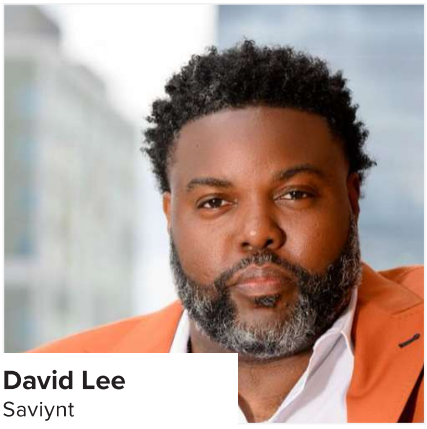
SAVIYNT

A unified way to manage identity security

An end-to-end, cloud-native, AI-powered identity security platform minimizes risk by bringing diverse tools and activities under one roof



David Lee
Saviynt

The shift to the cloud has been revolutionary for government. When data and workloads are in the cloud, agencies gain benefits in terms of scalability, security and costs, and they have access to new technologies faster. There are risks, of course, as there are in any IT environment, but issues often arise from how those cloud assets are managed.

Misconfigurations, overly broad access and gaps in visibility can create opportunities for attackers. In addition, sensitive data is at risk if encryption, compliance requirements or storage settings aren't properly addressed. On top of that, insecure APIs, legacy applications and third-party integrations expand the attack surface in ways that are easy to overlook.

At its core, keeping cloud environments secure hinges on a partnership between agencies and cloud providers to ensure that strong identity governance, disciplined configuration management, and continuous monitoring are in place and enforced.

End-to-end control over identities' lifecycles

The way agencies manage user identities has a big impact on security. Identity governance and administration (IGA) is a particularly effective approach because it directly addresses the core risks in the cloud—misconfigurations, excessive permissions and lack of visibility. IGA gives agencies end-to-end control over identities' lifecycles by enabling them to confidently answer the question: Who has access to what—and why?

IGA, a branch of identity and access management, encompasses the security processes that govern and manage identities. IGA validates requests upfront and ensures that access is provisioned in line with the organization's policies. Entitlements are continuously certified, and access is quickly revoked when it's no longer needed.

A robust IGA platform will secure human and non-human identities while automating the processes associated with application and data access, allowing security teams to streamline activities, ensure ongoing compliance and reduce organizational risk.

In a cloud environment where roles and permissions can multiply quickly, IGA provides the governance and oversight necessary to prevent toxic combinations of access, minimize the attack surface, and keep security aligned with business and compliance requirements.

Unified governance across all environments

The Saviynt Identity Cloud brings all those activities under one roof. We unify

governance across all environments—on-premises, cloud and hybrid—through a connector framework that talks to an agency's apps. A normalized identity schema makes sense of messy data, and unified risk analytics are baked into our cloud-native architecture from the start.

As a result, agencies no longer have to juggle multiple siloed tools, and the security gaps from point solutions are eliminated. Instead, agencies have one place for consolidated visibility, consistent controls and smarter decisions—whether their apps live on premises, in the cloud or somewhere in between. That means a reduced attack surface, faster compliance, operational consistency across the board and lower total cost of ownership.

No matter the identity—human, non-human, privileged or AI—Saviynt unifies identity governance, granular application access and privileged access, and it is the only cloud-architected, cloud-deployed IGA platform that has achieved a FedRAMP Moderate authority to operate. It is also built to meet the stringent security requirements of the Defense Department's Impact Level 5, which means our solution ensures the highest levels of protection for controlled unclassified information and national security systems.

The Saviynt Identity Cloud eliminates the struggle of keeping dozens of moving parts in sync, instead providing agencies with an identity ecosystem that functions as a single, easily managed system. ■

David Lee *is field CTO at Saviynt.*

"A ROBUST IDENTITY GOVERNANCE AND ADMINISTRATION PLATFORM WILL SECURE HUMAN AND NON-HUMAN IDENTITIES WHILE AUTOMATING THE PROCESSES ASSOCIATED WITH APPLICATION AND DATA ACCESS."