Protect the Data that Powers the Business of Government

Government entities and federal contractors must implement solutions that protect sensitive data without limiting its usage.

Hewlett Packard Enterprise

TERADATA.

Table of Contents

Security experts agree that no matter how strong the perimeter security of a network, a data breach is not just a possibility, but an almost certainty. Government agencies' network data is under constant attack from a dangerous mix of state-sponsored hackers, technology savvy criminal enterprises and "hacktivists" looking for weaknesses and access to valuable data.

To that you add the risk of "insider threat". Whether an intentional leak or simple human error, there is a major risk that insiders with access to valuable data, from network administrators to analysts, could mishandle and expose classified information and personal data. And in that scenario, perimeter security is not even a factor.

This means agencies and contractors on the federal, state, and local levels must change their entire strategy behind the protection and security of their most valuable information.

Protect the Data

To keep their information safe, these organizations must protect the data itself and ensure that if a breach does occur the information will be unusable for the attackers or the insider. The challenge is to achieve that level of security while also allowing the data to be used by analysts and applications in addition to meeting compliance and privacy regulations. With data in constant motion, governments and their partners must protect it from the moment of capture throughout its entire lifecycle.

The stakes have never been higher. Government agencies and the companies they do business with are collecting more data than ever.

Just a single breach can have far-reaching consequences. When the South Carolina Department of Revenue was hacked, for example, the incident exposed approximately 3.6 million social security numbers and nearly 400,000 credit and debit card numbers of the state's taxpayers.

The good news is that innovative data-centric security solutions, Format-preserving Encryption, and Secure Stateless Tokenization are key components of a layered defense security strategy for protecting even the most sensitive and classified data.

Data Security Has Never Been More Critical

According to September 2016 statistics from the Government Accountability Office[1] (GAO), between 2006 and 2015, the number of cyber attacks against federal agencies grew a staggering 1,300 percent, skyrocketing from 5,500 to more than 77,000 per year.

Many security technologies put in place to stop these intrusions end up limiting data access, which runs counter to the need to make full use of data and analytics, and subject that data to more applications and uses. Free movement of data between systems and applications is critical to gaining its full value. Compounding the problem are the legacy systems that many government entities are struggling to use as data volumes continue to grow exponentially.

These legacy systems can be vulnerable to hackers who want anything from social security numbers to tax information to background checks to other data that could lead to identity theft or loss of classified information. With governments, hacked data can put lives and national security at risk. If undercover agents and their families are identified, for example, they could be kidnapped or killed.

New Data Uses Require New Protections

As the public sector implements unified data architectures and Hadoop technologies such as data lakes, and ingests and leverages data from a wider range of sources such as the Internet of Things (IoT), the data must be protected. Big data and Hadoop have increased the complexity of security requirements. There is now more "surface area" to attack, as well as more devices, places, connections, and networks for hackers to target.

Data security should be part of governments' and federal contractor' strategies, and implemented when new technologies and applications are added, not bolted on later. Ideally, data is protected as close to its source as possible.

As a key part of a layered defense security strategy, encryption, tokenization, and data masking techniques all help effectively protect data in new and existing technologies. These capabilities are essential for meeting data privacy requirements, such as protecting personnel data and background check information, yet allowing the data to be accessible to authorized users.

Data-Centric Security Offers Unique Safety Features

According to Verizon's 2016 Data Breach Investigations Report, most data breaches, 84 percent, happen at the network application layer or in gaps between levels when data is potentially exposed. Fundamental security controls dramatically reduce the likelihood of a successful attack. Data-centric security, for example, provides protection from the moment data is ingested, through analysis, to back-end data storage.

Format-preserving encryption also offers protection benefits. It uses pseudonymization—actual data is replaced with artificial identifiers—to minimize the exposure of personal data and eliminate the ability to identify taxpayers and employees. As a result, the encryption mitigates the risks inherent in data processing.

Meeting Standards and Regulations

Data-centric encryption ensures greater levels of protection for government IT networks. The Cybersecurity Act of 2015 helps agencies and contractors establish guidelines for better security standards. The act requires agencies to "encrypt or otherwise render indecipherable to unauthorized users of 'sensitive and mission critical data stored by the agency' or transiting agency information systems."

The National Institute of Standards and Technology (NIST), meanwhile, recently released a computer security standard that makes encryption easier. The NIST mode standard[2] allows format-preserving encryption to protect sensitive data at rest, in motion, and in use while preserving data formats. The standard provides an approved and proven data-centric encryption method for government agencies and government contractors.

With format-preserving encryption, even if a security system is breached, the data is worthless to hackers because it's encrypted. However, because the encrypted data looks like the real thing, data scientists and analysts can use it to identify patterns, make discoveries, and run queries without decryption. This enables deeper insights in less time than traditional encryption. It also allows data to be mobile so it can be moved between systems, databases, and around the globe, and still be protected.

Protection Across Platforms

A single breach is all it takes for government secrets or millions of taxpayers' personal information to be stolen. With the right solutions in place, including a data-centric approach with format-preserving encryption, tokenization, and data masking protection, public sector agencies and government contractors can keep their data safe and secure across all platforms while leveraging the information to enhance the business of government.

For More Information

Teradata solutions allow businesses to leverage all of their data across all applications and uses to gain maximum value. The solutions should be part of security plan that relies on big data analytics to provide intelligence about threats and optimize cyber defense strategies, and an integrated data warehouse (IDW) to reduce the dispersion of data storage throughout an organization, increase the overall effectiveness and manageability of a comprehensive security program. When data is in an IDW, security efforts can be focused and easily monitored and maintained without the risk of weaknesses in a single uncontrolled database exposing the entire enterprise environment to risk.

Teradata advocates for a comprehensive approach to information security that includes an orchestrated combination of technology and best practice processes. Teradata helps protect data while empowering companies to achieve high-impact business outcomes. For more information, visit **Teradata.com**.

End-to-End Data Security

Protecting data isn't easy. Government agencies and the contractors doing business with them quickly discover the complexities and management challenges with traditional security approaches. Hewlett Packard Enterprise (HPE) offers innovative solutions such as format-preserving encryption for a highly granular approach to encryption.

Federal Information Processing Standard (FIPS) 140-2, a U.S. government security standard, specifies requirements that a cryptographic module must meet to protect sensitive information. HPE solutions meet all requirements specified in the standard—**HPE SecureData** is the only FIPS-140-2 level 2 validated solution on the market that also has format-preserving encryption certified under NIST SP 800-38G. That means it has passed extensive testing for strong physical security and a robust role-based access control system.

HPE SecureData unites the best market-leading encryption, tokenization, data masking, and key management technologies to protect sensitive information in one comprehensive solution.

- NIST certified HPE Format-preserving Encryption (FPE) sets the new standard for secure data protection that maximizes data usability
- HPE Stateless Key Management makes encryption scalable at the highest volumes, delivers keys on demand, reduces IT management costs with no key storage.
- HPE Secure Stateless Tokenization (SST) is an advanced, patented technology recommended for protection of Payment Card Industry (PCI) data.

Cyber Crime by the Numbers

1.9 Number of successful attacks per week on organizations[3]

46 Days needed to resolve a cyber attack (up from 14 days in 2010)[3]

$100 billion
Amount the U.S. government spent on cyber security over the last decade[4]

$14 billion
Amount the U.S. government budgeted for cyber security in 2016[4]

30 million
Number of known malicious intrusions to Department of Defense networks between September 2014 and June 2015. That's 100,000 attacks per day.[5]

93 Percent of breaches that take minutes or less to compromise a system[6]

63 Percent of confirmed data beaches that leverage a weak, default or stolen password[6]

End Notes

1. U.S. Government Accountability Office (GAO), "Federal Information Security – Actions Needed to Address Challenges," **www.gao.gov/assets/680/679877.pdf**
2. National Institute of Standards and Technology, "New NIST Security Standard Can Protect Credit Cards, Health Information," **www.nist.gov/news-events/news/2016/03/new-nist-security-standard-can-protect-credit-cards-health-information**
3. Ponemon Institute, "2015 Cost of Cyber Crime Study: Global," HP-commissioned study, October, 2015, **itnewsafrica.com/hp/IT%20management%20and%20monitoring/HPE_security.pdf**
4. Steve Morgan, "The Business of Cybersecurity: 2015 Market Size, Cyber Crime, Employment, and Industry Statistics," *Forbes*, October, 2015, **www.forbes.com/sites/stevemorgan/2015/10/16/the-business-of-cybersecurity-2015-market-size-cyber-crime-employment-and-industry-statistics/#6ac10fcd10b2**
5. Office of the Secretary of Defense, memo, Sept. 30, 2015, **www.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf**
6. Verizon, "2016 Data Breach Investigations Report," April, 2016, **www.verizonenterprise.com/verizon-insights-lab/dbir**

10000 Innovation Drive, Dayton, OH 45342 **Teradata.com**

01.17 EB7213