SAILPOINT | UBERETHER IAM ADVANTAGE PARTNER

Visibility: The key to a strong compliance posture

Gaining visibility and control over user access is essential for tackling the current challenges in cybersecurity

Frank Briguglio | SailPoint

Government agencies are confronted with a range of security guidelines, such as the Executive Order on Improving the Nation's Cybersecurity and the National Institute of Standards and Technology's Cybersecurity Framework. In addition, new mandates for protecting privacy and data are driving the need for agencies to adopt stronger cybersecurity controls.

Achieving those complex goals starts with visibility. Agencies need a clear picture of who has access to a government system, what they have access to, how they received that access and what they're doing with it. Once agencies have that level of visibility, they can better control what users are able to do on their networks.

Establishing a governance process for user access

SailPoint provides a solid foundation for visibility and access control. IdentityIQ, our identity and access management (IAM) solution, offers a comprehensive approach to managing user access across the IT environment. Its primary purpose is to ensure that the right people have the right access to the right resources at the right time so that agencies can maintain security while facilitating mission activities.

IdentityIQ institutes identity governance through automated provisioning, deprovisioning, entitlement management and policy enforcement to make sure a user's access aligns with his or her role in the organization. By establishing a governance process for user access, IdentityIQ enables agencies to remain compliant with the government's regulatory requirements.

In addition, IdentityIQ supports risk-based policies that give agencies the ability to identify potential risks or anomalies in user access. This critical feature for security operations can help agencies detect potential breaches or misuse of access privileges. Because it monitors user behavior, IdentityIQ can quickly detect any suspicious changes and take appropriate action to limit or block a user's access.

Streamlining and simplifying IAM

SailPoint is proud to be included in UberEther's IAM Advantage solution. Our technology forms the governance layer for web access management or privileged access management solutions to verify that a particular user should continue to have access to specified resources. We reach down into the authoritative data to build policies and visibility for compliance throughout the IAM Advantage stack.

SailPoint can also detect, classify and tag data within an agency's IT environment. We can use the attributes and the identity context to build an access model for data, and we can create that same visibility and access model for cloud-based users, workloads and data as well.

Our goal is to streamline and simplify IAM so that agencies can maintain compliance, mitigate risks and enhance operational efficiency. ■

Frank Briguglio is federal CTO at SailPoint.