Hewlett Packard
Enterprise

Business white paper

Mitigate security risks and embrace the cloud

HPE SecureData for Cloud

The cloud has expanded your security perimeter, creating a more dynamic risk landscape. Build security into the fabric of your organization so you can enjoy the benefits of the cloud while proactively protecting the interactions among your users, applications, and data.

Table of contents

Cloud efficiency comes at a cost

For digital enterprises, leveraging cloud capabilities allows you to quickly act on new business opportunities and meet changing market demands. Microsoft® Azure Cloud is a consistent cloud technology platform that enables you to quickly build, deploy, and manage applications across a global network of Microsoft managed data centers. Microsoft Azure offers a growing collection of integrated services, such as analytics, computing, database, mobile, networking, storage, and web, all delivered on a pay-as-you-need model. This helps enterprises like yours address global markets and quickly develop new services while benefitting from a low-cost cloud-operating environment.

Yet if you're managing sensitive corporate and customer data, including PII (such as names, addresses, social security numbers, and national ID cards), credit card information, medical files, and financial data, you probably have already recognized that adopting cloud capabilities comes with significant security challenges. Sensitive data that moves into and across cloud-based infrastructures is at an increased risk for data loss and compliance violations. To best support the business, you need to find a way to realize the efficiencies, faster time-to-market, and cost savings of the cloud, without compromising the control and protection of critical business data.

So before you move sensitive data into the cloud, you'll need to be sure you can protect it at the point of creation, before it moves out of the enterprise, or as it is entering the cloud. And you'll also need to ensure rapid and efficient regulatory compliance. Achieving these goals requires a security and data protection solution that's data-centric, adaptable, highly available, scalable, and supportive of your ongoing business goals.

Take a layered approach to data security

In the cloud, data travels anywhere and everywhere, and is replicated into multiple systems. Cloud systems are comprised of a shifting set of applications running and accessing data in a complex, dynamic set of data repositories, which often include backup, analytics systems, outsourced providers, and third parties. The most sensitive data, such as personal and payment identifiers, often flow through many applications and data stores, all of which must be protected in order to effectively secure the data.

In this environment, the traditional approach of protecting the repositories and applications where data is stored is no longer enough. Even so, many cloud security offerings on the market attempt to translate traditional technologies to the cloud, resulting in complex, time-consuming, and inadequate approaches that fail to effectively protect data as it moves into, through, and across the cloud.

Hewlett Packard Enterprise believes that the best way to retain control and protection of sensitive information is to adopt a layered approach to security:

- One that goes beyond the constraints of the old hardware-centric model to be extensible and adaptable across multiple applications and systems throughout cloud environments
- One that provides a single unified architecture for public, private, and hybrid cloud, including on-premises, mobile, mainframe, and Big Data environments
- One that is controllable, resilient, adaptive, and data driven

HPE SecureData for Cloud is a unique, proven, data-centric approach to protection, where the access policy travels with the data itself, permitting data encryption and tokenization without changes to data format or integrity, and eliminating the cost and complexity of issuing and managing encryption keys. HPE SecureData for Cloud comprehensively protects all enterprise data end-to-end—from the moment of capture and as it is processed, used, and stored across a variety of devices, operating systems, databases, and applications—enabling secure movement and use of data in the cloud.

Enable secure analytics

Protect privacy and maintain compliance

Comply with PCI guidelines

Enable secure analytics

Big Data, including increasing amounts of data created by the Internet of Things (IoT), has created the need for storage infrastructures, whether on-premises or in the cloud. This data is ingested and stored in multiple locations, and then correlated via analytics for business insights.

While the mobile-cloud era has enabled Big Data analytics at an unprecedented scale, the data needs to be protected as it moves into and through cloud analytics applications, and across your geographically dispersed organization. Most enterprises have implemented multiple tactics to protect sensitive data, such as security policies, employee training, intrusion prevention technology, and corporate firewalls—but it is not enough. The only way to truly protect data is to make it worthless to an attacker or other unauthorized user.

HPE SecureData "de-identifies" data using National Institute of Standards and Technology (NIST) validated format-preserving encryption (FPE), secure stateless tokenization (SST), and stateless key management to render data useless to an attacker—without complicating workflows or compromising an application's ability to utilize the data. This kind of flexible, data-centric protection enables secure, cross-cloud analytics on data from your extended enterprise or between cloud systems.

Big Data analytics using Hadoop or other Big Data solutions provides an example of how this works in a real-world situation. In this scenario, the data needs to be protected while moving between the Hadoop ecosystem and your trusted data warehouse environments. HPE SecureData for Cloud de-identifies the data to be sent for analysis and then de-identifies it again before it is returned to the data warehouse. And HPE SecureData isn't just for Hadoop—it can protect sensitive data in the data lake, including Teradata, HPE Vertica, and other Big Data platforms.

Table 1: Key considerations for HPE SecureData for de-identification

Considerations	Solution benefits
How are you managing data masking in test environments? Is it the same solution for production data and analytics?	HPE SecureData for Cloud delivers a single platform with production, analytic, test, and development protection and masking—all in one platform—and enables database integrity across geographically distributed and large data systems.
Does the solution require additional servers or databases, or increase management cost and complexity? What is the cost to implement and maintain it?	Because of its stateless solution, HPE SecureData for Cloud eliminates the need for mapping tables or databases, so it is well suited for projects requiring high scalability, and requires less than 0.1 full-time employee (FTE) per data center.
Can you easily incorporate data de-identification into existing workflows such as extract, transform, load (ETL) or data sub-setting tools? Does the solution support a heterogeneous data management environment?	HPE SecureData for Cloud builds data masking into existing workflows and data management frameworks using a set of APIs and processing tools that are compatible with ETL and data management solutions across Linux®, UNIX®, Windows®, IBM z/OS mainframe, HPE NonStop, Stratus, Teradata, Amazon Web Services, Microsoft Azure, Hadoop, and technology integration with Informatica.
Can you reverse the data masking? How is that done, and can it be done securely and without risk?	Securely reverse masked data through centralized key management to its original state, or make it irreversible using one-time, 256-bit format-preserving encryption (FPE) keys.
How are you masking data for secure analytics in Big Data platforms such as Hadoop?	HPE SecureData supports Big Data initiatives—it's available for Hadoop and certified for Cloudera, MapR, IBM Big Insights, and Hortonworks.
How does the solution support access rules from Active Directory, LDAP, or other systems?	On-the-fly masking dynamically applies access rules based on input from Active Directory, LDAP, or custom identity and access management (IAM) systems.
Is the solution built on proven security standards? Will it provide a safe harbor in the event of data breach?	HPE has a proven Security Leadership track record with NIST, ANSI, IEEE, and IETF Standards Bodies, where HPE SecureData data protection technology breakthroughs are published.

Protect privacy and maintain compliance

The sophistication and persistence of criminal attacks in online systems is growing, along with government regulations requiring adequate data protection measures and full disclosure of breaches. At the same time, cloud computing allows sensitive data to be pushed to the far reaches of the globe, which can create obligations under international data privacy regulations. But no matter where your data roams, your compliance mandate remains the same: you must own, maintain, and protect data wherever it is—including as it moves into and out of the cloud, as well as if you remove it from audit scope.

HPE SecureData for Cloud allows you to protect sensitive data—such as personally identifiable information (PII) and personal health information (PHI)—to remain in compliance with regulations such as the healthcare information portability and accessibility act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and the General Data Protection Regulation (GDPR), along with many more state, national, and international data privacy regulations. It can also help you extend Payment Card Industry Data Security Standard (PCI DSS) compliance into the cloud.

In addition, HPE SecureData for Cloud enables you to quickly pass audits and implement full end-to-end data-centric protection to greatly reduce the risks and impact of data breaches. And if there is a breach, the data is useless to non-authorized parties.

HPE SecureData for Cloud combines two technologies to vastly simplify data protection and mitigate data leakage at a fraction of the cost of traditional approaches. **HPE Format-Preserving Encryption (FPE)** and **HPE Secure Stateless Tokenization (SST)** work to protect data while preserving data formats and other attributes, effectively building the protection into the data itself. Replacing the original data with either an encrypted value or a random token narrows the possible exposure of data, and can greatly reduce audit scope and compliance costs.

Table 2: Key considerations for HPE SecureData for data privacy and compliance

Considerations	Solution benefits
Is security policy built into the technology?	Bolt-on solutions are insufficient to meet most security requirements because they cannot accommodate corporate security policies. HPE SecureData builds security and resiliency into the fabric of your organization.
Can you keep up with the reality of the data lifecycle?	Today, data travels among states and countries, users, and across different IT systems and end-user devices. No company can hope to contain data within traditional boundaries. HPE SecureData for Cloud protects data from the moment it's created, going into and moving through the Microsoft Azure Cloud.
Does your solution stand up to regulatory scrutiny?	If you're using a traditional approach to data security in the cloud, your data may not be as secure as you think, putting you in violation of data security compliance requirements. With HPE SecureData for Cloud, you can rest assured that data is useless to unauthorized users at any time.
Can you scale protection quickly and easily to meet business and IT requirements?	HPE SecureData for Cloud is architected to match the growth of your business and its data. HPE SecureData is horizontally scalable and serve applications independently of one another.
What is the impact on the business? How about the total cost of ownership?	The success of your company and its data protection solution is dependent on easy deployment and low cost of operation. The low implementation complexity and cost of HPE SecureData for Cloud means faster time-to-production.
How easy is it to adopt business-wide?	HPE SecureData for Cloud shields users from the complexity of data security regulations and the need for access control. Otherwise, adoption is deterred and the security initiative will be stalled.
Can we secure structured and unstructured data?	The types of data that run a company are varied—that's why HPE SecureData for Cloud secures structured and unstructured data equally while providing access to authorized parties as needed.
Does it support legacy systems?	IT environments today are heterogeneous, with new technologies working alongside legacy systems. HPE SecureData for Cloud works with these legacy systems without extensive and complex re-engineering.
Does it integrate with your hybrid cloud initiatives?	HPE SecureData for Cloud works with new, cutting-edge technologies—including Microsoft Azure Cloud and your mobility initiatives—without having to rip-and-replace.

The EU GDPR applies to all companies that deal with EU citizens' data.

Use HPE SecureData to comply with GDPR

The new EU GDPR regulations, effective May, 2018, sets the foundation for how any organization collecting and storing EU citizens' data must protect and derive value from sensitive customer information. By complying with its regulations, organizations can guard against the risks of lost customer confidence and sales, security breaches, fines, sanctions, and potential lawsuits, as well as gain greater insight into customer needs and enhance overall productivity.

Complying with this new and multifaceted set of regulations can be complicated. The GDPR provides guidelines around the use of encryption and de-identification as approaches to protect sensitive data for three main reasons:

- Encryption can be used to mitigate the risks inherent in data processing, such as unauthorized disclosure of, or access to, personal data.
- The requirement to notify data subjects of a data breach is removed if the data is rendered unintelligible using a measure such as encryption or de-identification.
- The use of de-identification can reduce the risks to data subjects while helping data controllers and processors meet their compliance obligations by minimizing both the exposure of personal data and the opportunities to identify data subjects.
- Although not explicitly stated in GDPR, the extensive rules around data transfers outside the EU can be simplified by encrypting the data and managing keys in-country (including on-premises).

As part of our complete portfolio of GDPR compliance offerings, HPE SecureData for Cloud with HPE Hyper FPE, HPE Hyper Secure Stateless Tokenization (SST), and HPE Stateless Key Management is a proven, standards-based approach to protecting PII as required by the GDPR—in use, in transit, and at rest—to ensure that when a breach occurs, the information remains confidential.

Maintain control with HPE Stateless Key Management

More and more organizations are moving data storage to the cloud. When you place data in the cloud, it still needs to be protected through all the layers of the cloud—from storage to file servers, to middleware, and on to the application layer. Electronic data keys enable this level of protection, but legacy key management solutions require complex replication and scaling architectures.

As part of the HPE SecureData for Cloud solution's data-centric approach to enterprise data protection, **HPE Stateless Key Management** enables on-demand key generation and re-generation without an ever-growing key store. The result is a system that can be scaled infinitely across distributed physical and logical locations with no additional overhead.

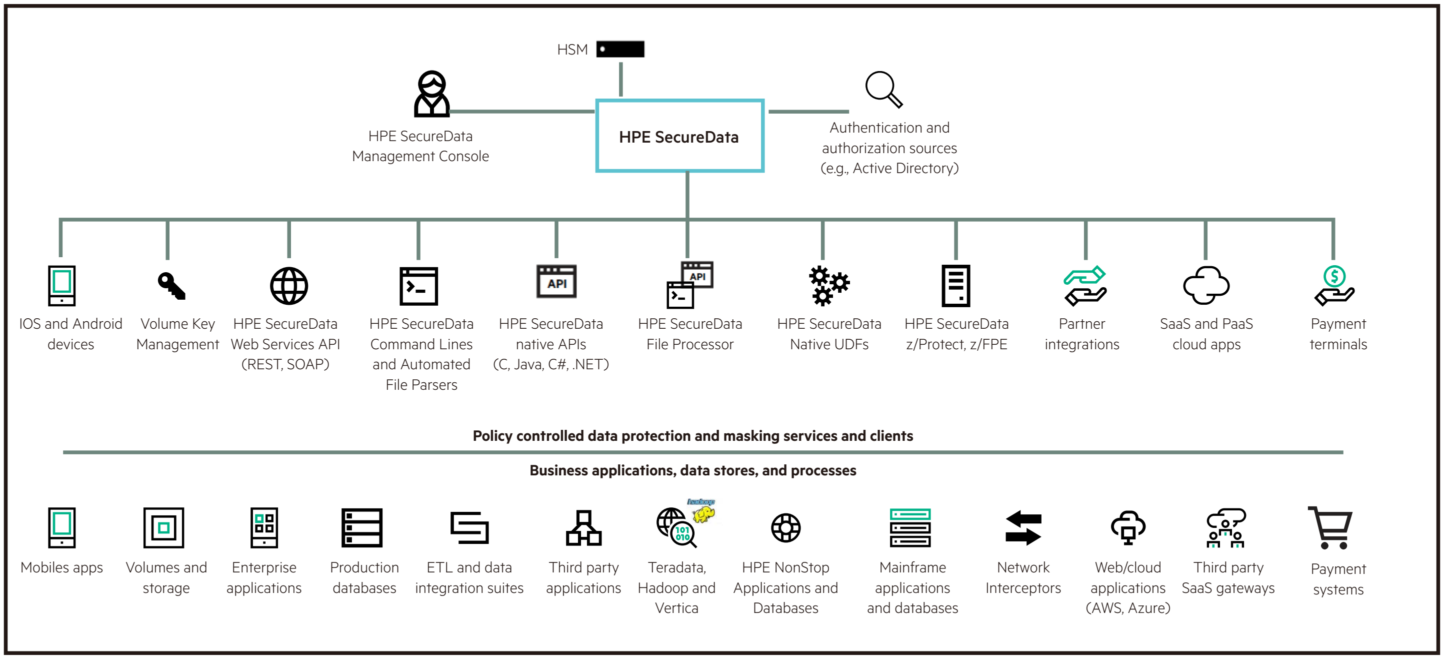
Eliminates operational complexities, guarantees keys cannot be lost. HPE Stateless Key Management is vital for global organizations—with a highly available, distributed architecture, it provides keys automatically with no key storage or database management issues such as key roll over, back up, recovery, and audit.

Extends IT investment in existing identity management infrastructure. HPE Stateless 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.

HPE SecureData: cost-effective, simple, and flexible

HPE SecureData is a unique, proven, data-centric approach to protection, where the access policy travels with the data itself. It permits data encryption and tokenization without changes to data format or integrity, and eliminates the cost and complexity of issuing and managing certificates and symmetric keys. As a result, leading companies in financial services, insurance, retail, healthcare, energy, transportation, telecom, and other industries have achieved end-to-end data protection across the extended enterprise with success in as few as 60–90 days because of minimum—in most cases, zero—impact to applications and database schemas.

HPE SecureData Architecture addresses use cases across diverse environments.


HSM
HPE SecureData Management Console
HPE SecureData
Authentication and authorization sources (e.g., Active Directory)
IOS and Android devices
Volume Key Management
HPE SecureData Web Services API (REST, SOAP)
HPE SecureData Command Lines and Automated File Parsers
API
HPE SecureData native APIs (C, Java, C#, .NET)
API
HPE SecureData File Processor
HPE SecureData Native UDFs
HPE SecureData z/Protect, z/FPE
Partner integrations
SaaS and PaaS cloud apps
Payment terminals
Policy controlled data protection and masking services and clients
Business applications, data stores, and processes
Mobiles apps
Volumes and storage
Enterprise applications
Production databases
ETL and data integration suites
Third party applications
Teradata, Hadoop and Vertica
HPE NonStop Applications and Databases
Mainframe applications and databases
Network Interceptors
Web/cloud applications (AWS, Azure)
Third party SaaS gateways
Payment systems

Solution benefits

HPE SecureData for Cloud provides cloud confidence for even the most sensitive business and enterprise applications, by providing:

Comprehensive data protection—HPE SecureData for Cloud provides a single framework that protects at the data level, enabling secure movement and use of data within cloud environments. This provides hybrid cloud protection that can integrate immediately with virtually any application, ranging from purpose-built web apps to the latest enterprise applications. The solution comprehensively protects all data before it moves into and travels through the cloud.

Optimized scalability and performance—HPE SecureData for Cloud features a scalable, client-server architecture that allows you 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, you can enjoy high-performance protection and still retain control, management, security separation, and audit for all security operations from the HPE SecureData Key Server.

Rapid and efficient 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.

Table 3: Responding to cloud needs with HPE SecureData for Cloud

Cloud architectural change	Data-centric protection with HPE SecureData
Cloud architectures remove the traditional IT infrastructure edge points (there are no WANs, LANs, WLANs, or VPNs/firewalls) found in traditional enterprise infrastructure.	HPE SecureData for Cloud allows you to lock data in place, achieving data protection via encryption, masking, and tokenization to protect data without fixed boundaries and as data moves across all application, storage, and compute environments of the cloud.
Data can now be accessed by enterprise and cloud IT resources not always under the strict control of the enterprise.	Data encrypted before it moves to the cloud with HPE SecureData for Cloud can remove cloud-based risk while increasing enterprise visibility and access control to sensitive data.
Many cloud-based applications can lead to an expanded set of authorized users that require access to applications and private data.	HPE SecureData for Cloud offers an extensive set of identity management and authentication connectors to common user repositories, such as LDAP, Active Directory, and CA's SiteMinder platforms. These authentication schemes can be combined to require multi-factor authentication for greater control and more governed access to sensitive records.
Cloud architectures present new opportunities to scale globally, driving the movement and consolidation of data in new territories, countries and regions, which can trigger different country-by-country data privacy and data residency laws.	Through HPE FPE and HPE SST, you can comply with data residency and compliance obligations, while having the flexibility to move data to any location.
The speed of the cloud may also introduce unexpected security risks and exposures that IT governance and security groups may be late in detecting, or never know about.	By starting with a new data-centric approach and end-to-end protection of sensitive data enabled by HPE SecureData for Cloud, you can encourage and deploy new applications with protective coverage.
Maintaining consistency and reversibility of sensitive data while it moves around different cloud applications, repositories, and databases/data warehouses is a challenge.	There are special demands on maintaining reversibility and referential integrity of protected data in the cloud. HPE SecureData for Cloud techniques for masking, tokenization, and encryption all maintain a common, identical representation of data in every instance, ensuring consistency and reversibility across the cloud.

Act now to protect data

With HPE SecureData for Cloud, data protection is now feasible across the global enterprise with a single approach. HPE SecureData offers huge reductions in cost and time-to-value for data protection and privacy and payment compliance. The data-centric approach mitigates data leakage and avoids disclosure from the outset, regardless of platform choice, outsourcing needs, scaling requirements, or IT processes. For the first time, information protection and database security are simple and easy to implement, becoming a natural extension of existing infrastructure and processes.

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

Our solution partner

Microsoft

Sign up for updates

Hewlett Packard
Enterprise