IDENTITY & CYBERSECURITY

Why Identity Management is Critical for Zero Trust

In a recent Identity Defined Security Alliance (ISDA) survey, 97% of IT security experts agreed that identity is a foundational component of a Zero-Trust security model. In this Q&A, **Frank Briguglio**, a global public sector identity strategist for SailPoint, explains how state and local governments can pave the way for a strong identity management program.

Why is Zero Trust critical for state and local governments?

Digital transformation and IT modernization were already driving explosive growth in the data, applications, infrastructure and, most importantly, the identities organizations were managing. Then we had this rapid shift to a remote workforce during the pandemic.

As the complexity of secure environments — and the need for speed and accuracy — grows, Zero Trust becomes a good way to enable access to any hybrid or on-premises system. It becomes foundational to our security model.[1] And identity is a critical component of that model.

What capabilities are needed to apply a Zero-Trust approach?

Zero Trust is a team sport. It includes cross-organizational and vendor involvement within every pillar of the security ecosystem. The domains of Zero Trust include identity, data, devices and applications. When you look at all of the connection points between them, there's a lot to unpack.

Organizations have to start with a strong identity management program, because even with just the identity elements — which include things like directory services, identity governance and administration, multifactor authentication, access management and federation — there's no single vendor that does it all. Identity governance provides the context, risk policies and workloads for all those things I mentioned.

How can organizations get started on identity governance?

Beginning with the correct attributes about the user — those personal identifiers that distinguish one user from another — and understanding organizational policies and how you're going to enforce those policies is foundational to the Zero-Trust model. Those identity attributes are used to make complex access control decisions, so you need to ensure that data is up to date and provided in a timely manner during the runtime authorization process.

I recommend starting with the easier identity challenges — for example, identity life-cycle management and automation of basic provisioning functions — and then separation of duty controls and evaluation of different levels of access prior to provisioning or deprovisioning access.

What types of changes are necessary to support Zero-Trust access?

Implementing Zero Trust has a huge impact on IT strategy, compliance strategy and more. In some cases, internal organizations are now working together, where in the past they may have had no reason to do so. Overall, that affects the IT staff and the task they have. I recommend creating a Zero-Trust governance board — just as many agencies have an identity credentialing and access management team — that goes beyond traditional stakeholders to involve compliance, business and application owners.

SailPoint

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity™ platform. The platform is designed to securely accelerate mission objectives while delivering adaptive security and continuous compliance. SailPoint provides a comprehensive view of access to all resources across multi-cloud infrastructure, and helps make faster, more informed access decisions, detect potential risks and easily enforce access policies for all users.

https://www.sailpoint.com/identity-for/government

[1] https://www.idsalliance.org/white-paper/2022-trends-in-securing-digital-identities/