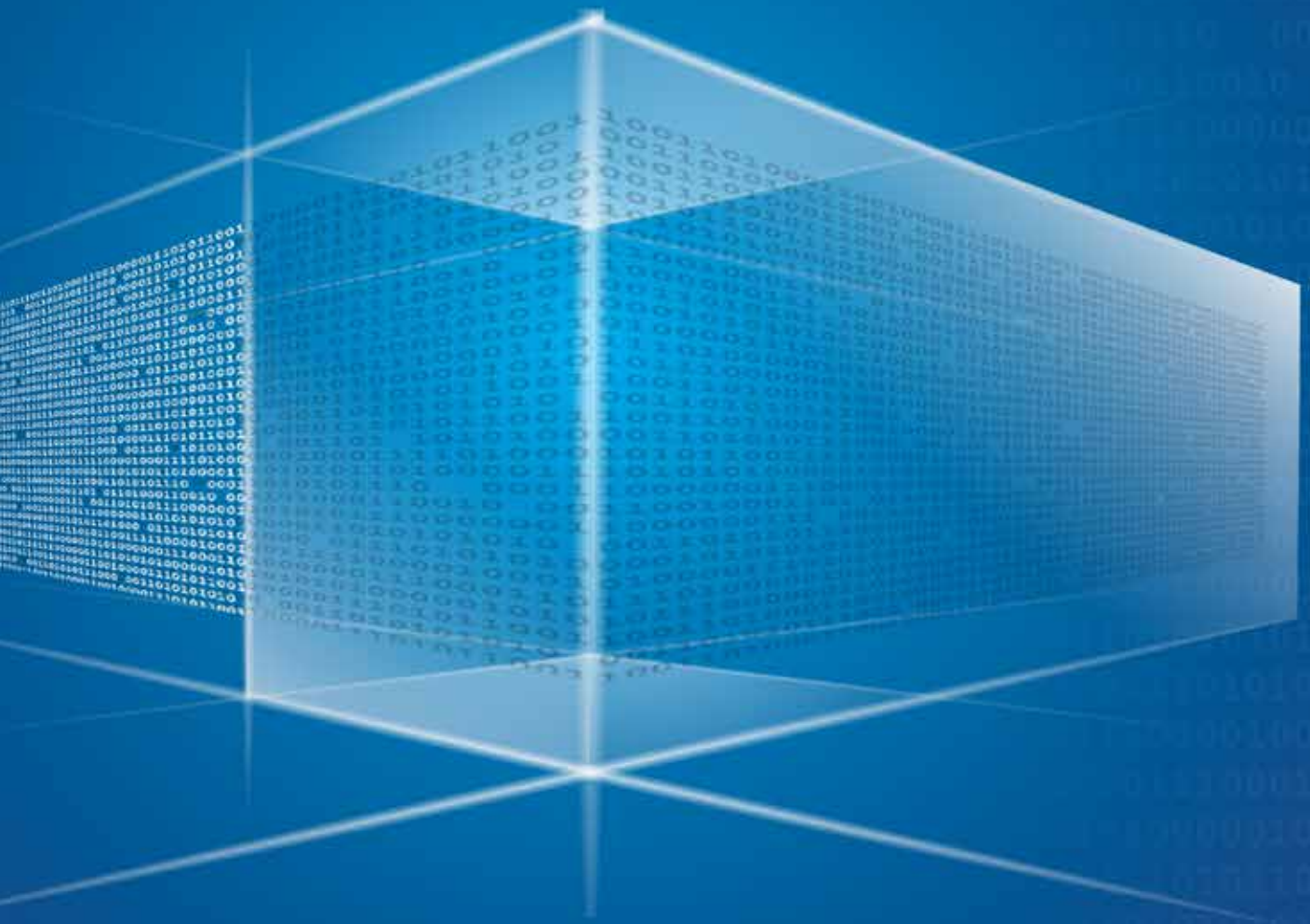
Protect Sensitive Data from Prying Eyes



Data-centric best practices for safeguarding high-value data in the government

CYBEREDGE GROUP

LICENSED BY Hewlett Packard Enterprise

HIGH-VALUE DATA = HIGH RISK FOR GOVERNMENT

Throughout the federal, state, and local government, there's a virtual treasure trove of high-value data and personally identifiable information (PII) on government employees, taxpayers, students, retirees, military personnel, and anyone with any business with the government. It's no secret—or surprise—that it's become a valuable target for cybercriminals.

Federal and state government agencies publicly disclosed a total of 203 data breaches between 2010 and 2016.[1] The year 2016 alone saw 72 breaches happen within the government sector.[2] In the majority of cases, government breaches involved PII such as names, Social Security numbers, and birthdates. The United States Office of Personnel Management (OPM) alone experienced the theft of PII and security clearance background investigation information for 22.1 million individuals in 2015.

With no end in sight to the growing threat of data breaches, the number one lesson government CIOs should learn is that current cybersecurity measures simply aren't enough to stop cybercriminals from exfiltrating high-value data. That's because most common cybersecurity measures—firewalls, intrusion prevention systems, antivirus software, and other security technology operating at the network and endpoint layers—are increasingly ineffective against advanced cyberattacks, leaving gaps where data is exposed.

Advances in data-centric security best practices and encryption technology can protect data no matter where it resides, how it is transported, and even how it is used. Widely implemented in the private sector to protect high-value data—without impeding mission performance—sophisticated, data-centric solutions are also available for government agencies. They render high-value and PII data useless for cybercriminals while supporting legacy systems and enabling compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), General Data Protection Regulation (GDPR), and others.

One agency's fight:

The Office of Personnel Management repels **10 MILLION** attempted digital intrusions per month.

1. Vijayan, Jai, "The 7 Most Significant Government Data Breaches," DARKReading, November 15, 2016.
2. "Identity Theft Resource Center 2016 End of Year Data Breach Report," CyberScout, January 18, 2017.
3. Koerner, Brendan I, "Inside the Cyberattack that Shocked the US Government," Wired, October 23, 2016.

CYBERCRIMINALS GET A BIG SLICE OF GOVERNMENT PII

Government personally identifiable information (PII) is a lucrative target for cybercriminals.
In fact, the government sector is second only to the healthcare industry in total records breached.

40%

increase in data breaches in 2016

52%

of breaches exposed Social Security numbers

36.6 million records exposed in 2016 in:

Financial Sector | Business Sector | Education Sector | Healthcare Sector | Government Sector

13.9

million records came from the government sector

Source: "Identity Theft Resource Center 2016 End of Year Data Breach Report," CyberScout, January 18, 2017.

A TANGLED SET OF CHALLENGES FOR GOVERNMENT DATA PROTECTION

Every industry is keenly aware of the increasing importance of cybersecurity countermeasures to protect high-value data. Government organizations are certainly no different. Yet, they often face a more unique combination of challenges than private businesses do when trying to secure sensitive data.

NEW USES FOR DATA

As the public sector turns to big data for new insights and understanding, data security becomes more complex. Unified data architectures, Hadoop technologies such as data lakes, and data from a wider range of sources such as the Internet of Things (IoT) create not only more data for hackers to target, but also increase the surface area for attacks, including more devices, locations, connections, and networks.

LIMITATIONS OF TRADITIONAL SECURITY

Common cybersecurity measures only protect data indirectly. For example, firewalls and intrusion prevention systems operate predominately at the network layer to control network access. Likewise, desktop antivirus software works to stop the spread of malware infections, but does not protect data directly. Worse yet, these measures may actually impede mission performance by interrupting or blocking legitimate network traffic or software without improving data protection.

GAPS IN DATA PROTECTION

Most data-protection techniques shield only stored data. While helpful when equipment is lost or stolen, relying on data-at-rest security to protect sensitive information is not sufficient because most data doesn't stay in one place. For instance, data can be exposed and vulnerable to attack after it is decrypted and retrieved from an encrypted database and before it flows through an encrypted link.

COMPLIANCE

Increasingly stringent, data-privacy requirements make greater data protection imperative while adding another level of complexity. Agencies must comply with federal standards and regulations such as GDPR, GLBA, HIPAA, the National Institute of Standards and Technology (NIST), and Federal Information Processing Standards (FIPS).

LEGACY SYSTEMS

Compounding the data security problem are the legacy systems that many government entities still have in place. These systems are often stretched to their limits to keep up with exponentially growing volumes of data. Another concern is that vendors of older, end-of-life legacy systems may no longer supply patches or otherwise maintain the code, making the software vulnerable to hackers.

TRADITIONAL DATA ECOSYSTEM AND IT INFRASTRUCTURE SECURITY

DATA AND APPLICATIONS
Authentication
Management

MIDDLEWARE
SSL/TLS/
Firewalls

DATABASES
Database
Encryption

FILE SYSTEMS
SSL/TLS/
Firewalls

STORAGE
Disk
Encryption

SECURITY GAP THREAT
Credential Compromise

SECURITY GAP THREAT
Traffic Interceptors

SECURITY GAP THREAT
SQL Injection, Malware

SECURITY GAP THREAT
Malware, Insiders

DATA-CENTRIC SECURITY: A PROVEN APPROACH IN THE PRIVATE SECTOR

PROTECTING DATA EVERYWHERE

Recent advances in data-centric security techniques protect data no matter where it resides, how it is transported, and even how it is used—without increasing complexity, requiring massive application changes, or impeding mission performance.

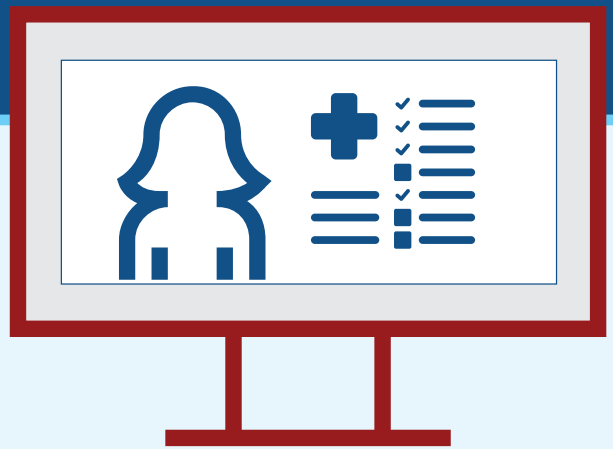
An essential part of a layered-defense security strategy, data-centric security includes encryption, tokenization, data masking, and enterprise key management techniques to help effectively protect data from the moment it is ingested, through analysis, to backend data storage. These capabilities are imperative for meeting data-privacy requirements—such as protecting personnel data and background check information—yet allowing the data to be accessible to authorized users.

TAKING ADVANTAGE OF BEST PRACTICES

In the private sector, a data-centric security approach that includes format-preserving encryption (FPE) helps reduce exposure of personal data to cyber thieves or internal threats. One example that most Americans have become accustomed to is providing only the last four digits of the SSN or credit card number when interacting with a company. FPE that is customizable to provide partial data de-identification can leave just enough data in the clear for the organization to use it for identification, but protect the rest of the sensitive data.

Reducing risk and enabling secure data analysis

A leading U.S. health insurer deployed a data-centric security solution to protect customer PII and personal health information (PHI). The new solution provides secure data access for analysis without jeopardizing customer privacy or compliance with regulations such as HIPAA. It also helps reduce prescription fraud and claim overpayment by enabling analytics and fraud detection on protected data by de-identifying and sharing data from multiple data sources.



DATA-CENTRIC SECURITY: TECHNOLOGY

Format-Preserving Encryption (FPE)

Format-preserving encryption (FPE) makes it far easier and more cost effective for organizations to use encryption. It is critical in protecting sensitive data-at-rest, in-motion and in-use while preserving data format. FPE enables government organizations to de-identify sensitive personal data without extensively revamping existing IT infrastructure. It improves security and lowers the cost of strong data protection.

With FPE, even if a security system is breached, the data is worthless to attackers because it's encrypted. However, because the encrypted data looks like the real thing, analysts can still use it to identify patterns, and run queries without decryption. It also allows data to be mobile so it can be moved between systems and around the globe and still be protected, without breaking databases.

Older AES Encryption:

lja&3k24kQotugDF2390^320OWioNu2
(*872weWOiuqwriuweuwr%oIUOw1@

- ! Long strings of data that don't fit original data formats
- ! Breaks databases and applications
- ! No analytics possible

FPE Encryption:

SSN/ID	EMAIL	DOB
934-72-2356	bob@agency.gov	31-07-1955
↓	↓	↓
347-98-8309	hry@ghohaw.jlw	20-05-1972

- ✓ De-identifies data but maintains formats
- ✓ Allows data to move through existing applications/ databases
- ✓ Data can be shared and analyzed

Secure Stateless Tokenization (SST)

SST solutions use a FIPS random-number generator to produce a unique, random token for each clear-text input, resulting in a token with no relationship to the original number. It's widely used to protect payment card information.

Enterprise Key Management (EKM)

EKM solutions protect valuable encryption keys for protecting data-at-rest, in-motion, and in-use. They can use tamper-resistant hardware and software to manage encryption keys that protect data-at-rest, or stateless key management for securing encryption keys for data-in-motion and in-use. EKM solutions secure servers, storage, and cloud storage against losses or mishandling of encryption keys.

THE NEW NIST STANDARD: BRINGING FPE INTO THE GOVERNMENT

In 2016, NIST released a computer-security standard that makes encryption easier using an approved and proven data-centric encryption method for government agencies and contractors. The NIST standard allows the use of FPE to protect sensitive data-at-rest, data-in-motion, and data-in-use while preserving data formats, making the data-centric best practices and technology used in the private sector available for government agencies.

NIST SP 800-38G creates standards for FPE, which makes long strings of numbers indecipherable in both binary and decimal formats. Previously NIST standards were only applicable to binary data; it wasn't technically feasible to encrypt decimals while also allowing computer programs to read a number in its original format.

What government organizations should look for in a data-centric security solution

- "Kills" the high-value data and PII through encryption that renders it unusable if stolen or lost, even while it maintains the format, context, relationships and meaning of the data for use in analytics, applications, and processes
- Requires minimal effort and change to existing applications and systems
- Enables your organization to meet relevant regulations and standards
- Adapts to changes easily
- Handles today's compute-intensive demands and variety of data formats
- Supports big data and IoT environments

FROM THE SPONSOR:

NOT ALL FPE TECHNOLOGIES ARE MADE EQUAL

HPE SECUREDATA WITH HYPER FPE

HPE SecureData with HPE Hyper Format Preserving Encryption (FPE) is NIST-standard compliant using FF1 AES Encryption to encrypt virtually unlimited data types. Hyper FPE technology delivers a proven and approved method of protecting data that allows U.S. federal and other governmental agencies to take full advantage of the new NIST standard and delivers best-of-breed capabilities, including:

HYPER PERFORMANCE

Accelerated encryption for hyper performance—up to 170 percent faster than previous FPE technology—supporting high-volume needs of next-generation big data, cloud, and IoT scenarios.

HYPER FLEXIBILITY

Encryption of virtually unlimited data types, including IDs, VINs, bank accounts, and any classified data types that need encryption. Preserves format, relationships, context, meaning, and fit to legacy systems.

HYPER USABILITY

Wide access to de-identified data, powers big data, cloud, and IoT initiatives while using granular policy management control to limit access to highly sensitive data.

HPE SecureData with HPE Hyper Secure Stateless Tokenization (SST) offers an enhanced, patented approach to tokenization that maximizes speed, scalability, security, and manageability of the tokenization process, effectively doubling the existing "high octane" HPE SST tokenization performance.

HPE SECUREDATA DATA-CENTRIC SECURITY

HPE SecureData protects data independent of the subsystems that use it. It protects sensitive data as soon as it is acquired and ensures that it is always used, transferred, and stored in protected form. Selected applications decrypt the data only at the time that it is processed, while others work with encrypted or masked data.

DATA AND APPLICATIONS	MIDDLEWARE	DATABASES	FILE SYSTEMS	STORAGE
Authentication Management	SSL/TLS/ Firewalls	Database Encryption	SSL/TLS/ Firewalls	Disk Encryption

END-TO-END PROTECTION

HPE meets federal standards

HPE SecureData with Hyper FPE is NIST-standard compliant using FF1 AES encryption to encrypt virtually unlimited data types. Hyper FPE technology delivers a proven and approved method of protecting data for U.S. federal and other governmental agencies, and global enterprises.

THE FEDERAL GOVERNMENT: HPE SECUREDATA IN ACTION

An increasing number of government organizations are turning to HPE SecureData to protect sensitive, high-value data.

Protecting nuclear weapons systems

A U.S. government organization needed to meet advanced security requirements for nuclear weapons systems. Using HPE SecureData, the organization now protects mission-critical, weapons-systems data by automating security key management for thousands of encrypted disk drives.

Defending the data about defenders

Protecting military healthcare data is a top priority for a large federal agency. HPE SecureData helps protect soldiers' healthcare data, enables the organization to meet assurance and risk reduction guidelines for sensitive healthcare data, and unifies controls with a single pane of glass that simplifies management.

Analyzing economic data securely

A large domestic agency needed to protect high-value, economic, and PII data used in a risk-management analytical system. HPE SecureData protects PII and sensitive data on the analytic platform and enables secure analysis and sharing of risk management data with external users.

Securing high-value logistics data

Military logistics data is a high-value target for cyber criminals. HPE SecureData delivers persistent, end-to-end protection across multiple core systems for defense department clients—with FIPS-level security assurance and no changes to database schemas required.

Counting on HPE SecureData to protect financial information

A federal credit union needed to protect the sensitive financial data of its members. Using HPE SecureData, the credit union not only secures its global payments infrastructure but also meets the highest government and financial industry standards for data protection.

About HPE Security—Data Security

HPE Security—Data Security, is the leading data protection provider, delivering secure, scalable, and proven data-centric encryption, tokenization and key management solutions, enabling our customers to effectively combat new and emerging security threats. Our powerful data protection solutions allow any organization to seamlessly secure all types of sensitive government, corporate, and customer information, wherever it resides, while efficiently meeting regulatory compliance and privacy requirements.

About CyberEdge Group

CyberEdge Group is an award-winning research, marketing, and publishing firm serving the needs of information security vendors and service providers. Our highly experienced consultants have in-depth technical expertise in dozens of IT security technologies, including:

- Advanced Threat Protection (ATP)
- Application Security
- Authentication, Authorization, and Auditing (AAA)
- Cloud Security
- Data Protection, Encryption, and Tokenization
- DoS/DDoS Protection
- Endpoint Security
- Enterprise Mobility Management (EMM)
- Intrusion Prevention Systems (IPS)
- Network Behavior Analysis (NBA)
- Network Forensics
- Next-Generation Firewall (NGFW)
- Patch Management
- Penetration Testing
- Privileged Identity Management (PIM)
- Secure Email Gateway (SEG)
- Secure Web Gateway (SWG)
- Security Analytics
- Security Configuration Management (SCM)
- Security Information & Event Management (SIEM)
- Virtualization Security
- Vulnerability Management (VM)