A FRAMEWORK FOR MODERNIZING SECURITY

The NIST Cybersecurity Framework offers federal agencies a flexible approach to securing today's multifaceted IT systems.

THE PUSH FOR IT MODERNIZATION at federal agencies is converging with the need for stronger cybersecurity. And as agencies seek to manage increasingly complex IT environments, demand is growing for tools that simplify the adoption of new security standards and guidelines.

Enhancing security, improving service delivery, and making more efficient use of resources are the key goals in the American Technology Council's draft report on federal IT modernization. In addition, the recently signed Modernizing Government Technology Act promises to provide a much-needed source of funding and further drive agencies' commitment to revamping their systems so they can take advantage of the latest advances in security and other technologies.

Central to all that activity is the White House's executive order on cybersecurity, which stresses the importance of building and maintaining "a modern, secure, and more resilient executive branch IT architecture." It also mandates the use of the National Institute of Standards and Technology's Cybersecurity Framework as a mechanism for achieving that goal.

Federal agencies had begun adopting the framework even before the mandate. Introduced in 2014 after a collaborative development process among industry, academia, and government agencies, the framework offers guidelines for securing systems and responding to threats. Although it provides a common language and systematic methodology for managing cyber risk, it is inherently flexible so that agencies can tailor the guidelines to their specific risks and environment.

That flexible, comprehensive approach has contributed to the framework's popularity. In a survey conducted at a public-sector conference shortly after Trump's executive order was issued, 88 percent of federal employees and contractors said the framework helps organizations manage risk, and 83 percent said they were in favor of the framework being mandated across federal agencies.

The Role of Authentication

Quest's solutions for managing Microsoft platforms are well-designed to support agencies' adoption of the Cybersecurity Framework, particularly when it comes to tackling the risks associated with Active Directory.

According to Microsoft, Active Directory is the main source of authentication, identity management, and access control for more than 90 percent of organizations, including government

MaximP/ImYanis/Shutterstock

agencies. In a Dimensional Research survey, IT professionals said 73 percent of IT infrastructure is built on Active Directory and 82 percent of applications rely on its data, making it a prime target for cyberattackers.

By taking control of their Active Directory infrastructure, federal agencies can improve their security posture both on-premises and in the cloud. And when they properly secure Active Directory, they help ensure the security of their Office 365 applications and the productivity of their employees.

Securing Active Directory requires a delicate balance of granting federal employees the rights they need to do their jobs while limiting access to sensitive resources. Quest's Microsoft security suite can help agencies achieve that balance by aligning with the Cybersecurity Framework's five functions:

By taking control of their Active Directory infrastructure, federal agencies can improve their security posture both on-premises and in the cloud.

- **Identify** — It is impossible to mitigate risk without understanding who is able to do what. Agencies can better identify and mitigate suspicious activity by gaining insight into users, groups, and privileges and assessing permissions on an ongoing basis. Quest's Enterprise Reporter can identify who is a member of sensitive groups, who has access to unstructured data on premises and in Office 365, and where delegated permissions might exist in Active Directory.
- **Protect** — Quest tools can reduce the number of people who have access to unstructured data and limit the number of people who can make changes in Active Directory. Active Roles helps agencies create a least-privilege access model for Active Directory, and GPOADmin can do the same for Group Policies. Change Auditor can add another layer of protection to prevent even privileged accounts from making changes to the environment. In addition, workflow approval can be configured to only allow an employee to perform a certain task or to prevent collusion by ensuring that several people approve a task before completion.
- **Detect** — Federal IT leaders make more informed decisions when they receive meaningful information and alerts about the changes that are occurring. Quest products provide audit information for on-premises environments and Office 365 and also configure who receives alerts. Change Auditor provides information beyond what's natively available in Active Directory, such as exactly what was changed (who, what, where, when, and workstation). And InTrust can detect and notify administrators of changes to native operating system logs and analyze event logs across multiple platforms and devices.
- **Respond** — When responding to an incident or security breach, it is vital to have immediate insight into all activities as they happen. Quest can expedite the delivery of information that shows the chain of events in a security incident and help security personnel decide what to do next. In addition, InTrust can be configured to automatically execute when a specific event has occurred, thereby minimizing the incident's impact.
- **Recover** — Because Active Directory is the primary authentication source in most organizations, its availability is a core component of security. Recovery Manager for Active Directory Forest Edition provides full recovery and restores file and folder permissions from a previous state so that agencies can continue to operate securely in the event of a major disaster or corruption of Active Directory.

Furthermore, automated tools like Quest's allow agencies to take advantage of constantly evolving knowledge about cyberthreats. "If you designed your Active Directory early following Microsoft's best practices and you look at those best practices today, they're not the same," says Bryan Patton, a principal strategic systems consultant at Quest. "That's really what modernization is all about. Those practices are constantly being updated, but you didn't have to rebuild your infrastructures to support that."

Adopting the latest security tools and strategies helps agencies reap the benefits of IT modernization, which frees them to focus on more strategic endeavors.

For more information, please visit:
quest.com/solutions/federal-government

Quest