SecurID™

Improving the Nation's Cybersecurity

Make Identity Part of Your Plan

Identity: The Common Denominator in Zero Trust, Cloud Security and Multi-Factor Authentication

Woven throughout the 2021 Executive Order on Improving the Nation's Cybersecurity are prominent references to zero trust, cloud security and multi-factor authentication (MFA)—areas that support achieving the goals of modernizing government cybersecurity and enhancing supply chain security.

These three diverse aspects of cybersecurity have one thing in common: identity.

On the following pages, you'll learn how identity and access management (IAM) delivers the zero trust, cloud security and MFA capabilities your organization needs to achieve critical national cybersecurity goals.

Identity and access management (IAM) enables the capabilities needed to achieve critical national cybersecurity goals.

Zero Trust: Part of a Modern Approach to Government Cybersecurity

The federal government has been exploring the concept of zero trust as an element of cybersecurity since at least 2019, when the National Institute of Standards and Technology (NIST) published its first draft of Special Publication 800-207 on zero trust architecture. Two drafts later, the 2020 final version defined zero trust as a cybersecurity paradigm in which trust—in a user, device or other entity—undergoes constant reevaluation. In the 2021 executive order on improving cybersecurity, advancing toward zero trust is one of the main modernization goals for government cybersecurity.

The role of identity in zero trust

"Who are you, and what do you want access to?" are the first questions IAM asks of a user, device or other entity asking to be trusted with access to resources. An environment of zero trust poses the same questions, but the answers are subjected to constant reevaluation. To support zero trust, an IAM solution must have capabilities that enable the ongoing evaluation of trust, such as:

Role-based access control, attribute-based access and conditional access

Risk-based analytics, as part of a policy engine for dynamic access decisions

Governance-focused access driven by constant visibility into identities and access

Learn more about zero trust and how SecurID can help you adopt a zero trust approach to security.

NIST defines **zero trust** as

> "a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated."

Source: NIST, SP 800-207, "Zero Trust Architecture"

Cloud Security and the Modernization of Government Cybersecurity

Following "historic" growth in federal cloud migration in 2020, **continued expansion** is expected, as government continues to prioritize securing the IT infrastructure while also controlling costs. That expectation is consistent with the 2021 executive order, which calls for accelerating movement to secure cloud services and making zero trust architecture (see previous page) part of the migration to cloud technology. The Federal Risk and Authorization Management Program **(FedRAMP)** helps agencies use cloud services securely by providing a standardized approach to security authorizations for cloud service offerings.

IAM in the cloud

Cloud security is about protecting cloud-based data, applications and infrastructure, and IAM is critical to that effort. It's about ensuring the right people have access to the right resources in the cloud—and the wrong people don't. IAM solutions for the cloud should make this aspect of cloud security not just achievable, but *easily* achievable, so that the security team is unencumbered in its pursuit of the agency mission. That requires cloud IAM that delivers:

Documented high availability (99.99%) to help ensure solution reliability

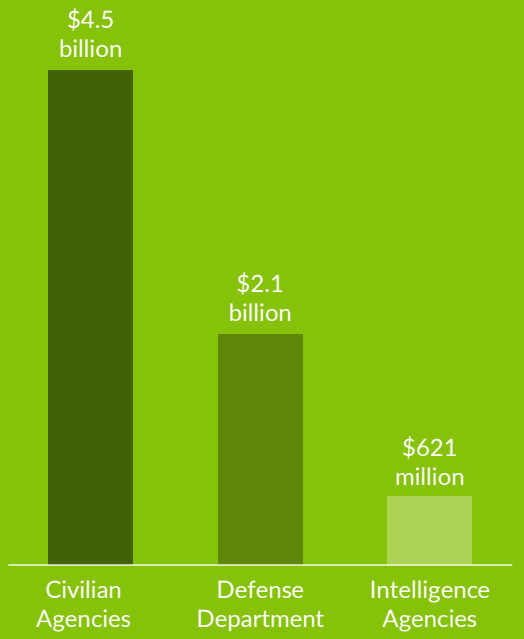
A variety of authentication options that work in multiple user computing environments

Ease of extending on-premises capabilities to the cloud over time based on agency cloud strategy

Learn more about identity security in the cloud and how SecurID can help you achieve it.

Projected Federal Cloud Spending FY21

(October 2020 – October 2021)



Source: ECT News Network, **"Federal Spurt in Cloud Spending Will Extend Well Into the Future,"** November 23, 2020

The Far-Reaching Power of MFA

The 2021 Executive Order on Improving the Nation's Cybersecurity speaks to the power of MFA to both modernize cybersecurity and enhance software supply chain security. Already mandated for access to government websites, MFA is now required by executive order to be fully adopted by all agencies across the Federal Civilian Executive Branch (FCEB) and to be included in guidance for software supply chain security practices. Given the risk posed by compromised credentials, both in the public sector and private industry, MFA is inarguably critical to securing the digital environment today.

The growing need for flexible MFA solutions

Flexibility has become an increasingly important quality for MFA solutions, as the cloud, remote work and other developments continue to erode the perimeter that has historically protected resources. People are connecting from many different locations—some without internet access—and the many diverse environments and types of users today present a range of authentication challenges. It's crucial that MFA solutions offer a variety of ways to reliably deliver secure, convenient authentication, with:

Multiple authenticator choices to meet different agency requirements and user preferences

Multi-platform functionality (Windows, macOS, iOS, Android)

Documented high availability, including when network connectivity is interrupted

Learn more about the broad range of MFA options available from SecurID.

of **hacking-related breaches** involved brute force or the use of lost or stolen credentials.

Source: Verizon, 2020 Data Breach Investigations Report

Modernize Cybersecurity and Secure the Software Supply Chain with SecurID

SecurID supports the goals of the 2021 executive order with a variety of IAM capabilities related to zero trust, cloud security and authentication. These include:

Role-based access, conditional access and risk-based analytics to support zero trust

Governance-focused and visibility-driven access authorization for continual trust evaluation

Ability to easy and seamlessly extend on-premises capabilities to the cloud

Admin visibility into access across blended cloud and on-premises deployments

FedRAMP JAB prioritization of SecurID Access to achieve a Provisional Authorization to operate

Technology integrations to enhance authentication in cloud environments

On-premises and cloud MFA with a range of authenticator choices to address different needs

MFA options tailored to user environments, risk profiles and agency preferences

99.99% documented IAM solution availability

Learn more about IAM for the **public sector** and how SecurID can help.

About SecurID

SecurID, an RSA business, is the trusted identity platform for 13,000 organizations around the world, managing 50 million identities and providing secure, convenient access to 30 million users. SecurID empowers organizations to thrive in a digital world, with complete capabilities for modern authentication, lifecycle management and identity governance. Whether in the cloud or on-premises, SecurID connects people with the digital resources they depend on everywhere they live, work and play. For more information, go to securid.com.

SecurID™
An RSA Business