Secure Information Access for State & Local Governments

As Internet accessibility and mobile technology adoption have increased in the United States, governments at all levels are embarking upon or extending e-Government initiatives to provide a higher, more convenient level of service to the public and lower the cost of those services.

The explosion of connectivity and mobile device usage has induced a change in the security threat landscape. Symantec's latest Internet Security Threat Report indicates that public administration is at high risk of targeted attacks, and that the average number of user identities exposed per breach in the government sector is approaching 100,000. Distributed denial of service attacks are on the rise, with government agencies often on the receiving end of foreign cyber warfare and "hacktivism." Risky behavior by constituents aggravates the situation. In general, the average constituent is disinclined to utilize security features of personally owned devices, tends to mix personal and work data, and often engages in risky behavior such as storing sensitive information online.

State and local governments are responsible for protecting critical infrastructure and computer systems from intrusion. At the same time, they must contend with a rapidly diminishing security perimeter, as the move to mobility and the delivery of services online require greater access from outside the organization or from devices not under the management of the organization. In addition, government agencies must provide contractors and consultants with access to reliable and automated systems, and they must protect those systems from threats than can be introduced through contractor systems that may have a weaker security posture than the government's.

Regulations and standards such as FICAM, FERPA, PCI, HIPAA, and CJIS offer accepted protocols to secure systems and data, including personally identifiable information, protected health information, and criminal justice information. To secure systems and comply with these regulations, government IT must first seek to understand the institution's specific risks and vulnerabilities and then map a strategy that will guide and help prioritize the needed initiatives of each agency.

Initiatives to create a better identity ecosystem that relies on third parties for verification are on the horizon. For example, the National Strategy for Trusted Identities in Cyberspace (NSTIC) is working to that ensure government organizations can access secure, efficient, easy-to-use, and interoperable identity credentials to obtain online services, greatly relieving the burden of managing and operating identity systems.

SECURE INFORMATION ACCESS BEST PRACTICES FOR STATE AND LOCAL GOVERNMENT

Until a better solution is found, state and local government IT agencies must sail these treacherous waters on their own. On-premise authentication solutions that verify identities or in-house public key infrastructure (PKI) that create and manage digital certificates are expensive and resource-intensive. In addition, PKI is rarely considered a core competency, and expertise can be hard to find. However, understanding secure information access best practices and adopting appropriate technologies can help government agencies provide public services consistently, securely, and cost-effectively. The following best practices should be implemented to help protect agency systems from unauthorized access.

User Authentication

Government IT is responsible for securing access to the network and protecting confidentiality. To this end, user authentication technology must be in place to verify that systems and people are who they say they are, and it must go beyond the flawed and inadequate user name and password mechanism. Strong authentication can enable government agencies to secure access to networks and applications while preventing incursion by malicious unauthorized attackers. A unified solution that provides both two-factor and risk-based, token-less authentication and is based on open standards is either explicitly required in regulations, or an accepted best practice.

Identity Proofing and Level Of Assurance (LOA)

Government IT must determine the appropriate level of identity assurance for access to a given set of data or applications, provide secure access to these assets, and establish a mechanism to confirm the identity of users attempting to access them. To accomplish these goals, an appropriate identity proofing process must be in place that vets the credentials offered against a broad range of attributes. Different classes of exposed information require different levels of identity assurance, and selecting a single solution that can provide multiple levels of assurance as needed will lower the total cost of both implementation and ongoing management.

Access Management, or Context-Based Authentication and Authorization

Allowing access to a secure network does not stop with vetting an identity to an appropriate level of assurance. In fact, government institutions must further protect their network assets once a user's identity is proven and access granted. Context-based (device, network, and directory attributes, for example) access control is driven by a user's memberships, roles, and privileges within the network. Selecting a solution based on open standards will allow integration with most applications and sources of identity.

Encryption

In the event of a breach, government institutions that have data on desktops, laptops, and removable storage devices encrypted in line with regulations will not be subject to penalties. Advanced data encryption and file encryption for desktops, laptops, and removable storage devices is, therefore, a must. A robust solution offers scalable, enterprise-wide security that prevents unauthorized access by using strong access control and powerful encryption. A central management console enables safe, central deployment of encryption to endpoints.

Endpoint and Infrastructure Security

Adversaries are targeting all control points from the gateway to email to the endpoint. With users still the weakest link in the security chain, organizations must know exactly where sensitive data resides, including all servers and end-points, and then actively secure those points. Security practices should employ a layered data loss prevention methodology that focuses on protecting the infrastructure, the data center, and all endpoints. In addition to data loss prevention, government IT should consider intrusion detection and prevention services and access control systems.

Single Point of Control

Maintaining a single, secure access point to applications and services is increasingly important as government resources are digitized and moved to the cloud. A data loss prevention solution can identify specific information that needs to be protected—and then help government IT make decisions on how to secure that information. In addition, organizations should make sure the data stored in the cloud is encrypted.

SYMANTEC SOLUTIONS FOR SECURE INFORMATION ACCESS

According to Symantec's 2014 Internet Security and Threat Report, targeted attacks on personal data increased 91 percent, exposing more than 550 million identities in 2013. Comprehensive information access solutions that allow state and local governments to deliver on their mission to serve citizens, while protecting the network from unauthorized access, are more critical than ever. Regardless of the required level of security or level of assurance in user identity—from simple two-factor authentication all the way up to PKI-grade smart certificates—Symantec offers reliable and secure solutions, including advanced data and file encryption for desktops, laptops, and removable storage devices and strong access control. Our identity proofing offering is Kantara Initiative-approved, meets the requirements of NIST 800-63-1, and is certified compatible with FICAM guidelines to minimize the occurrence and cost of fraud.

Symantec can help government agencies at all levels comply with industry best practices and standards, discover information vulnerabilities, establish security across the organization, and protect constituents.

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 2014, it recorded revenue of $6.7 billion.

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