Hewlett Packard Enterprise

Business white paper

Protecting Data Into and Throughout the Cloud

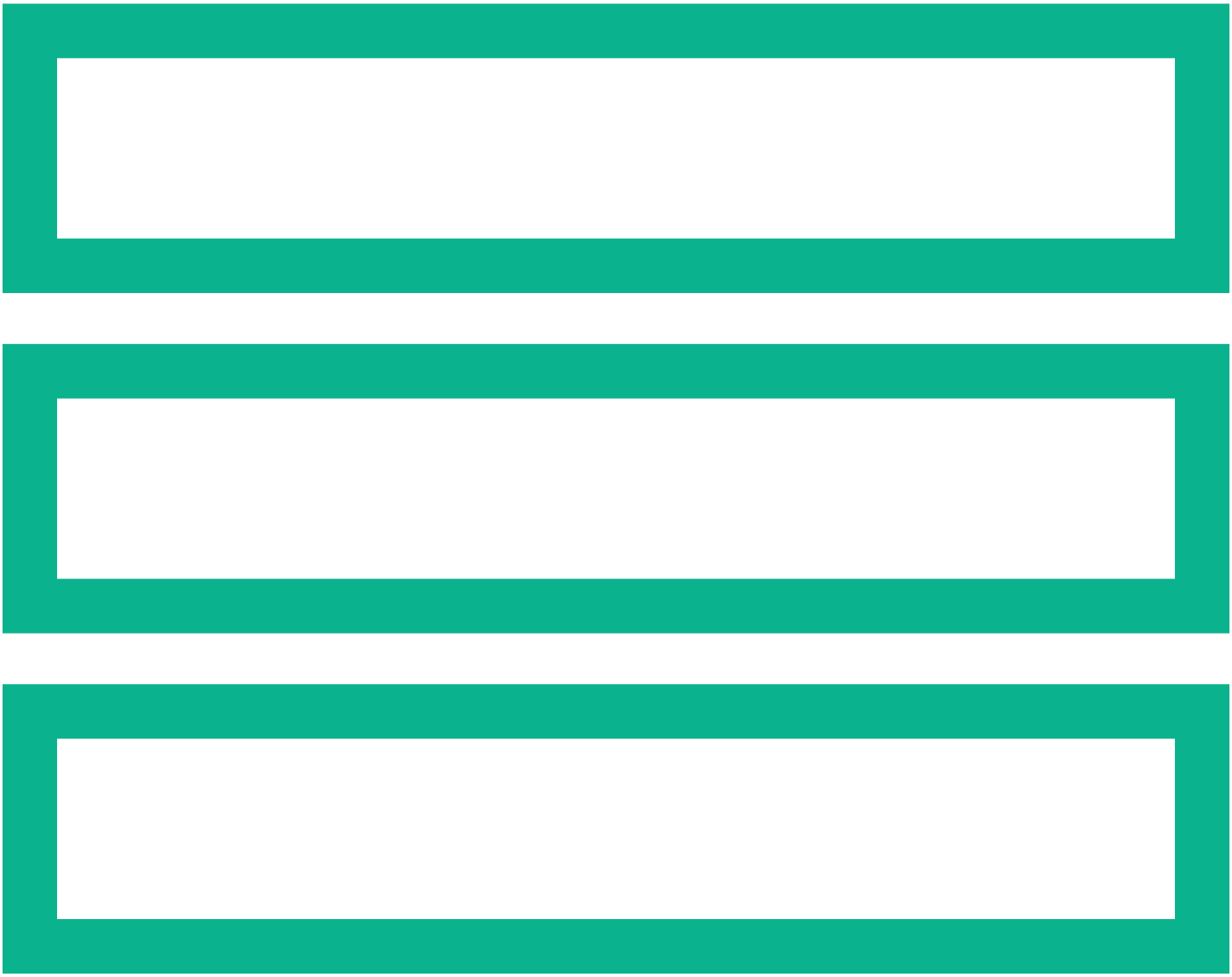


Table of contents

The Cloud Outlook: It Changes Data Security—Forever

In the borderless world of Cloud computing, everything changes. You cannot deliver Cloud without a fundamental redesign of your security infrastructure. Period.

"Data security and privacy are the top concerns that must be overcome as companies decide whether, and how, to migrate to the Cloud."

– Cloud Industry Forum "UK Cloud Adoption and Trends for 2013." **cloudindustryforum.org**

With information in the Cloud, suddenly a new team of people has access to your data. At every turn, they are working hard to protect, tackle, and block access to sensitive data in 'your' infrastructure. In fact, to protect your data in the Cloud, several of the fundamental building blocks of a secure enterprise IT infrastructure have to be re-envisioned. Make no mistake, this new realm will forever shatter the traditional infrastructure toolset.

Think of it this way: Your company's data center may now be run by people you don't employ or manage, making you reliant on their security decisions for infrastructure such as networks, administration, databases, patches, and updates. In addition, your Cloud applications and data may sit next to, or even be highly shared or co-located with other customers, even potentially competitors. Making matters more complex, with Cloud computing, sensitive data may be governed by different rules and requirements in different countries, yet can be pushed and pressed to the far reaches of the globe nearly instantaneously. This could trigger unintended violations in privacy and personal information records that by law should never even leave certain countries or jurisdictions in readable formats. While the speed and scalability of Cloud computing offer significant advantages in enabling your company to optimize your IT resources, speeding up business processes and new service deployments, it also means that your firm needs security and data protection that's adaptable, highly available, scalable and supportive of your ongoing business goals.

Companies everywhere are increasingly adopting Cloud computing strategies to gain significant market advantages and broad economic savings versus an on-premise solution and an on-demand, dynamic allocation of resources all enabled with reallocated staff and resource. Beyond the economic incentives of moving data management, business and analytic processes, and existing IT infrastructures into the Cloud, it also significantly improves the ability to scale a solution. It speeds time to market and provides rapid deployment for companies in a broad cross section of industries. According to IDC, a five-year total savings from an online Cloud-based solution can be over 80 percent or more than $516,000 per application. Yet for companies managing sensitive corporate and customer data, including credit cards, medical data, or corporate financial data, adopting new Cloud capabilities is fraught with security challenges that get at the foundation of the Cloud architecture. Namely, how do you protect your data into and throughout the Cloud? How do you achieve rapid and efficient regulatory and data residency compliance, and increased responsiveness and control? How do you truly realize the efficiencies, faster time to market, and cost savings opportunities afforded by Cloud services, and do so without compromising the control and protection of critical business data?

This white paper explores these topics, highlighting current Cloud-based data protection requirements, and offers an innovative look at a data-centric protection strategy that extends privacy controls to several key Cloud paradigms. With a data-centric approach, companies can deliver a comprehensive data protection strategy that protects any data before it enters the Cloud, and continues to do so as it moves throughout the Cloud. It is a flexible, scalable, end-to-end protection strategy that provides a unique platform for rapid adoption of Clouds by even the most security demanding business and enterprise applications.

Why Other Cloud Security Solutions Fall Short

With the new technology enablers around mobile, Big Data, and SaaS applications, the advantages of adopting Cloud-based IT applications and services are accelerating. Yet, at the same time, companies are mindful of the new security challenges presented, and are hardpressed to take full advantage of Cloud-based IT infrastructures if there are corresponding increases in the risk of data loss or compliance violations. Companies today must take into account increased requirements for data protection, as well as compliance with security and data residency regulations, both domestic and international.

With Cloud, traditional endpoints and boundaries don't exist anymore—data is the new boundary. Since data now dynamically travels anywhere and everywhere, armoring the repositories and applications where data is stored simply doesn't work. Even if you could manage to keep up with the rapid-fire changes in infrastructure by installing and managing security solutions from a wide range of vendors, you will still have security gaps in between the armored repositories. Today, many firms are offering Cloud security solutions piecemeal or ad-hoc. These solutions attempt to leverage traditional security technologies in new Cloud environments. Unfortunately, these solutions are ineffective as they cannot adequately address the new security challenges presented by the Cloud. Several of these traditional security technologies include:

- **Host solutions:** These solutions are typically deployed at each desktop, and cannot easily be retrofitted to Cloud environments. Using existing end-point security products limit your organization's ability to effectively protect data. This is because data no longer moves between applications and data repositories in static, well defined paths to fixed limited applications.
- **Network or point-to-point offerings such as Secure Socket Layers (SSLs) or Virtual Private Networks (VPNs):** These solutions cannot address the reality that in Clouds, data travels everywhere and anywhere. While in an ideal world, sensitive data could travel in well-defined paths from data repositories to a well-understood set of applications. In the real world, the IT environment consists of a constantly shifting set of applications running on an ever-evolving set of platforms. In larger enterprises, for instance, the data lifecycle is complex and extends beyond the container and applications, often falling outside traditional enterprise IT departments into places like offsite backup services, Cloud analytic systems, and outsourced service providers. So armoring the repositories, applications and links doesn't provide the needed protection, since data won't stay in one place. And having to manage infrastructure from a wide-range of vendors opens up security gaps.
- **Cloud-based access control:** For some organizations, a Database Access Control (DAM) or generalized Identity and Access Management framework is an important building block for managing and controlling who can access what types of systems, applications, and data sets. However, access control on its own will not stop or prevent certain Advanced Persistent Threats (APTs) or privilege escalation attacks that will essentially sidestep or work around these controls. These systems can complement, but likely not entirely replace, data protection strategies that lock data even from insiders with access to Cloud applications.
- **Cloud-based encryption:** These solutions approach the problem by encrypting entire data-stores with technologies such as Transparent Data Encryption (TDE) or encrypting each and every Virtual Machine (VM), and cannot achieve any level of granularity 'underneath' the protection at the container level. In other words, any calling application or user that needs access to any part of an encrypted database generally gets access to everything.

All told, these traditional approaches are complex, time-consuming, and inadequate for effectively protecting data into and across the Cloud.

Table 1: Past approaches to data protection are complex, time consuming, and inadequate to comprehensively protect data through the full life-cycle

TRADITIONAL METHODOLOGY	CHALLENGES
Whole Database Encryption	• Encrypts data within db, degrades application performance • No granular access control • Separate solution for each database vendor • No separation of duties—DBA can decrypt • No security of data within applications and networks
Database Column	• Encyrpts data via triggers and stored procedures • Requires schema changes • No data masking support or separation of duties
Native or Traditional Application-level Encryption	• Encyrpts data itself, throughout lifecycle • Required database schema and application format changes • Heavy implementation costs
Shuffling	• Shuffles existing data rows so data doesn't match or align • Breaks referential integrity • Can still leak data
Data Tables and Rules	• Consistently maps original data to fake data • Allows for referential integrity, reversibility • Security risk due to use of lookup tables
Non-Proven, Non-Reviewed Encryption	• E.g., stream ciphers, alphabetic substitution • Not secure, easily reversible by hacker • Key management challenges

The Need for a New Security Paradigm

Faced with an architectural re-design that introduces new exposures to your data, the best way to retain enterprise control is to shift to data-centric security an approach that is extensible and adaptable across multiple applications and systems throughout Cloud environments. In this way, the only boundary is the data itself. In other words, if you have assets that are out in the Cloud and shared with third-parties, there is no way to lock it, or tunnel it anymore; the only way to protect that information is to secure it at the data level. That's a control point you can own. When data is protected at creation, before it moves out of the enterprise or as it is entering the Cloud, it offers a comprehensive data protection strategy that will enable your business to capture the efficiencies and cost savings by moving to the Cloud.

Cloud systems also require a shifting set of applications running and accessing data in a complex, dynamic set of data repositories, which often extends the definition of the application to include backup, analytic systems, outsourced providers, and additional third parties accessing Cloud applications. Often times, the most highly sensitive data, such as personal and payment identifiers, transactions will flow through many applications and data stores, which all must be protected to secure data in the Cloud. As mentioned above, this means that locking the repositories, applications, and links doesn't provide complete protection because the data is in flight and won't stay in one place.

Many companies today see a need for a single unified architecture for Cloud, hybrid, on premise, mobile, mainframe and Big Data environments. There is a critical need for 21st century architectures to have these traits: be controllable, resilient, adaptive, and data-driven. In today's world, application deployment is now about small, loosely coupled stateless building blocks. Modern architectures today go beyond the constraints of the old hardware server-centric model.

"Protecting against the exposure of confidential and sensitive information to unauthorized systems or personnel, as well as protecting against confidential data loss or leakage are the top-ranked challenges related to securing information within the cloud that a data centric security solution should address."

– Information Security professionals, from a 2011 (ISC)2 Survey

The right Cloud data protection strategy can make all the difference, and requires a data-centric approach. Only this approach provides the necessary levels of data protection, enabling your business to capture the efficiencies and cost saving by moving to the Cloud.

A data-centric approach can deliver the following benefits:

- Comprehensive data protection for structured and unstructured data, across the entire data life cycle
- Increased ability to rapidly and efficiently meet and maintain regulatory and data residency compliance requirements
- Increased responsiveness to the business and management control of data, scalable to support business processes that requires secure data

Where Data-centric Meets the Cloud: The HPE SecureData for Cloud Security Solution

Data-centric strategies can protect sensitive data as soon as it is acquired and ensure 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. HPE SecureData for Cloud provides two technologies for protecting data: HPE Format-Preserving Encryption (FPE) and HPE Secure Stateless Tokenization (SST) technology. These independent methods are proven to protect while preserving data format and other attributes, effectively building protection into the data itself. Replacing the original data with either an encrypted value or a random token narrows the possible exposure and can greatly reduce audit scope and compliance costs.

In this way, HPE SecureData for Cloud delivers a comprehensive data protection solution to protect any data before it enters, and as it moves, in and through the Cloud. The solution addresses application security, database, data warehouse, ETL, and online application protection for structured, semi-structured, or unstructured data.

Key Differentiators of the HPE SecureData for Cloud Solution

Data-centric Encryption
Cloud architectures remove the traditional IT infrastructure edge points such as the WANs, LANs, WLANs, or VPNs/Firewalls found in traditional enterprise infrastructure. HPE SecureData for Cloud allows enterprises to lock the protection of the data in place, achieving data protection via encryption, masking and tokenization that can protect data without fixed boundaries and as data moves across all application, storage, and compute environments of the Cloud.

With HPE SecureData for Cloud Solution, data agnostic of type or source is encrypted at capture and protected throughout the entire data lifecycle, wherever it resides and wherever it moves. In other words, the protection travels with the data, eliminating traditional security gaps in transmission into and out of different network and external environments. This means that data can be protected and shared enterprise-wide without the need to encrypt/decrypt as the data enters or leaves environments, thus also reducing the bottlenecks that often degrade performance.

"Market research firm Gartner recommends that enterprises adopt measures that will simultaneously boost the security of sensitive data as well as assist them in satisfying regulatory compliance with data resiliency laws."

– Gartner Research, "Five Cloud Data Residency Issues That Must Not Be Ignored "

HPE Format-Preserving Encryption—Data Masking and Referential Integrity for Common Identity
HPE SecureData for Cloud uses HPE Format-Preserving Encryption (FPE), a fundamentally new approach to encrypting structured and unstructured data. It protects data, while keeping the same size and format, and helps preserve business operations and data that are hidden no other vendor's encryption technology can do this. This HPE SecureData for Cloud innovation makes it possible to integrate data-level encryption into legacy business application frameworks that were previously difficult or impossible to address. It uses a published encryption method with an existing, proven algorithm to encrypt data in a way that does not alter the data format. The result is a strong encryption scheme that allows for encryption with minimal modifications to the way that existing applications work.

In supporting enterprise Cloud security, HPE FPE retains the structure of the original data set, while ensuring the protected data still fits into existing schemas. The fact that an encrypted value has the same size and format as the original enables HPE FPE to be used with little or no changes to database schemas and applications. It includes data masking that protects identity by masking a field such as address but keeping a field such as state, thereby maintaining usability for analytics in low-trust or untrusted environments such as Big Data and Cloud services. HPE FPE preserves referential integrity which enables the same individual to be identified in protected data in different data stores and applications. This is important for applications that depend on the pervasiveness of common identification data, such as credit card numbers or social security numbers. With HPE FPE, data can be analyzed without having to decrypt it first, and the same infrastructure serves people with different privilege levels, thereby simplifying administration HPE SecureData for Cloud techniques for masking, tokenization, and encryption all maintain a common, identically formatted representation of data in every instance, ensuring consistency and reversibility across the Cloud.

High Performance Processing—Ability to Encrypt Terabytes on the Fly
High performance encryption results from eliminating constant encryption and decryption processes as data moves through the enterprise. HPE Stateless Key Management and HPE Secure Stateless Tokenization (discussed below) also remove performance bottlenecks and enable linear scalability. Encryption can be performed locally at the application, database, or webserver level, and HPE FPE can encrypt terabytes of data on the fly into one node or thousands of nodes in parallel.

HPE Stateless Key Management—Reduces IT Maintenance Complexity

HPE Stateless Key Management eliminates the need for dedicated IT headcount for key management because it removes the need to constantly backup key stores a huge advantage. HPE Stateless Key Management provides keys automatically with no storage or database management issues because database synchronization and frequent backups are not required. Key management can be linked to existing identity management infrastructure including roles and groups. Permission to decrypt or de-tokenize can be assigned on an application or user basis, and can be managed through external LDAP directories, taking advantage of LDAP groups to simplify user management. The result is role-based access to data at a data field level, mapping directly to enterprise data access rules and policies, and enabling extension of enterprise controls into the Cloud. These capabilities dramatically reduce the complexity of implementation and maintenance for IT security.

HPE Secure Stateless Tokenization—Meets Domestic and International Data Residency and Privacy Requirements

Cloud architectures offer new opportunities to scale your organization globally, driving the movement and consolidation of data into new territories, countries and regions around the globe, and triggering different country-by-country data privacy and data residency laws. HPE Secure Stateless Tokenization (SST) technology can help with compliance while still offering the flexibility your organization requires. HPE SST is an advanced, patent pending, data security solution that provides enterprises, merchants and payment processors with a new approach to help protect payment card data. HPE SST technology is stateless because it eliminates the token database that is central to other tokenization solutions, and removes the need for storage of cardholder or other sensitive data. HPE SecureData for Cloud has developed an approach to tokenization that uses a set of static, pre-generated tables containing random numbers created using a FIPS random number generator. These static tables reside on virtual appliances commodity servers and are used to consistently produce a unique, random token for each clear text Primary Account Number (PAN) input, resulting in a token that has no relationship to the original PAN. No token database is required with HPE SST technology, thus improving the speed, scalability, security and manageability of the tokenization process.

HPE SST allows companies to meet national and international data residency and privacy requirements, as sensitive regulated data can be maintained in a valid jurisdiction with only a representation of the data being moved to other geographies for data processing and management. This allows in-scope data to be securely moved and stored across Cloud environments, and only be decrypted and used within jurisdictions where it is specifically permitted.

Cryptographic Standards and Proofs

HPE FPE and HPE Identity-Based Encryption (IBE) are based on industry standards, and are NIST validated. Published standards and security proofs from HPE Security—Data Security and qualified independent validation are critical to the enterprise for both risk mitigation and compliance. Conversely, solutions that have not been proven provide no assurances on back doors that create more security risk.

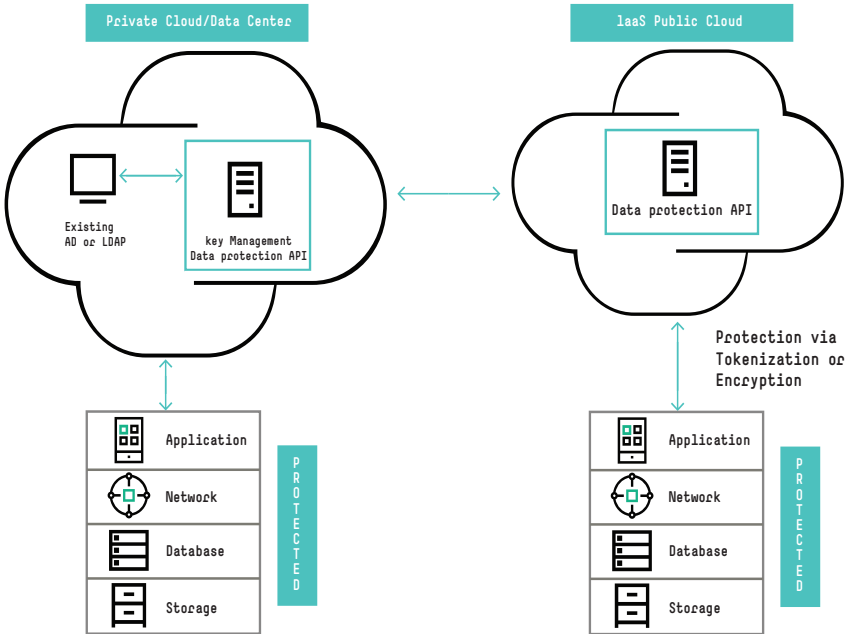
HPE Security—Data Security continues to innovate. Patents relating to HPE IBE and HPE FPE and other HPE Security—Data Security innovations have now been issued. HPE Security—Data Security also works closely with standards bodies such as the IETF and IEEE to explore making these technologies available to a broad range of ISVs through reasonable and non-discriminatory licensing.

NOTE: FPE is a mode of AES, recognized by the U.S. National Institute of Standards and Technology (NIST).

The HPE SecureData for Cloud Solution

HPE SecureData for Cloud solutions leverage core encryption and key management technology that protect data independent of the applications, storage methods, and subsystems that use it. Only this approach provides the necessary levels of data protection, and enables the business to capture the efficiencies and cost saving by moving to the Cloud. Data-centric protection extends privacy controls to sensitive data in several Cloud paradigms:

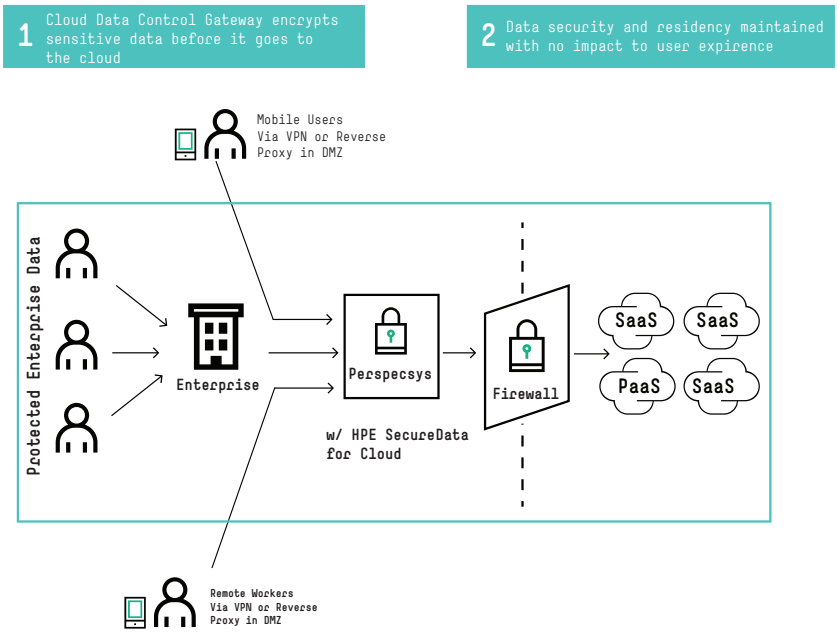
- **Information-as-a-Service (IaaS):** As a custom Cloud application, HPE SecureData for Cloud IaaS Solutions can help you control where and how data is exposed within the application architecture. In this solution example below, keys can be transiently used, and are never written to a disk in the Cloud—an important security point.
- **Platform-as-a-Service (PaaS):** As a custom Cloud application, HPE SecureData for Cloud PaaS Solutions at the platform level can help a company get ready for a big surge in traffic, as in this example of an insurance provider using HPE SecureData Web. Encryption takes place on the desktop or mobile browser before it gets to the Cloud, and is locked until it reaches its destination.



- **Software-as-a-Service (SaaS):** SaaS applications are taking even more control over data, how it is stored, backed up, archived, and accessed by Cloud system administrators. With HPE SecureData for Cloud, new Cloud security for SaaS applications renders all private data and attachments encrypted inside SaaS Clouds, bringing data access and audit control back to the enterprise. In other words, HPE Security—Data Security's data-centric solutions selectively protect data on the field and subfield level to keep sensitive data out of the Cloud while enabling Cloud applications to operate. A technology partnership between HPE Security—Data Security and Perspecsys further extends Cloud data protection capabilities and enables many types of data to be transparently protected in popular Cloud applications.

The combined solution—HPE Security—Data Security's patented Format-Preserving Encryption (FPE) integrated into Perspecsys' Cloud Data Protection Gateway leverages HPE Security—Data Security's innovations in end-to-end encryption and stateless key management with Perspecsys' award-winning Cloud data protection platform to give enterprises full control of their sensitive data, protecting it before it leaves the corporate environment for processing and storage in the Cloud. This helps address critical security and usability requirements associated with using encryption technology to safeguard sensitive information in Cloud environments, including the ability for encryption to work within Cloud application restraints; the necessity to be transparent to the end-users of Cloud applications; and the need for strong, industry-reviewed and approved encryption.

HPE SecureData for Cloud is part of the HPE Security—Data Security's data protection portfolio of products, including HPE SecureData Enterprise, HPE SecureData Web, and HPE SecureData for SaaS.



HPE SecureData Enterprise provides a comprehensive approach to enterprise data protection. It includes market-leading HPE Format-Preserving Encryption, HPE Secure Stateless Tokenization technology, HPE Stateless Key Management, and data masking to address the entire lifecycle of sensitive data as it moves through the enterprise and beyond. It also extends data protection beyond organizational borders, enabling protection of data to be shared with partners, suppliers, and outsourcers.

HPE SecureData Enterprise is the only comprehensive data protection framework that secures data as it is captured, processed, and stored across a variety of devices, operating systems, databases, and applications used by enterprises, merchants, and service providers.

HPE SecureData Web protects payment data captured at the browser, from the point the customer enters their cardholder information or personal data, and keeps it protected all the way through the web tier, the application tier, Cloud infrastructure, and upstream IT systems and networks to the trusted host destination.

HPE SecureData for SaaS protects data on the field and subfield level to keep sensitive data out of the Cloud while enabling Cloud applications to operate. HPE Security—Data Security and Perspecsys partnership enables many types of data to be transparently protected in popular Cloud applications.

The Bottom Line: Business and Technology Benefits of the HPE SecureData for Cloud Solution

The HPE SecureData for Cloud Solution delivers a data-centric approach that can help your company gain cost efficiencies and savings, and get to market faster. It delivers the greatest ability to protect sensitive corporate, financial and customer information and it can help you comply with security and data residency regulations and be more adaptive. Simply put, your organization can do more with less. It offers the advantages of scalability, flexibility, and developer efficiency.

- **A Single Data Protection Framework—**HPE SecureData for Cloud delivers a single framework that protects all enterprise data at the data level, enabling secure movement and use of data within Cloud environments. Cloud protection that can immediately integrate with virtually any application, ranging from purpose-built Web apps built around Linux Apache MySQL Perl/PHP/Python (LAMP) to the latest enterprise applications. SDKs/APIs and command line tools enable encryption and tokenization to occur natively on the widest variety of platforms, into portfolios including ETL, XML gateways, databases, and applications. The solution comprehensively protects all data before it moves into and travels through the Cloud.
- **Optimized Scalability and Performance—**HPE SecureData for Cloud has a scalable, client-server architecture that allows enterprises to push encryption services down to specific calling applications, databases, and web services, while centralizing key services in a separate key server system. By splitting encryption from key management, high performance protection can occur, and organizations can still retain control, management, security separation, and audit for all security operations from the HPE SecureData key server.
- **Streamlined Administration and Compliance—**Typical pilot installations take a few days and HPE SecureData for Cloud ensures that sensitive corporate data is protected, while efficiently meeting industry, regulatory and data residency compliance requirements. Cloud initiatives often aggregate data from global sources crossing national boundaries. With HPE Stateless Key Management, data can be analyzed in protected form in one jurisdiction, and data decryption de-tokenization applied in another jurisdiction where specifically permitted.
- **SaaS, PaaS, and IaaS Ready—**Whether you need to adopt new SaaS applications for customer relationship management (CRM) using applications such as Salesforce or Oracle CRM, or platform protection for Microsoft Azure projects, or fully host and build 100% web-based applications inside Amazon Web Services, HPE SecureData for Cloud has solution coverage to address application security, database, data warehouse, ETL, and online application protection for structured, semi-structured, or unstructured data moving to the Cloud.

Get the Best Cloud Coverage: Flexible, Scalable, End-to-End Data Protection From HPE Security—Data Security

In summary, HPE SecureData for Cloud delivers a comprehensive data protection solution to protect any data as it's created, before it enters the Cloud, and as it moves throughout the Cloud. Only HPE SecureData for Cloud delivers these key benefits:

- **Comprehensive Data Protection Across the Cloud for all Structured and Unstructured Data:** HPE SecureData for Cloud is a single framework that comprehensively protects all data at the data level, enabling secure movement and use of data within Cloud environments.
- **Rapid and Efficient Regulatory and Data Residency Compliance:** HPE SecureData for Cloud ensures that all sensitive corporate data is effectively protected, while efficiently meeting industry, regulatory and data residency compliance requirements. It ensures that corporate data is protected at the moment of creation or capture, before it moves into the Cloud.
- **Increased Responsiveness and Control:** With the HPE SecureData for Cloud solution, your business can quickly implement an enterprise data protection program to respond to Cloud initiatives and opportunities that deliver the efficiencies of moving your organization to the Cloud.

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

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-0830ENW, April 2016, Rev. 1