Hewlett Packard Enterprise

Solution brief

Mitigate cloud risks

HPE SecureData for Microsoft Azure Cloud

End-to-end protection for your most sensitive data, on-premises and in the cloud.

Protect privacy and PII

Enable secure analytics

Comply with PCI guidelines

As digital enterprises expand into to the cloud, many are choosing the flexibility of Microsoft® Azure, a consistent cloud technology platform that enables them to quickly build, deploy, and manage applications across a global network of Microsoft managed data centers. With a pay-as-you-need model and a growing collection of integrated services—including analytics, computing, database, mobile, networking, storage, and web—Microsoft Azure helps enterprises address global markets. It also helps them develop new services at lightning speed and benefit from the substantial savings of the cloud as a low-cost operating environment.

But you have probably already recognized that these benefits are accompanied by significant data security risks.

If you're managing sensitive corporate and customer data, including credit card, medical, or corporate financial data, your ability to adopt the cloud may be impeded by security challenges. That's because sensitive data that moves into and across cloud-based infrastructures is at an increased risk for data loss or compliance violations. Sensitive data needs to be protected at the point of creation, before it moves out of the enterprise or as it is entering the cloud.

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.

"When data is transferred to a cloud, the responsibility for protecting and securing the data typically remains with the collector or custodian of that data."[1]

HPE SecureData for Cloud protects sensitive data-at-rest, in-motion, and in-use as it moves in and through public, private, and hybrid clouds.

[1] Cloud Security Alliance, Guidance v3.0

Sign up for updates

Hewlett Packard Enterprise

HPE SecureData for Cloud comprehensively protects all enterprise data end-to-end—from the moment of capture and as it is processed and stored across a variety of devices, operating systems, databases, and applications—enabling secure movement and use of data in the Microsoft Azure Cloud. This data-centric encryption helps you to protect sensitive data in compliance with security, privacy, and data residency with security, privacy, and data residency regulations including the European Commission's General Data Protection Regulation (GDPR).

What type of protection do you need?

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 HPE SecureData for Cloud.

Payment card industry (PCI) compliance: Neutralize breaches, protect payments
Maintaining compliance with PCI guidelines is expensive, challenging, and time consuming. Compliance alone doesn't equate to security, and is not enough to prevent data breaches. HPE SecureData technologies provide enterprises, merchants, and payment processors with a new approach to protecting payment card data that starts from the moment the information enters the system. HPE SecureData is also compatible with PCI DSS 3.2 requirements on transport encryption, enabling compliance ahead of deadlines, as recommended by the PCI council.

Enable secure analytics using data de-identification
Most enterprises have implemented every type of deterrent, policy, training, intrusion prevention, and firewall to protect data and enable secure analytics, but it is not enough. The only way for organizations to truly protect data is to make it worthless to an outsider or unauthorized eyes. HPE SecureData "de-identifies" data using encryption, tokenization, and data masking, rendering it useless to outsiders while maintaining its usability for collaboration, data processes, applications, and services.

For example, if you want to perform Big Data analytics using Hadoop, the live 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 so it can be analyzed in a protected form and then returned to its original form once back in the data warehouse. This kind of flexible, data-centric protection is extremely valuable for enabling secure, cross-cloud analytics on data from your extended enterprise.

Protect privacy and personally identifiable information (PII)
With cloud computing, sensitive data can now be pushed to the far reaches of the globe, causing unintended violations in privacy and PII regulations. HPE SecureData for Cloud helps to protect information in compliance with the healthcare information portability and accessibility act (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and GDPR, along with other state and national data privacy regulations. HPE SecureData for Cloud enables organizations to quickly pass audits and implement full, end-to-end data protection to reduce the risks and impact of data breaches.

Take full advantage of cloud economics

If security concerns are preventing you from putting data in the cloud, it's time to find out more about HPE SecureData for Cloud.

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

4AA6-8398ENW, November 2016