

How an Identity-Centric Strategy Can Drive Government Security

Identity is key to a modernized government experience. As a means of protecting IT systems, identity security also supports a smooth, simplified and secure employee experience.

Externally, a coherent and deliberate approach to identity can help drive improved constituent engagements, meeting rising citizen expectations around their government encounters.

"Identity's not just the credential we use to represent ourselves. It's the metadata that makes up the identity. That's what makes it so important as the foundation of zero trust," said Frank Briguglio, Public Sector CTO of SailPoint. He spoke during a recent GovLoop panel discussion with government and industry executives.

govloop SailPoint Deloitte.

A Complex Security Landscape

Many federal agencies still struggle to implement effective identity management as they seek to secure systems while supporting a seamless user experience.

Data accuracy: Data drives security; information about devices and end users can be used to design and implement identity-based safeguards. Yet accurate data is not always available, "and without data accuracy, zero trust doesn't work," Briguglio said.

Hybrid work: With the rise of remote and hybrid work, traditional identities aren't enough. "I have to better secure my infrastructure and my resources, so that I'm not dependent on a physical location," said Rebecca Nielsen, Specialist Leader or Risk & Financial Advisory at Deloitte.

Lack of coordination: In an increasingly interconnected IT environment, it's no longer practical to take a siloed approach to security. "Cyber is now a team sport," Briguglio said. The engineering team, the application owner, the compliance officer, the data officer – "all these people have to be in unison."



Key Terms in Identity Security

Business role: Business roles define the desired state of a user's access – what do we want someone with this job function to be able to do, or not do? Using business role, access can then be assigned to users based on their functions within the organization.

Entitlement: Permissions granted within a computer system, such as access to files and folders or access to certain parts of websites. Entitlements also define the actions a user is allowed take against those identified items.

Identity profile: Instructions for creating and managing identities from the associated authoritative sources. These instructions determine a variety of security settings around such functions as provisioning and access, with the ability to adapt access as roles change.

Recommendation engine: An AI service that uses peer group analysis and identity attributes to recommend access to users and help certifiers decide whether access requests should be approved.

Integrated identity: Creates a common link across environments, applications, devices, APIs and data. An identity program integrates with data, cloud and DevOps, enabling business transformation and technology innovation. Algorithms will detect attacks and calibrate responses based on common identity linkage, reducing enterprise risk.

Dynamic trust: A model where access evolves based on an identity's behavior and interactions, just as humans learn to trust each other. Artificial intelligence will understand interactions across environments and adjust each identity's access accordingly.

Key Elements of an Identity Security Solution

What are some of the key characteristics of an effective approach to identity security?

Centralized identity management: Agencies need a strong understanding of users' responsibilities and authorities. "Centralized identity management is an ability to verify those users' identities when they attempt to access the system," said Kenneth Myers, Director of Identity Assurance and Trusted Access Division for the General Services Administration Office of Government-wide Policy.

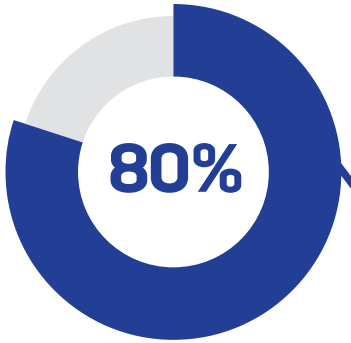
A user-centric model supporting zero trust: In zero trust, the focus shifts from the physical perimeter to data, devices and users themselves. "Is Frank suitable for the access that he's trying to use? Is he really a privileged user?" Briguglio said. "All of this comes from a very mature identity ecosystem."

A risk management approach: IT leaders need to know what the threats are and where they come from. This applies to identity management, too: understanding how personal attributes are assigned and validated. "It all comes down to risk management," Nielsen said.

Unmatched intelligence: Leverage artificial intelligence and machine learning to provide 360-degree visibility, insight and remediation so you can adapt and ensure the security of every identity.

Comprehensive integration: Extend your ability to embed identity context across your hybrid environment and centrally manage and control access to all data, applications, systems and cloud infrastructure – for all identity types.

By the Numbers



Around 80% of all data breaches occur as a result of weak or stolen passwords.

$36.96

The market for identity and access management tools is projected to reach $36.96 billion by 2030.

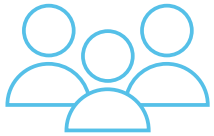
72% Ease of Integration

62% End User Experience

61% Product Performance and Effectiveness

Organizations prioritize ease of integration (72%) in identity and access management solutions, followed by end user experience (62%), and product performance and effectiveness (61%).

Best Practices in Identity-Centric Security



Have a Dedicated Identity Team

Agencies need a dedicated identity security team, "whether that's a cross-functional team, whether that's an operational team," Myers said. "There's one structure in place."

A dedicated team can help ensure consistent governance. That core team supports centralized identity management, ensuring there is "a holistic view of users, with a strong understanding of their responsibilities and authorities," he said.



Start With an Inventory

To apply effective identity-based security controls, agencies first need to know what they're protecting and from whom. In addition to taking stock of systems and data stores, "you have to identify the different types of users," Briguglio said. "That allows us to build an access model."

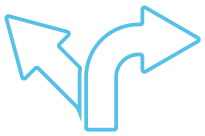
In turn, that model should be tailored such that the individuals have access only to the systems they need to do their jobs, and the data they are entitled to see. "It all falls in line with that concept of identifying, and then protecting and then detecting any anomalous access attempts," he said.



Use the Right Tools

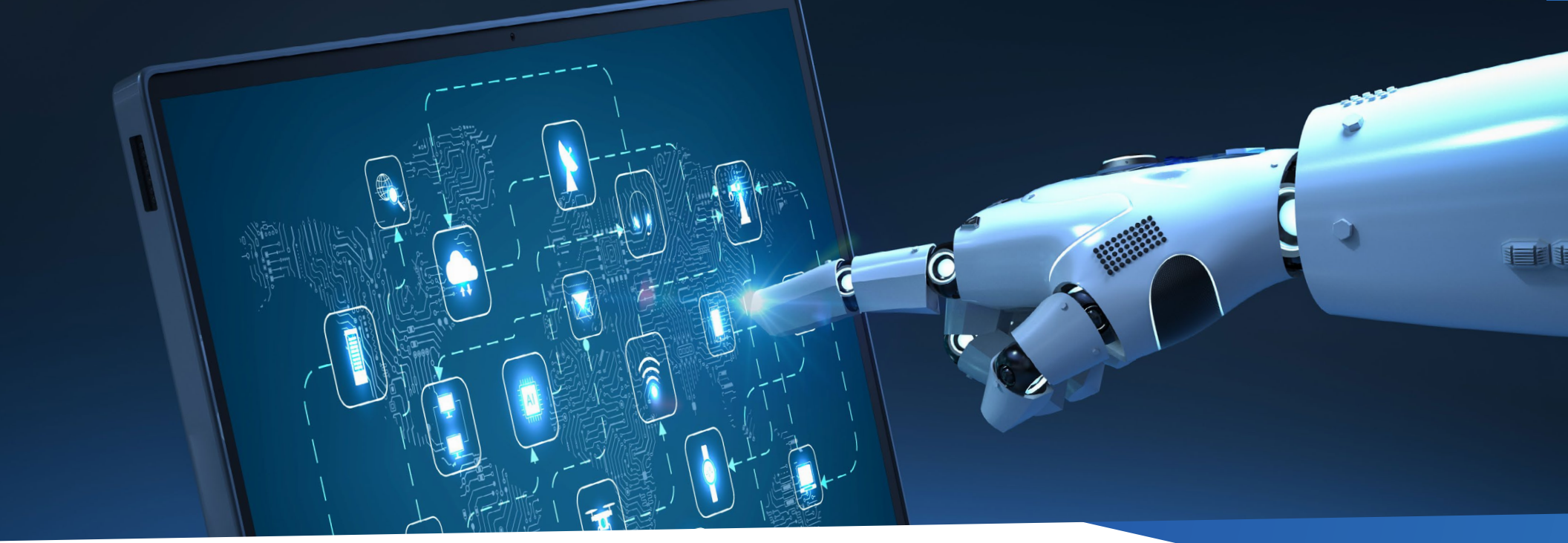
With a wide range of identity-management tools available, it's important to ensure you're using the correct tools for a given requirement. Nielsen pointed, for example, to the use of a dynamic access model that can make real-time decisions about access on an individual level. If the rules around that are tool complicated, "it might make sense to keep that particular resource using a more traditional provisioning model."

She added: "It's really important to look at all of these things and think of them as tools in a toolbox. Using the right tool for the right job ... is really critical and something we should all pay attention to as we move forward."



Pivot From Manual Processes and Reporting

Relying on manual segregation of duties (SoD) controls, manual provisioning and emergency access contribute to many potential points of failure and doesn't guarantee compliance. Agencies can see benefits to automating with audit-ready, actionable reports and bandwidth to focus on riskier users and other vital initiatives.



Deep Dive: The Need for AI, Automation

As agencies pivot to cloud infrastructure and Software as a Service (SaaS) applications, they face challenges around the sheer scale of the cybersecurity need. “Identity is becoming a problem that’s not human-achievable,” Briguglio said.

“To solve the visibility that we need, the types of queries that we need to grant that dynamic access – that is not a human-readable query,” he said. “It's going to require compute power.”

Automation, supported by artificial intelligence (AI), makes the task manageable. To begin, every agency should automate “how they onboard a new employee and contractor, and grant them access to the things they need to do their job on Day One,” he said.

Automation also helps with change management, as roles and responsibilities evolve. “We all end up being over-entitled; we get more entitlements and typically they don't go away. We don't relinquish them on our own: We wait for someone to take them away,” Briguglio said. Automation can close that gap.

Critically, automation can also support the effort to get users off the system when they leave the agency. “When someone leaves, it's time to disable them, remove all of their access. Rather than make this a manual process, it makes sense to have it happen automatically," he said.

AI, meanwhile, is a powerful ally when it comes to role modeling and access modeling: the behavior analytics and peer group analyses that feed an effective identity-centric strategy. “It's allowing us to develop products that will get to our ultimate goal: autonomous identity,” he said.



How SailPoint Helps

SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with all identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time–matching the scale, velocity and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous and integrated solution puts identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.

How Deloitte Helps

Deloitte Government & Public Services is committed to improving public outcomes through a focus on people. Deloitte provides agencies with fresh perspectives that help them anticipate disruption, reimagine the possible, fulfill their mission objectives and develop relevant, timely and sustainable solutions.

Thank you to SailPoint and Deloitte for their support of this valuable resource for public sector professionals.



About SailPoint

SailPoint is the leading provider of identity security for the modern enterprise, empowering organizations worldwide to put identity security at the core of their business. With a foundation of artificial intelligence and machine learning, SailPoint identity security delivers the right access to the right identities and resources at the right time.

Learn more about SailPoint here.



About Deloitte

Deloitte Government & Public Services is committed to improving public outcomes through a focus on people. At Deloitte we think about the complex issues facing the public sector and develop relevant, timely, and sustainable solutions for our clients.

Learn more about Deloitte here.



About GovLoop

GovLoop's mission is to inspire public sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to the public sector.

For more information about this report, please reach out to info@govloop.com.

www.govloop.com | @GovLoop