Hewlett Packard Enterprise

Business white paper

Mainframe Data Protection in an Age of Big Data, Mobile, and Cloud Computing

HPE SecureData z/Protect

The Imperative for Data-centric Security

Compelling business value propositions such as improved time-to-insight, customer access, business agility, and cost savings are driving rapid adoption of Big Data, mobile, and Cloud computing. While these technologies offer extraordinary opportunity for businesses, they also cause the traditional IT security perimeter to dissolve. As data becomes the most valuable corporate currency, it is subject to increased privacy and compliance regulations and ever more advanced, persistent cyber-threats.

As frequent, massive data breaches have demonstrated, holding, processing, and transmitting data can be perilous if it isn't properly protected for its entire lifecycle. But most data protection schemes impose adoption, staffing, and overhead burdens, and leave "gaps" between islands of security-insufficient to defend against modern advanced persistent threats (APTs).

Add the rising tide of data privacy regulations, from Sarbanes-Oxley to HIPAA to HITECH to PCI DSS, the EU's General Data Protection Regulation (GDPR) data privacy legislation, and beyond, and protecting corporate data becomes even more critical; even without an actual breach, non-compliance can be costly.

But most enterprises find that even contemplating a data protection project is daunting, due to their volume of applications and databases. This is particularly true given that most approaches to data protection require modifications to every application.

The IT organization urgently needs a better, more comprehensive security strategy-to enhance mainframe data protection even while it enables the secure movement, access and use of data throughout the enterprise.

"Information is where the money is...information processing has now become the means of production, providing the underlying value in almost everything we do in business today."

- Ed Ferrara
Forrester Research, Inc.,
Determine The Value Of Information Security Assets And Liabilities — Information Security Economics 102, 2013

ETL Offload Use Case:
Mainframe-based Big Data is typically made accessible on other platforms such as Hadoop, Teradata, or IBM's Netezza, all of which lack mainframe-grade protections. Flexible HPE SecureData synergies provide secure Big Data storage, processing, movement, and availability in and between all environments. Protecting data first with HPE SecureData z/Protect avoids data breaches at rest and in transition between SSL and secure repositories, no matter whether mainframe data is pumped into Hadoop Distributed File System (HDFS) via extract/transform/load (ETL) tools, the Sqoop JDBC connector, or other means of ingestion.

Heightened Threats and Compliance Challenges

System z-though justifiably legendary for strengths such as reliability, availability, serviceability, and scalability falls short in enterprise class data protection. It provides powerful building-blocks for security, but these facilities require significant "assembly before use". And a z/OS-only solution does not address broader ecosystem issues, like mobile devices, Cloud, Hadoop, or even global business partners who need data access.

Traditional all-or-nothing data protection leaves the data vault either sealed tight or wide open.

- Hardware-, filesystem-, and database-level encryption approaches are appealing because they provide transparent data protection, requiring no changes to applications. However, that transparency means that such point solutions fail to provide the separation of duties mandated by regulations.
- Point solutions—home-grown or conventional encryption or tokenization—may seem simple at first, but management difficulty grows exponentially. Solutions requiring storage of live credit card data, for example, not only grow in complexity but also remain in scope for PCI DSS compliance audits.
- Point solutions also increase disclosure risks, since they only protect data "below" the layer of protection: hardware-level encryption is meaningless to any program that can read the disk, file system-level is bypassed by any program that can read a file, and so on.
- Most encryption changes data formats, requiring database schema changes; worse, it renders data into unpredictable character sets and field lengths.
- First-generation and home-grown tokenization technology simply does not scale, due to issues like database backup and replication, failover, key management, and data integrity problems arising from database synchronization issues.
- Finally, the growing requirement for System z participation in Big Data introduces new risk-management challenges, uncertainties, and decisions. For example, when mainframe data repositories are accessed, analyzed, and mined as Big Data, where should they be protected? While System z processing can be expensive, z/OS is vastly more secure than Hadoop. If data is protected before it leaves z/OS, it remains safe throughout its journey.

Which way forward?
What's required is a comprehensive way to easily integrate data protection and regulatory compliance that leverages existing investments in technologies such as System z, as well as people and processes. Success metrics can be identified in terms of reduction in PCI compliance costs and audit scope, shrinking the cost of breaches, and improving service to lines of business with enhanced access and speed of data flow. The most effective data protection is clearly end-to-end, at the application level—encrypting or tokenizing specific fields containing sensitive data at the point where the data is collected or created, then decrypting or detokenizing only when appropriate, under site-specified policy control.

Such data-centric security provides superior information protection by persistently protecting the data itself, far outshining just securing end-point servers and networks where data resides. A data-centric strategy empowers IT to quickly respond to ever-evolving security and compliance requirements, by securing data at its inception.

HPE SecureData z/Protect: Easy, Native Data Protection

A data protection technology is no stronger than the underlying hardware/software platform on which it is built. HPE SecureData z/Protect is faithful to industry-leading native mainframe strengths, preserving and extending System z security. It isolates via built-in z/OS and System z hardware facilities, and cannot be subverted by flawed or malicious application programs. HPE SecureData z/Protect provides separation of duties through granular data protection access controls, defined by policy and mediated by standard z/OS security facilities (RACF, ACF2, or Top Secret).

HPE SecureData z/Protect is part of the HPE SecureData platform, widely used in diverse installations on virtually all platforms. HPE SecureData provides proven, peer-reviewed, patented data protection—encryption and tokenization at the data field level—with far less implementation and operational impact than alternatives. It offers flexible toolkits and services to rapidly integrate data protection with current IT infrastructure, from mainframe to open systems and in a wide variety of languages-including providing native tokenization and encryption on System z with little or no data structure changes, while correspondingly minimizing application changes. Innovative, patented and standards-based HPE SecureData technologies reduce application changes to hours or days, not months or years. HPE Format-Preserving Encryption (FPE) and HPE Secure Stateless Tokenization (SST) technologies simplify processing and enable secure use and analytics on protected data, since data size and character set are unchanged when data is protected. HPE Stateless Key Management eliminates the complexity of key management, with its ever-growing databases requiring constant replication and backups, tedious DR procedures, and lengthy key rollover processes.

HPE Format-Preserving Encryption (FPE)
HPE FPE is a fundamentally new approach to protecting structured data—names, addresses, credit card PANs (Primary Account Numbers), Social Security numbers, etc.—integrating data-level protection into application environments that were previously difficult or impossible to address. It uses a proven, peer-reviewed AES encryption mode (NIST SP 800-38G) to encrypt data without altering data size or character set. This enables data protection with minimal modifications to existing applications and data stores.

HPE Secure Stateless Tokenization (SST)
HPE SST is an advanced, patent-pending data security technology for payment card data, with significant PCI DSS audit scope reduction. HPE SST dramatically improves speed, scalability, security, and manageability over first generation tokenization approaches. By removing the data vault employed by older tokenization solutions, HPE SST eliminates data integrity, management, and replication issues. HPE SST uses static, pre-generated tables containing random numbers created using a FIPS random number generator.

HPE Stateless Key Management (SKM)
HPE SecureData includes highly efficient HPE Stateless Key Management technology that generates and manages encryption keys. Unlike traditional systems requiring complex, ongoing backup procedures, it derives keys "statelessly" on demand, requiring backups only when the configuration is changed. SKM supports multiple authentication methods for flexible access control, and authentication settings can be changed as requirements evolve. This single key facility centralizes governance, management, and administration, and ensures secure, reliable, consistent key management enterprise-wide.

Integrating HPE SecureData z/Protect with z/OS Applications

Applications using HPE SecureData z/Protect add a single line of code to protect or unprotect a field. Programmers need no knowledge of cryptography: the z/Protect administrator defines the operations available, and native system security controls determine who has access to those operations. Cryptids, a z/Protect construct, simplify application development via abstraction. Defined in the (secure) started task configuration, they combine all aspects of a data protection definition into a single named entity.

With their customer-defined names, Cryptids are much easier to use and manage—and are less error-prone—than ciphers, key names, options, etc. Centralized administration ensures that applications use correct data protection operations, and provides granular, policy-based controls, such as limiting which users can protect/deprotect. In addition, application programs don't need security credentials because the job owner or CICS user id provides the authentication. The started task architecture also facilitates auditing operations (answering, "How much does application XYZ use data protection?") and chargeback (billing for each operation).

HPE SecureData z/Protect provides enterprise-ready mainframe data protection by interoperating with the overall HPE SecureData platform; hybrid computing support maintains the critical/central mainframe role as data repository, while exploiting other platform strengths. Data protected on z/OS can be translated from EBCDIC to ASCII without decryption or detokenization, transferred to distributed platforms, and then unprotected there as needed. This works because HPE SecureData for z/OS converts data to Unicode before protecting it, so if "1234" protects as "5678" in EBCDIC, it does in ASCII, too, and is thus interoperable.

Native encryption and tokenization services across z/OS environments, including CICS, IMS, DB2, MQ, and batch, enable comprehensive cross-application and cross-platform compatibility, speeding application implementation, security retrofitting, and minimizing training requirements.

Benefits of HPE SecureData and z/Protect

The HPE SecureData z/Protect solution is not just a new way to protect mission-critical enterprise data end-to-end, but a new way to process protected data.

Preserves and extends mainframe security
Since applications using HPE SecureData no longer contain sensitive data, there's no ability to decrypt or detokenize data without authorization. And as data moves between platforms, it stays protected: a value protected in EBCDIC can be translated to ASCII, and still decrypted or detokenized correctly. HPE SecureData protects sensitive data so that in the event of a breach, a hacker only acquires useless protected data.

Reduces audit/compliance scope
Proper governance is essential for protection, reliability, and compliance, but is too often an afterthought. Data residency laws can place complicated requirements and constraints on IT strategy—from delaying adoption of distributed application architectures, including Big Data and Cloud, to requiring expensive in-country data center operations with dedicated staff. United States and European Union cross-border data laws, offshore banking rules, and federal mandates also have conflicting data governance requirements, leading to high compliance complexity and costs. With z/Protect, burdensome and expensive compliance auditing is minimized because most applications operate transparently on protected data—at the same time mitigating risk of breach.

Faster data protection without disruption to existing processes
Complex environments impose technology requirements. A significant z/OS security shortcoming is the lack of application-level data protection facilities for Customer Information Control System (CICS), used by the vast majority of z/OS customers. z/Protect provides fully compatible data protection services across all z/OS environments, including native CICS APIs, allowing the HPE SecureData platform to provide comprehensive cross-application and cross-platform compatibility, speeding application implementation and security retrofitting, and minimizing training requirements.

HPE SecureData z/Protect has a centralized design that not only provides better control and management, but also enables faster auditing. Every data protection operation can be accounted for, on a per-user or per-application basis. As data protection usage grows, this allows verifying that applications are using it as mandated, and allows chargeback to business units for resources used. z/Protect can generate standard z/OS SMF data, seamlessly integrating with enterprise performance tuning and capacity planning processes.

Besides HPE Format-Preserving Encryption, z/Protect Cryptids can perform a rich set of other cryptographic operations, including Advanced Encryption Standard (AES), HPE Secure Stateless Tokenization, and various digest functions. Using the identical API, these further simplify use by application programmers.

How Did They Do It?
Telecom—Critical Infrastructure

Challenges:

- Mission-critical project with high visibility
- Petabytes of sensitive data to protect, dozens of data types (PII), several hundred apps
- Brand risk and breach mitigation
- Compliance cost and scope reduction; covered by nearly every privacy regulation: PCI, HIPAA, state privacy laws, etc.
- Multiple z/OS systems with CICS, IMS, DB2, VSAM, and a wide range of other platforms

Solution:

- HPE SecureData selected and deployed at approximately 15-30 applications per month
- HPE SecureData z/Protect for mainframe data protection
- HPE FPE on z/OS shares protected data with ASCII systems
- Embedded HPE FPE as a corporate standard
- Currently protecting data in > 10,000 servers, petabytes of data

Benefits:

- Enterprise-wide data-centric protection
- Speedy implementation, with minimal or no application changes
- RACF exploitation fits z security model; SMF data integrates with operations processes
- HPE Stateless Key Management technology ensures easy Disaster Recovery

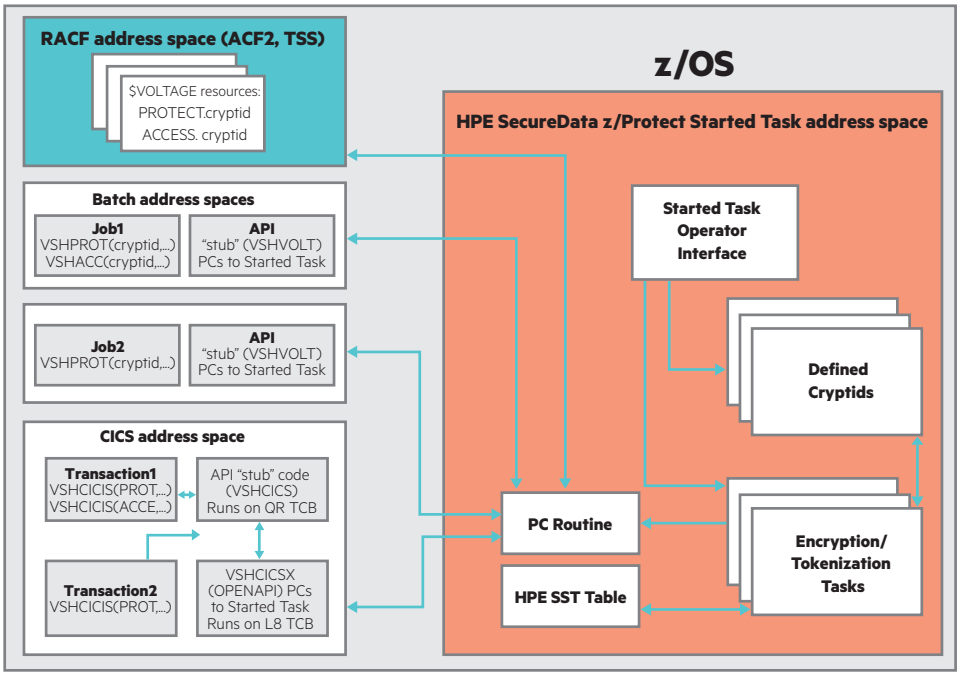
HPE SecureData z/Protect Enables Data-centric Security Enterprise-wide

Data-centric protection with HPE SecureData z/Protect enhances and extends System z security, maximizing return on value of data resources and providing compelling value from the mainframe as enterprise repository and server.

Overall, the HPE SecureData Enterprise data security platform unites market-leading encryption, tokenization, data masking, and key management to protect sensitive corporate information in a single comprehensive solution. HPE SecureData z/Protect, designed for z/OS, implements native data protection on System z, while providing full interoperability with HPE SecureData on other platforms.

The HPE SecureData framework ensures that sensitive and regulated data, including customer, financial, employee and partner data, remains protected anywhere it moves, anywhere it resides, and however it is used.

HPE SecureData



HPE SecureData z/Protect Architecture (Batch and CICS)

Learn more at
voltage.com
hpe.com/software/datasecurity

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-0083ENW, May 2016, Rev. 1