Identity Governance
Addresses US Government Cybersecurity Frameworks

SailPoint

The impact of cybersecurity breaches is staggering – for example, in the 2016 Office of Management and Budget, Federal Information Security Act, Annual Report to Congress, federal agencies reported 30,899 information-security incidents, 16 of which met the threshold of being a major incident. With billions of identities and sensitive data compromised, it's clear that traditional security doesn't solve the problem. Cybersecurity threats now come in many different forms, from insiders, ransomware and malware to phishing – the list of ways into an organization's sensitive underbelly is growing. What this shows us is the perimeter as we know it is dead – the identity is the new attack vector.

Modern security architectures and frameworks such as Zero Trust Architecture (ZTA) and the NIST Risk Management and Cybersecurity Framework (CSF) attempt to address and manage cyber threats. This modernization requires a system of interconnected components working together to efficiently and confidently grant appropriate policy-driven access and identify known and unknown threats and to prevent or limit the damage done by nefarious actors.

The ZTA security concept embraces a new model for access, which is a paradigm shift from traditional perimeter-based access to a user-centric model. For people, non-person entities, systems, assets, and data that requires strong authentication principles and the use of contextual access policies and interrogation, the use-centric model delivers an integrated security approach.

The ZTA approach for addressing cybersecurity threats follows the CSF Functions: Identify, Protect, Detect, Respond, and Recover. These Functions are the highest level of abstraction included in the cybersecurity framework. They act as the backbone of the Framework Core that all other elements are organized around (e.g., NIST 800-53 Security Controls). Within each function Identity Governance and Administration (IGA) plays a key role in keeping technology resources and data secure - over **3 dozen ways as a matter of fact.**

What Identity Governance Provides

Identity Governance provides deep insight and visibility into: Who currently has access? Who should have access? Is the access appropriate? and, How the access is being used?

Identify – a comprehensive view of enterprise systems, people, assets and data and the relationship or context related to cybersecurity risk for systems, assets, and data.

Protect – a model-based – Role, Attribute, Policies, Risk – approach to provisioning and access control ensuring that access is authorized and appropriate and that only necessary access has been granted to systems, assets, and data.

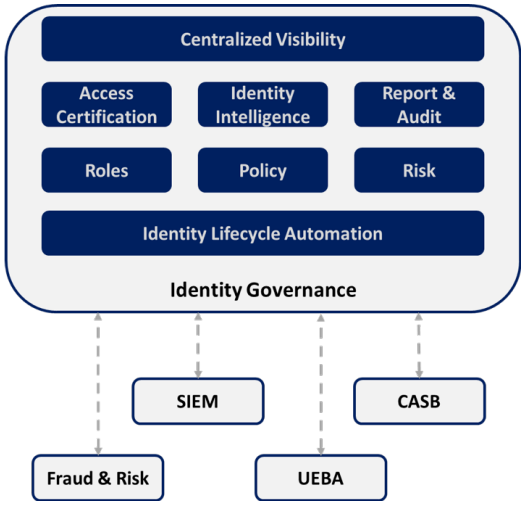
Detect & Respond – extends the Detect & Respond function areas by providing the baseline of what a user's access should look like or which activities they can perform. Identity analytics provide visibility into unauthorized access, over entitled and risky users and systems, assets, and data. Identity metadata provides contextual information and enriches security event analysis to validate and identify compromised or rogue users significantly reducing noise for security operations analysts.

Recover – provides business process automation and workflows to ensure that all access is authorized, appropriate, and suitable and removed when no longer valid or required.

NIST Cybersecurity Framework

The Role of Identity Governance

Identity Governance defines and grants users access they should have and removes any access that is unsuitable, inappropriate or no longer needed. Identity Governance is critical in the ZTA model and prescribes the same principles of access control as defined in the cybersecurity framework. A model-based approach – Attribute (ABAC), Role (RBAC), Risk, and Policy – defines and governs access rights to minimize risk associated with entitlement creep, orphaned accounts, separation of duty and suitability requirements. By evaluating identity context during the authentication and authorization process, this ensures that a user is: *who they say they are; using the device they should be; and accessing the network from an authorized location*.



Cyberattacks are malicious behaviors that uses stolen credentials to gain access to systems and sensitive data for the purpose of downloading or transferring data for exfiltration. To be in a better position to deter, detect, and mitigate a cyberattack, the goal of the CSF is to guide organizations on how to make their cyber threat programs more robust.

As prescribed by the CSF, the security approach involves efficient user activity monitoring, analytics, and incident response. These capabilities are typically deployed as an integrated capability of Security Orchestration, Automation and Response (SOAR) systems.

In order to gain meaningful identity Governance insights, the process of data enrichment adds contextual information to security event data.

Security events can be enriched with contextual information from IGA systems, geolocation tools, threat intelligence, and a host of other sources.

Enriched data allows security operations to better perform threat detection, threat hunting, and incident response. As anomalous activity is identified, the SOAR system sends an alert to the security operations center analysts who then uses the data to examine and remediate the threats.

Depending on the severity of the event, the security analyst (or an automated trigger) can send the event alert directly to the IGA system, which triggers an automated lifecycle event such as disabling or removing access or an access certification.

An integrated Identity Governance solution can:

- Help with modern security architecture and frameworks
- Ensure appropriate access is granted timely and efficiently
- Initiate identity, application, or entitlement-based certifications
- Enrich security events with contextual identity information
- Use continuous monitoring to gain insight into events and behaviors that move into and through your cloud environment
- Leverage security orchestration automation and response (SOAR) technologies to auto-remediate events - automatically disable or remove access from identities
- Reduce noise in your environment

Identity-defined Zero Trust touches almost every aspect of an organization's IT and security infrastructure. Forward thinking organizations are achieving Zero Trust through the integration of existing identity and security technologies. Additionally, they have implemented architectures that share identity context and provide risk-based access to critical resources, improving security without compromising compliance with government directives, standards and frameworks.

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.

EB1340-2002