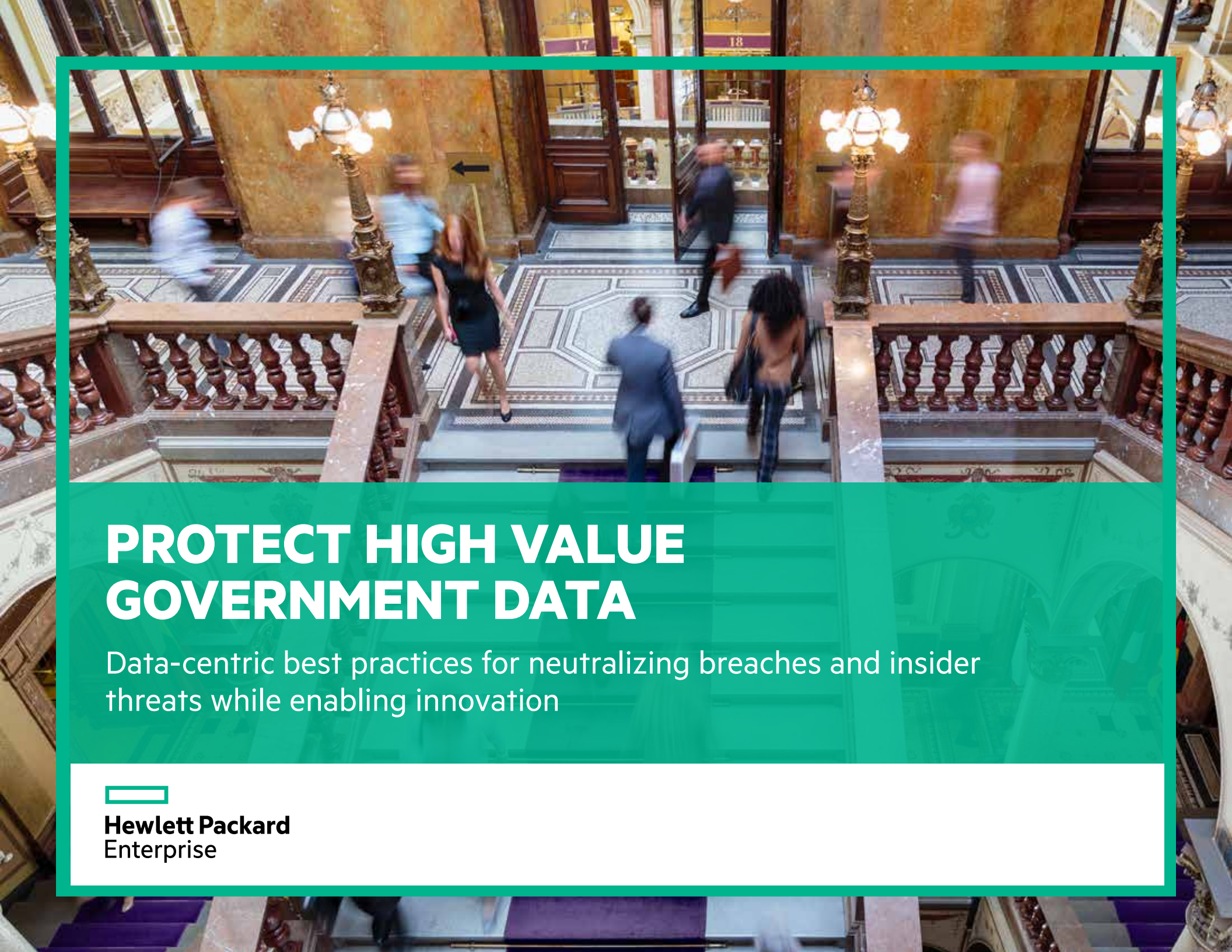


PROTECT HIGH VALUE GOVERNMENT DATA

Data-centric best practices for neutralizing breaches and insider threats while enabling innovation

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 almost 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 across networks, systems and endpoints—are increasingly ineffective against advanced cyberattacks, leaving gaps where data is exposed. A new approach is needed to address today's complex threat environment.

Advances in data-centric security best practices by applying 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 application 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.

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.

One agency's fight:

120 MILLION

Attempted Cyberattacks per Year[3]

The Office of Personnel Management repels

10 MILLION

attempted digital intrusions per month.

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.[4]

40%

increase in data breaches in 2016[4]

52%

of breaches exposed Social Security numbers[4]

36.6 million records exposed in 2016[4] in:

Financial Sector | Business Sector | Education Sector | Healthcare Sector

13.9

million records came from the government sector[4]

4 "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.

Data sharing and big data

Government agencies are challenged with providing better citizen services and be more transparent, but that requires increased data sharing between agencies and with contractors. It also requires big data analytics and adoption of new technologies to manage the data lake such as Hadoop.

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.

Limitations of traditional security

Common cybersecurity measures only protect data indirectly. For example, firewalls, intrusion detection systems and access controls 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.

Compliance

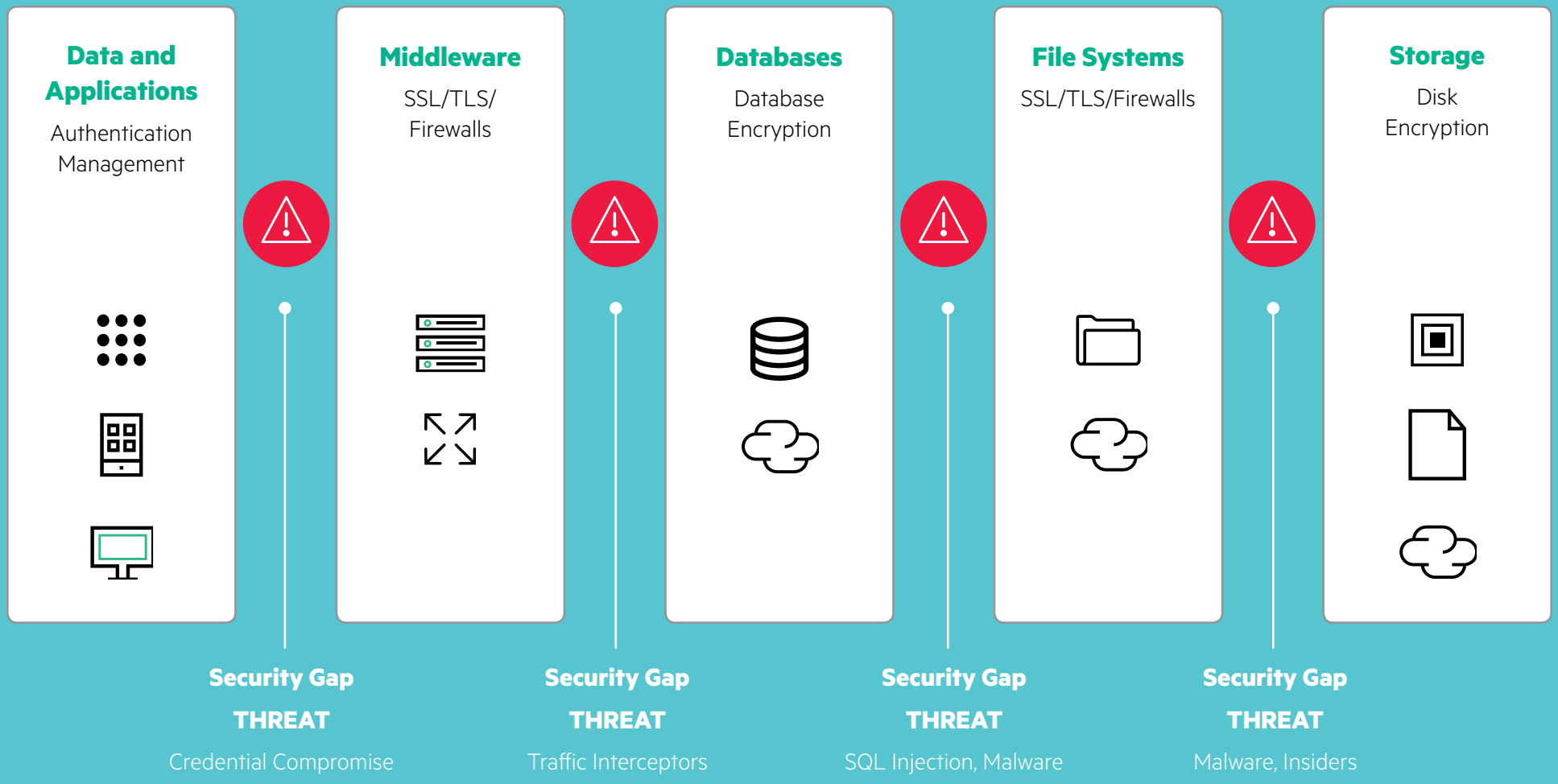
Increasingly stringent data-privacy requirements make greater data protection imperative while adding another level of complexity. Agencies must comply with federal standards and regulations such as Cybersecurity Act of 2015, DFARS CUI, the General Data Protection Regulations (GDPR), the National Institute of Standards and Technology (NIST), and the 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

In an ideal world, sensitive data travels in well-defined paths from data repositories to a well-understood set of applications. In this scenario, data can be protected by armoring the repository, the links, and the applications using point solutions such as database encryption and SSL network connections. In real systems, data travels everywhere. Today's IT environment is a constantly shifting set of applications running on an evolving set of platforms. Gaps in data security appear naturally, especially when data needs to be used. These are the gaps that are exploited by hackers on most attacks.



DATA-CENTRIC SECURITY:
Transforming cyber-security in the private sector

Filling the gaps: 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.

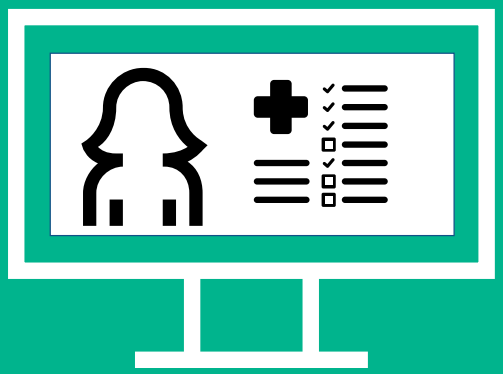
An essential part of a layered-defense security strategy, data-centric security includes encryption, tokenization, data masking, and large scale key management techniques to help effectively protect data from the moment it is ingested, through analysis, to backend data storage. These capabilities are 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 next generation 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. FPE is customizable to provide partial data de-identification, leaving just enough data in the clear for the organization to use it for identification, but protect the rest of the sensitive data. 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.

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.

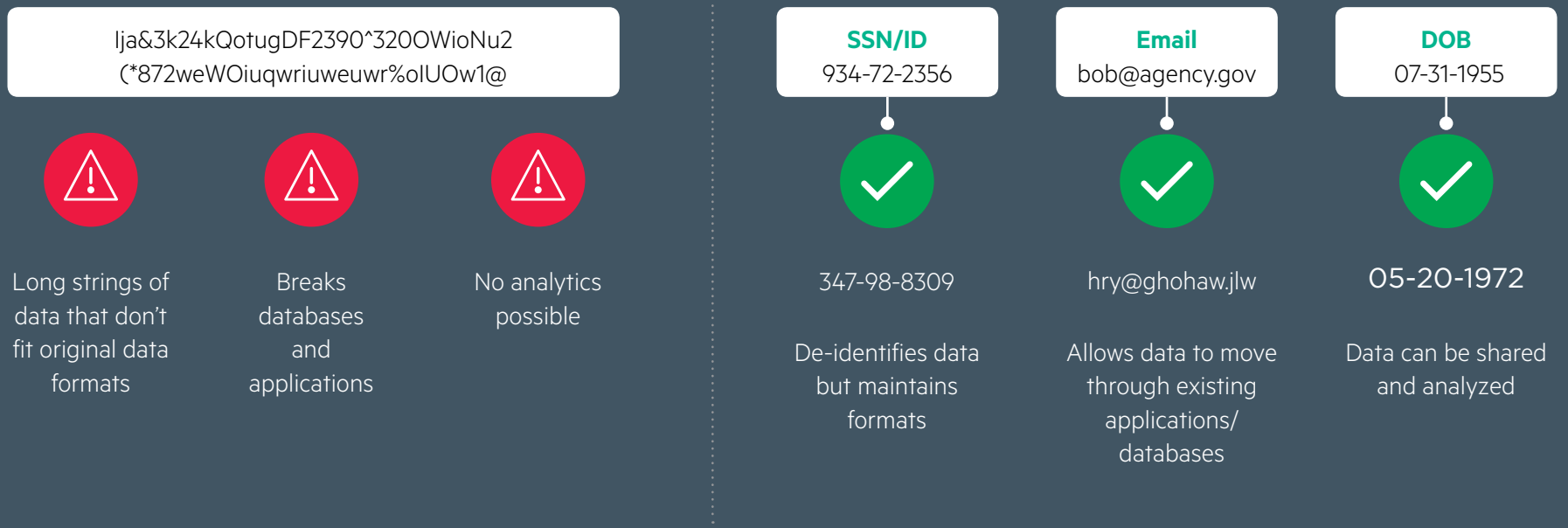


DATA-CENTRIC SECURITY: TECHNOLOGY

Format-Preserving Encryption (FPE)

Format-preserving encryption (FPE) makes it 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 departments and agencies 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 an application or system experiences a security breach, the data is worthless to attackers because it's encrypted. However, because the encrypted data looks like the original data, 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 while still remaining protected, without breaking databases and similar data repositories.



THE NEW NIST STANDARD FOR FORMAT-PRESERVING ENCRYPTION (FPE):

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 new NIST FF1 AES encryption standard recommends the use of Format Preserving Encryption to protect sensitive data-at-rest, data-in-motion, and data-in-use while preserving data formats. This makes data-centric best practices and technology used in the private sector available for government agencies.

NIST SP 800-38G recommends methods 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.

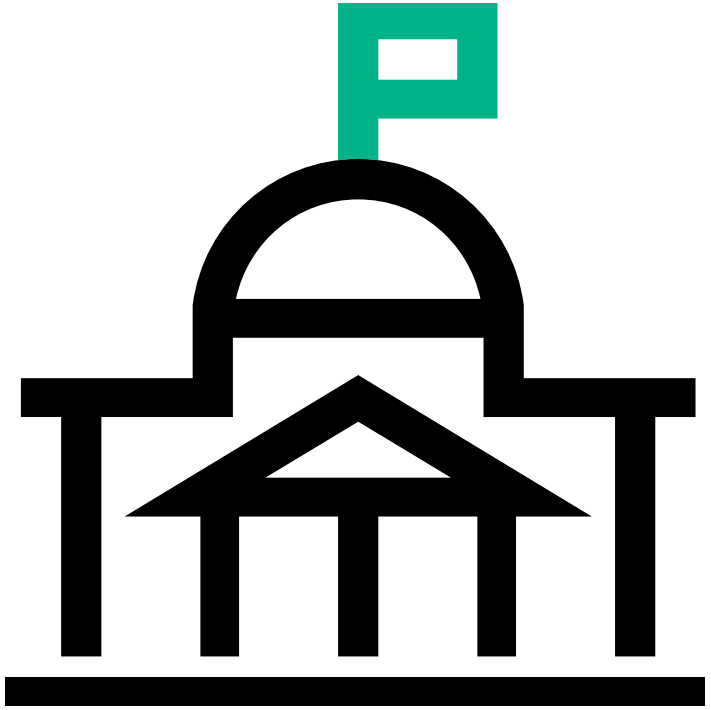
What government organizations should look for in a data-centric security solution

- Protect the high-value data such as 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 to implement and changes to existing applications and systems.
- Helps meet relevant regulations and standards.
- Adapts to changes easily by offering flexibility to handle diverse classes of data.
- Handles today's compute-intensive demands and variety of data formats.
- Supports big data and IoT where scale and performance are mission-critical.

HPE SECUREDATA WITH FIPS-VALIDATED FPE: BRINGING FPE DATA-CENTRIC SECURITY TO THE FEDERAL GOVERNMENT

HPE SecureData includes the industry's first Federal Information Processing Standard (FIPS) 140-2 validation of Format-Preserving Encryption (FPE). Now government departments and agencies, and private contractors serving government customers, can leverage the same powerful and proven technology that has transformed cybersecurity in the private sector.

HPE SecureData with Hyper FPE "de-identifies" sensitive personally identifiable information (PII) such as social security numbers (SSN), and other high value data, rendering it useless to attackers in the event of a security breach. This allows government agencies to securely leverage the de-identified data for big-data analytics, and collaborate with shared data between other agencies or contractors. It also allows government departments and agencies to adopt new deployment models and technologies, such as the cloud or Hadoop or invest in innovations such as IoT, all while helping lower the risk of disclosing sensitive personal data and helping to avoid compromising high value classified data.

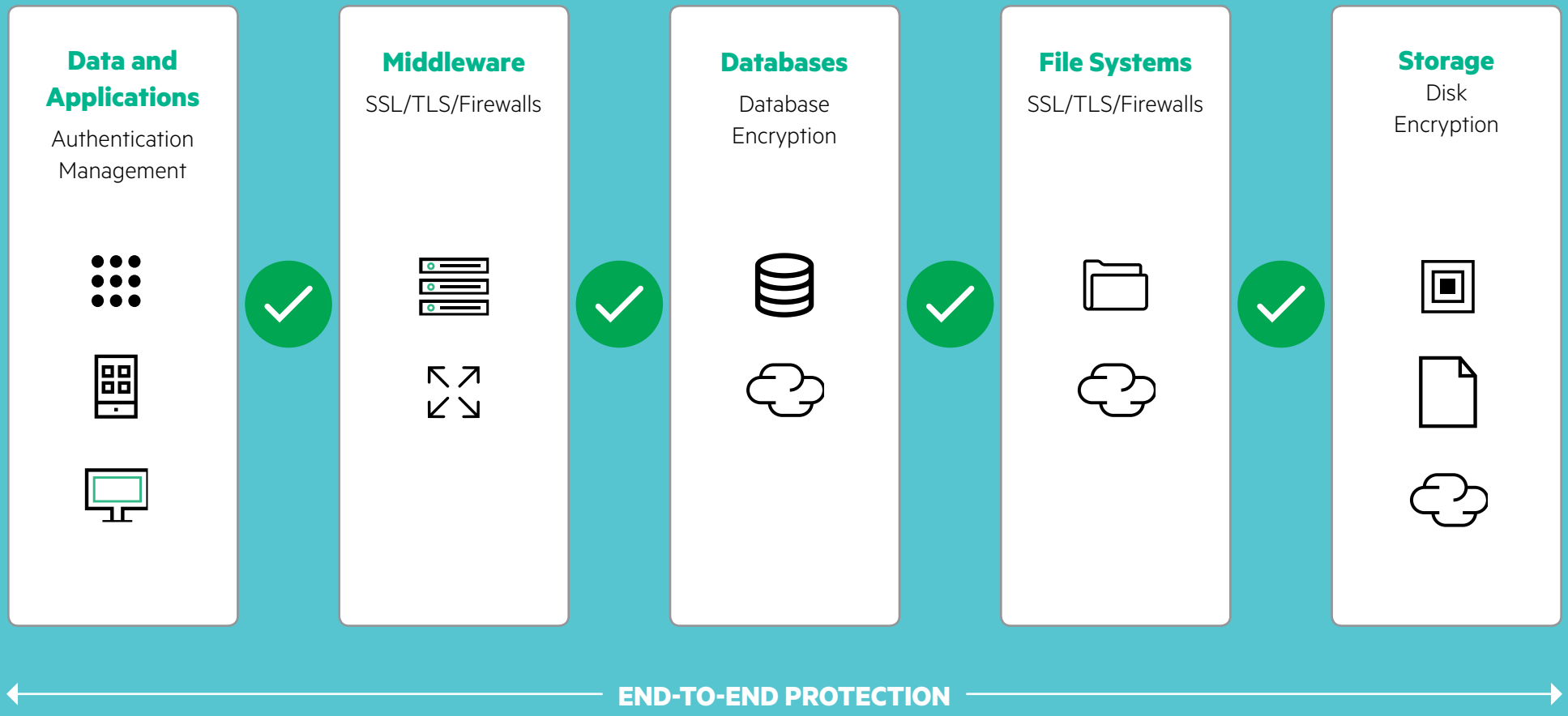


NIST standardized, FIPS validated.

HPE SecureData with Hyper FPE delivers a NIST-standardized method of protecting data at-rest, in-motion, and in-use, and maintains the format, meaning, value and logic in the data. HPE SecureData also has the world's first FIPS-validated AES-FF1 encryption configuration option to operate in strict FIPS mode, delivering a proven method of protecting data for U.S. federal agencies and departments, and global enterprises.

HPE SECUREDATA: END-TO-END PROTECTION FOR DATA IN-USE, IN MOTION AND AT REST.

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



NOT ALL FPE TECHNOLOGIES ARE CREATED EQUAL:
HPE SECUREDATA WITH HYPER FPE

HPE SecureData with HPE Hyper Format Preserving Encryption (FPE) can encrypt virtually unlimited data types. Hyper FPE technology delivers a proven method of protecting data that enables 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 classified data types that need encryption. Preserves format, relationships, context, meaning, and fit to legacy systems.

Hyper usability

Give data scientists, analysts and developers wide access to de-identified data, powering 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 is fully integrated with HPE Atalla HSM, a FIPS 140-2 Level 3 validated hardware appliance, offering organizations greater physical and logical data protection. HPE Atalla HSM stores and manages root keys, with centralized configuration and security policy enforcement.

BENEFITS TO GOVERNMENT DEPARTMENTS, AGENCIES AND CONTRACTORS

- Protect high value data such as Personally Identifiable Information (PII), Personal Health Information (PHI) and classified data.
- Layer data-centric security into decades - old legacy systems and applications.
- Safely expand access to de-identified data, expand big data analytics.
- Enable departments and agencies to share data (data portability), improve citizen services, and collaborate with others, including contractors.
- Enable growth of digital government and transparency initiatives.
- Adopt innovations such as cloud computing, Hadoop, and IoT.
- Leverage a brand new tool when building compliance programs for regulations such as the **Cybersecurity Act of 2015, DFARS CUI, and General Data Protection Regulations (GDPR)**.

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

Governments need to meet advanced security requirements for the protection of their nuclear weapons systems. HPE SecureData protects mission-critical, weapons-systems data by automating key management for thousands of encrypted disk drives.

Defending healthcare data

Protecting healthcare data is a top priority for any federal agency. HPE SecureData helps protect sensitive healthcare data, enabling agencies to meet assurance and risk reduction guidelines for personal health information (PHI), and unifying controls with a single pane of glass that simplifies management.

Analyzing economic data securely

Protection of high-value data needs to be balanced with the use of this data for analytics. HPE SecureData protects PII, economic and other sensitive data on the analytics platform, enabling 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—with FIPS 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 a 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.

Our data-centric security solutions are used by six of the top eight U.S. payment processors & nine of the top ten U.S. banks. HPE Security-Data Security has enterprise customers across industries including transportation, retail, financial services, payment processing, automotive manufacturers, insurance, high tech, healthcare, telecom & public sector across the Americas, Europe, Asia-Pacific and Africa.

HPE Security-Data Security is a key contributor to new data security standards through leadership and innovation with over 80 patents and 51 years of expertise.

Learn more at:
voltage.com/solutions/industries/government/

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

2017, Rev 1.