Balancing Zero Trust with a **Strong AI-driven Identity Strategy**

SailPoint

The impact of the latest cybersecurity breaches is staggering. With billions of identities and sensitive data compromised, it's clear that traditional security doesn't solve the problem.

Here's what the latest breaches show us: three out of 5 organizations expect to be breached.

On average, it takes an average of 74 days to find and contain a malicious actor, and 80 percent of breaches involve privileged credentials. Furthermore, 67 percent of companies breached could not produce a report showing who has access to sensitive systems and accounts within a 24-hour period. What this shows us is the perimeter as we know it is dead–we are the new attack vector.

The attack lifecycle continues to get advanced, from both internal and external threats using existing access and compromising the perimeter. Once inside malicious actors are able to elevate privileges perform reconnaissance and move laterally inside the network and disrupt business and extract data.

Here's where the Zero Trust Security concept comes in. Created by Forrester Research, it embraces a new model for access and treats all users as untrusted. It is a paradigm shift from traditional perimeter-based access to a model that is user-centric. Zero Trust is an integrated security approach for users, applications, data and networks that requires strong authentication principles, multifactor authentication, step-up authentication and the use of contextual access policies and interrogation.

In the Zero Trust model, cloud applications and security are looked at the same with the same importance as on-premises systems and applications. The model encourages the use of advanced analytics, artificial intelligence and machine learning for better detection of threats and breaches.

How can you enable efficient access without compromising security and compliance? Access is just one piece of the security puzzle. What the Zero Trust model does not clearly call out for is that in order to achieve the full effectiveness of Zero Trust is that enterprises must start with the identity of the user itself. There must be a strong identity governance and administration strategy in place.

The identity strategy should include:

- Identity governance controls for roles, entitlements, suitability and SOD policies and risk
- Lifecycle automation for all identities including employees, contractors, business partners, as well as RPA/bots
- Credential management and strong/multifactor authentication
- Privileged account and entitlement management
- Centralized application access and self-service fulfillment
- Access certification, auditing and reporting

Analytics provide rich context to access control decisions, enforcement of policies and detection of anomalous activity. An identity strategy provides simple and secure access and ensures that it's the right access efficiently. The strategy should define and govern access rights to minimize risk associated with entitlement creep, orphaned accounts and separation of duty and suitability policies. When properly implemented the solution will provide visibility to – Who has access to what? Who should have access? What do they do with that access?

Access management is critical in the Zero Trust model. Evaluating identity context during the authentication and authorization process ensures that a user is who they say they are, using the device they should be, accessing the network from an authorized location. Identity defines and grants the access they should have and removes any access that is unsuitable, inappropriate or no longer needed.

An identity strategy should include High Value Assets (HVA), sensitive and critical data, structured applications, unstructured data, hosts and networks. Cloud applications, on-premises applications should be centrally managed by the Identity platform and treated alike.

Here's how identity can help with a Zero Trust approach:

- Advanced analytics, artificial intelligence and machine learning provide valuable insight to all identity data and events
- Continuous evaluation and governance of assignments, policies and risk
- Identifying orphaned, potentially toxic, overexposed or unauthorized access, and
- Exposing behavioral and historical events that may identify risky behaviors or malicious intent.

Zero Trust is a concept. It's not a single product or solution. It is a paradigm shift in how we think about security. People are now the new security perimeter. Identity is the new firewall and should be at the center of any Zero Trust strategy.

To learn more about how an AI-driven identity can address your Zero Trust initiatives, visit **www.sailpoint.com.**

SAILPOINT: RETHINK IDENTITY

sailpoint.com

SailPoint, the leader in identity management, delivers an innovative approach to securing access across the enterprise with the SailPoint Predictive Identity™ platform. With SailPoint, enterprises can ensure that everyone and everything has the exact access they need, exactly when they need it, intuitively and automatically. Powered by patented Artificial Intelligence (AI) and Machine Learning (ML) technologies, the SailPoint Predictive Identity™ platform is designed to securely accelerate the business while delivering adaptive security, continuous compliance and improved business efficiency. As an identity pioneer and market leader serving some of the world's most prominent global companies, SailPoint consistently pushes the industry to rethink identity to the benefit of their customers' dynamic business needs.

Stay up-to-date on SailPoint by following us on **Twitter** and **LinkedIn** and by subscribing to the **SailPoint blog**.

EB1342-2003