Brochure

Enterprise Cloud Security

Hewlett Packard Enterprise

Key business drivers for Cloud computing today

Cloud computing is one of the largest, most dramatic forces changing the IT landscape today. Driven by key economic advantages, as well as factors that re-shape how fast enterprises can address global markets, and develop new services, there are substantial business benefits to the cloud. The savings can be substantial. According to IDC, the five-year total cost savings from utilizing an online cloud based service, such as Amazon's Web Services (AWS) over enterprise data-center resources can be over 80%, or over $516,000 USD 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 inhibited by the security challenges around the very nature of cloud architectures. For customers that need to protect sensitive data, moving to the cloud creates substantial new risks and changing landscapes for how to protect private information.

Beyond economics, cloud computing delivers significant benefits in helping businesses grow, expand, and plan for capacity management. As applications drive more demand for networking, storage, computing, cloud systems can rapidly provide these services, while charging the customer for only if and when these scaled-out services are used. Running applications in the cloud also lets businesses more easily operate and grow to in global marketplaces without the costs, complexity, and time required to setup country-specific computing, people, and infrastructure. By re-designing business applications to a cloud presence, the requirements for an enterprise to run applications from anywhere, for anyone, in any global location becomes easier, but at the same time, forces enterprises to find new ways to guarantee those applications and the valuable information inside them stays protected.

Clouds drive new data protection strategies

Each of the core benefits of the cloud highlighted above introduces new security challenges and business risks. The lightweight, outsourced aspect of cloud IT also means that a whole new set of people now have access to, and are responsible for protecting and blocking access to sensitive data in their infrastructure. The ability to scale and more rapidly reach global markets introduces new considerations around compliance to data residency regulations. With cloud computing, sensitive data that is governed by substantially different rules and requirements in different countries can now literally be pushed and pressed to the far reaches of the globe, triggering unintended violations in privacy and personal information records that by law, should never leave certain countries or jurisdictions in readable formats. And lastly, while the speed and scale of cloud computing allows companies to optimize how they use and manage IT resources, speed and scale also require all the surrounding systems, including security and data protection to be adaptable, highly available and supportive to the goals of the business.

New protection strategies

Attempting to secure applications and data in the cloud with existing end-point security products limits the ability of an organization to effectively protect data. First, data no longer moves between applications and data repositories in static, well defined paths to fixed and limited applications. Point-to-point protection, such as that offered by Secure Socket Layers (SSL) or Virtual Private Networks (VPNs) can not address the reality that in clouds, data travels everywhere. And newer, cloud-focused encryption solutions that approach the problem from encrypting entire data-stores or VMs 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.

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. This means that locking the repositions, applications, and links doesn't provide complete protection because the data is in flight and won't stay in one place.

HPE SecureData for Cloud solutions—Flexible, scalable, end-to-end data protection

HPE SecureData for Cloud solutions leverage core encryption and key management technology that protects data independent of the applications, storage methods, and subsystems that use it. The solution can protect data upon upload, or application creation, providing pinpoint protection of sensitive data as soon as it is acquired and ensure that it is always used, transferred and stored in protected form as it moves around the cloud. Selected applications decrypt the data only at the time that it is processed, while others work with encrypted or masked data.

The solution capabilities provide enterprises with specific, precise control over how to protect data while preserving data format and other attributes, while at the same time delivering a key management system that is scalable, highly available, and distributed to any cloud instance in any geography or region with minimal overhead and effort. By ensuring data-level protection that reduces the risk of inappropriate access and attack, while providing this service in a highly replicable, distributed manner, it enables enterprises to achieve the secure access and use of data across the entire cloud system.

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 two key cloud paradigms:

- Software as a Service (SaaS): HPE SecureData data-centric solutions can 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 SecureData and PerspecSys further extends cloud data protection capabilities and enables many types of data to be transparently protected in popular cloud applications.
- Custom Cloud applications (IaaS/PaaS): HPE SecureData key management and encryption services can be used by cloud hosted custom application to control where and how data is exposed within the application architecture.

The following table highlights the specific cloud architectural changes and a data-centric protection strategy for securing cloud data.

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 enterprises to lock 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.
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.
SaaS applications can take even more control over data—how it's stored, backed up, archived, and accessed by cloud system administrators.	New cloud security for SaaS applications can render all private data and attachments encrypted inside SaaS clouds, bringing data access and audit control back to the enterprise.
Many cloud-based applications can lead to an expanded set of authorized users that require access to applications and enterprise's 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 Format-Preserving Encryption and HPE Secure Stateless Tokenization, organizations 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, end-to-end protection of sensitive data by HPE SecureData for Cloud solution, IT organizations 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.	There are special demands on maintaining reversibility and referential integrity of protected data in the cloud. The 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.

Solution benefits

HPE SecureData for Cloud provides a unique platform for rapid adoption of clouds by even the most security demanding of business and enterprise applications:

Comprehensive data protection—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.

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.

SaaS, PaaS, and IaaS Ready—Whether you need to adopt new SaaS applications for customer relationship management (CRM) utilizing 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 AWS, 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.

Conclusion

Enterprises adopting cloud-based IT applications and services achieve dramatic cost and competitive advantages, and those advantages appear to be accelerating with new technology enablers around mobile, Big Data, and SaaS applications. At the same time, companies are mindful of the new security challenges presented, and cannot take full advantage of cloud-based IT infrastructures if there are increases in the risk of data loss or compliance violations. Companies moving into the cloud must demonstrate compliance to security, as well as domestic and international data residency regulations. HPE SecureData for Cloud delivers comprehensive data protection that can accelerate these deployments while ensuring the end-to-end security protection required for sensitive, private information, and compliance to international and state privacy laws and regulations.

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

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-0207ENW, May 2016, Rev. 1