities and access – across your hybrid IT environment. As the leader in the identity market, SailPoint offers identity security technologies that automate the identity lifecycle; manage the integrity of identity attributes; enforce least privilege through dynamic access controls, role-based polices, and separation-of-duties; and continuously assess, govern and respond to access risks using AI/ML.

To learn more, visit **sailpoint.com/solutions/zero-trust**

SailPoint®

About SailPoint
SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.