LOCKING DOWN FEDERAL INFORMATION SYSTEMS THROUGH USER AUTHENTICATION

Industry Best Practices & Standard

Data Sheet: Industry Perspectives—Federal Government

Today's federal employees depend on immediate access to a growing wealth of information. Data is a driving force behind their everyday jobs. Much of it is proprietary, and needs to be kept secure.

Today, much of this data resides online or in the cloud. Information is seemingly everywhere, and can be accessed through nearly any device, by conceivably just about anyone.

Further, internal and external threats abound. Malicious attacks can result from unauthorized users gaining access to government employees' credentials, or from the employees themselves being able to access data they should not have rights to (think Edward Snowden).

How do agencies ensure that only the correct people are provided with access to information? How do they keep data from falling into the wrong hands? How do they maintain their core focus on security while still allowing fast, easy access to critical information?

A Strong User Authentication Protocol is the Key

Implementing strong user authentication is the first—and possibly most important—step that should be taken in making sure that data does not get into the wrong hands.

USER AUTHENTICATION:

Assigns user rights and restrictions pertaining to network access.

Combines multiple identification factors together to form an enhanced security barrier.

Allows administrators to set up and manage profiles of authorized or unauthorized users – particularly important as agencies incorporate a number of different types of users, from full- to part-time employees to contractors.

Incorporates easy-to-use and implement secure credentials and digital certificates to ensure that data remains protected.

Symantec™

Some typical examples of user authentication procedures include:

Federated Identity Services: Common set of practices or standards to help manage the identity of specific users across an organization. Examples include single sign-on authentication that works across systems and agencies, establishing a secure system for sharing and managing user authorization data between agencies, etc.

Intelligent Authentication: A deeper level of security that includes fingerprinting, user behavior monitoring, and geolocation access monitoring.

Two-factor Authentication: Requires users to provide two means of authentication. Example: a one-time password (first factor) accompanied by a keycard or other physical token (second factor).

As important as it is, user authentication remains an overlooked part of many government agencies' security procedures. In fact, according to the Federal Information Security Management Act review of cybersecurity (released February, 2015), "strong authentication for civilian agency user accounts remains at only 41 percent, well below the 75 percent target."

While upping that percentage requires addressing a few challenges, the ultimate outcome will be a far more secure—and less vulnerable—organization.

User Authentication: The Challenges and the Need

User authentication and credential management can be challenging for websites that require high security. Federal government sites fit this bill even more so than any others, so it's imperative that the teams behind them implement systems that verify users' identities without developing burdensome or costly services for managing user authentication.

Currently, online security is based on users creating separate login IDs for each website they visit. But there are distinct shortcomings to this method. For users, it's annoying to have to remember scores of logins and passwords. To simplify things, they may create easy-to-remember passwords that are susceptible to compromise. For organizations, it's challenging to proactively identify new users in order to prevent fraud let alone develop cost-effective, efficient processes for managing thousands or even millions of user accounts and passwords.

The White House-authored National Strategy for Trusted Identities in Cyberspace (NSTIC) report recognizes the need to make online transactions more trustworthy for reliably authenticating individuals while streamlining the process for users and organizations. The purpose is to drive adoption of online identity technologies that support confidence, privacy, choice, and innovation (National Strategy for Trusted Identities in Cyberspace, The White House, April, 2011).

NSTIC complements other federal initiatives that focus on the need for strong user authentication. For example, the Federal Identity, Credentialing, and Access Management framework provides a roadmap for high assurance authentication, while the Department of Defense's External Certification Authority Program supports the issuance of DoD-approved certificates to industry partners and other external entities and organizations.

COMPREHENSIVE SECURITY PLAN

LEVEL OF ASSURANCE (LOA)	CONTEXT-BASED AUTHENTICATION AND AUTHORIZATION	ENDPOINT AND INFRASTRUCTURE SECURITY	SINGLE POINT OF CONTROL
			
It's not enough to simply have the system accept a passcode.	Allowing access to a secure network does not stop with vetting an identity to an appropriate LOA.	IT administrators must know exactly where sensitive data resides and secure against unauthorized users and devices.	Agencies should provide software that affords a single point of control to manage user access and permissions.

Adopting Best Practices

User authentication best practices come in several flavors. All of them should be considered as part of a comprehensive security plan.

Level of Assurance (LOA): It's not enough to simply have the system accept a passcode. Government IT must determine the appropriate LOA for access to a given set of data or applications, provide secure access to these assets, and establish a mechanism to confirm the identities of users attempting to access them. There are typically four levels of assurance, with level one asserting little or no confidence in the user's identity, up to level four, which asserts very high confidence. Different classes of exposed information require different LOAs, and selecting a single solution that can provide multiple LOAs as needed can lower the total cost of both implementation and ongoing management.

Context-based authentication and authorization: Allowing access to a secure network does not stop with vetting an identity to an appropriate LOA. Agencies must further protect their network assets once a user's identity is proven and they are granted access. Context-based authentication and authorization takes into consideration devices, directory attributes, and the network itself, and is driven by a user's memberships, roles, and privileges within that network.

Endpoint and infrastructure security: IT administrators must know exactly where sensitive data resides, including all servers and end-points, and secure those points against unauthorized users and devices. Security practices should employ a layered data loss prevention methodology that focuses on protecting the infrastructure, data center, and all end-points. Intrusion detection, prevention services, and access control systems should also be considered.

Single point of control: Agencies should provide IT administrators with software that affords them a single point of control through which they can manage user access and permissions. A single point of control allows managers to limit actions based on user identity and the devices, from anywhere and at anytime through a single dashboard. This is especially important as government resources and data become digitized and cloud-based.

Symantec™

Symantec Solutions for Strong User Authentication

Symantec offers a wide array of software designed to help agencies keep their data safe through solid user authentication procedures. They include:

Symantec Validation and IP Protection Service, a cloud-based strong authentication solution that protects networks, applications, and data against unauthorized access.

Symantec Managed PKI Service, a cloud-based solution that automates the configuration of authentication, encryption, and signing applications across platforms and browsers.

All Symantec user authentication products adhere to government security standards, including those laid out by the Federal Information Security Management Act (FISMA). For more information, as well as a complete list of Symantec user authentication solutions, visit http://www.symantec.com/user-authentication

More Information

For more information about all Symantec security products, visit www.symantec.com.
To learn more about security, visit http://www.symantec.com/security_response/, or visit Symantec's security community.
To speak with a Product Specialist in the U.S. Call toll-free 1 (800) 745-6054

About Symantec

Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company, operating one of the largest global data-intelligence networks, has provided leading security, backup and availability solutions for where vital information is stored, accessed and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2013, it recorded revenues of $6.9 billion. To learn more go to www.symantec.comor connect with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec