Hewlett Packard Enterprise

Business white paper

Embrace risk: secure your hybrid cloud

Protected to innovate with the right mix

Table of contents

Hewlett Packard Enterprise

Embrace risk knowing your cloud is secure

Protected to innovate with the right mix

12%

cost increase, per capita, of a security breach

23%

increase in total cost of data breaches since 2013

$154

USD the average cost of a lost or stolen record

HPE Helion

Introduction

An optimized hybrid IT infrastructure enables innovative business outcomes—but rapid IT transformation also creates new risks, threats and vulnerabilities. Coupled with increasingly sophisticated cyberattacks and complex regulatory pressures, managing risk in today's digital environment becomes even more critical to the enterprise.

Finding the right mix of hybrid cloud as a part of a hybrid IT infrastructure strategy sets an enterprise on a path toward greater innovation. But weaving cloud into their IT DNA can be complex and risky. By building in security upfront, this barrier can be removed, offering the freedom and flexibility to transform their business with hybrid cloud resources while ensuring their hybrid cloud is secure and compliant. Security must be at the foundation of an enterprise IT strategy, when defining, powering and optimizing the right mix of hybrid IT infrastructure.

Security challenges businesses face today

Not that long ago organizations deployed security strategies focused on securing the perimeter, locking down users, access and data. The new, digital style of business has dissolved this perimeter. Users are interacting with data and applications in the cloud, on mobile devices and within the internal network. To protect the digital enterprise, interactions between business-critical digital assets must be secured, allowing the safe free flow of information throughout the entire enterprise and across customers, employees, partners and suppliers.

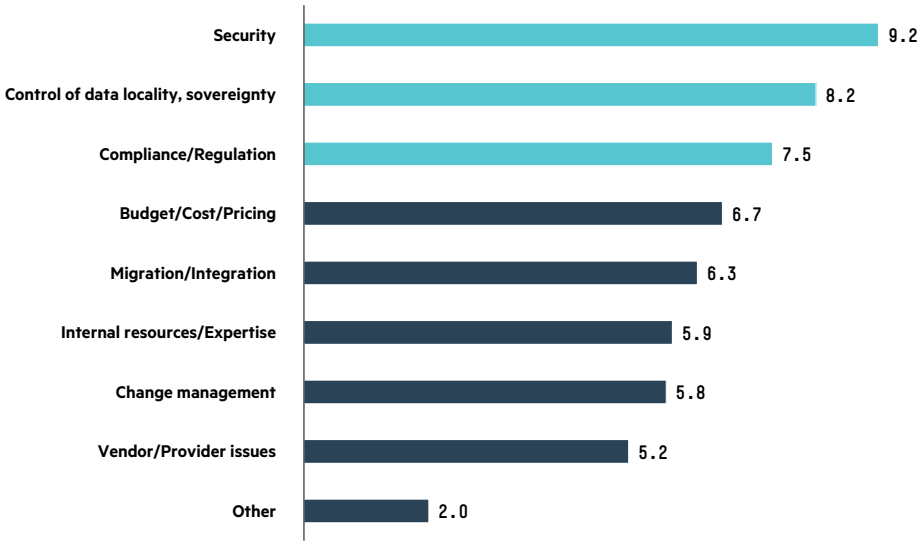
Adopting the new style of IT has distributed data everywhere, which has created new exposures and attack surfaces. The shift to hybrid cloud computing, mobile connectivity and the explosion of big data have created new and more frequent security challenges. The ever-increasing IT footprint from these new capabilities, and the resulting security exposure, has also grown the available attack surface that can potentially be exploited.

The cost and complexity of regulatory pressures also continues to grow in areas like compliance, privacy and data protection. Conflicting regulatory priorities, sovereignty challenges and industry-specific issues means that there is no clear path for organizations to achieve regulatory success. These regulatory pressures further increase enterprise risk with compliancy requirements that are non-optional. Organizations are being hit with large fines because of noncompliance. In addition, growing stakeholder demands and increasing public scrutiny mean security and risk officers are grappling with ever more complex regulatory issues. These include compliance regulations, privacy rulings and data protection mandates, which continue to expand and change regularly.

Figure 1: Transformation fuels innovation, but brings new risks

In addition to expanding attack surface area and regulatory issues, increasingly sophisticated cyberattacks are growing exponentially—and the criminals are getting smarter. We live in a world of increasingly more complex security threats. They can be external or internal in nature and can represent malicious or unintentional actions. More and more, they are a result of cybercriminals who have created an adversarial environment that has become more specialized, more efficient and more lucrative. The criminal marketplace has advanced beyond basic capabilities and is innovating and changing tactics every day. They are getting smarter, more collaborative and are highly motivated to gain access to information for profit, politics and corporate espionage. According to a recent article in InfoWorld, there are even websites selling subscriptions and support, offering malware-as-a-service, which allows virtually anyone with little to no skills to potentially breach even advanced IT security environments.[1] Attacks continue to be more sophisticated, more frequent and more damaging.

A recent survey by 451 Research, "Voice of the Enterprise", clearly shows that security in a cloud computing environment is a top concern for enterprises (see figure 2). Regulatory and compliance concerns closely follow. To increase time to value, enhance customer experiences and improve workforce productivity, organizations must embrace the opportunities that cloud and mobile computing bring. Yet, business-critical digital assets and their interactions must be protected, regardless of location or device, whether on-premises or off-premises.



Source: 451 Research, Voice of the Enterprise: Cloud Computing, Q3 2015

Figure 2: Top concerns for enterprise IT

[1] infoworld.com/article/3031193/security/jsocket-offers-cyber-criminals-one-stop-shop-for-malware.html

million USD annualized average cost of cybercrime

USD average cost per day of undetected attacks

mean number of days to resolve cyberattack

million USD average annual cost savings from implementing SIEM

Consequences of a poorly implemented security strategy

In 2014 alone, more than one billion personal records were illegally accessed—including health, financial, email, home addresses and other personal information like Social Security numbers. That statistic is up more than 49 percent on the year prior[2] and 2015 was proving to be even worse. The average annual cost of cybercrime to an enterprise is $7.7 million USD and the average cost per day of undetected attacks is $21,155 USD. The potential liability and resulting financial cost to an enterprise today is undeniable.

In the USA, Excellus BlueCross BlueShield discovered a breach that ended up leaking more than 10 million records. Even worse, the breach happened two years earlier in late December 2013. Names, birth dates, Social Security numbers and mailing addresses were taken, including financial accounts and claims information. Virtually all of the UK's major banks and lenders—including Barclays, HSBC, Lloyds Banking Group, NatWest, Nationwide and Santander—have reported multiple incidents to the Information Commissioner's Office (ICO) in the past two years, including 158 disclosures of personal information. In Asia Pacific, the Anonymous hacking collective, through a member known as The Messiah, hacked into various Singapore government platforms, including the prime minister's official website. In one single day, the actions led to 19 government websites being taken down.

These are just a sample of the breaches that occurred globally and across multiple business sectors. The obvious point here is that the lack of a rigorous security-first strategy and poor implementation, detection, response and auditing processes has far-reaching consequences for companies that do not make security their number one IT priority. The costs of a security breach are increasing, which create significant financial consequences to the enterprise.

Security for an open hybrid cloud

Based on 451 Research's data,[3] the top security issues enterprises need to address in their hybrid cloud infrastructure are listed below:

- Maintain consistent access, security and authorization controls across environments
- Secure movement of data and workloads across environments
- Secure data residing in and processed by a third-party or hosted environment
- Maintain consistent network security policies for security domains
- Ensure compliance with regulatory and policy requirements

Although these security concerns are paramount, the flexibility advantage of implementing cloud resources is compelling. A Brookings Institution study has shown that enterprises can save up to 50 percent of their costs by moving to the cloud. This is especially true for variable workloads like high-performance computing (HPC), Hadoop and dev/test. Further, fast standup of dev/test environments, use of platform as a service (PaaS) and other tools make it possible for lines of business to cut the time from concept to deployment by up to 80 percent.

However, two issues are holding back the enterprise's use of cloud resources: how to secure their workloads and how to do it cost effectively and universally.

So what's the best approach to mitigate security breach risks? It starts by integrating security-first principles into the enterprise's IT collective mindset.

[2] "**Gemalto Releases Findings of 2014 Breach Level Index**," Gemalto, 12 February, 2015

[3] **www8.hp.com/us/en/cloud/helion-hybrid.html?originid=510066847&action=downloadpdf&tcmid=tcm:52-21726644&assetcode=560017301&jumpid=em_72st3wxqzk_AID-510066847**

Three security-first principles

Hewlett Packard Enterprise's (HPE) plan for an evolving hybrid infrastructure is based on three security-first principles: shaping security standards, shared responsibility and defense in-depth.

Shaping security standards: The foundation of a trusted security solution provider requires supporting industry standards. But that's not good enough. You want a partner that provides industry leadership by helping define security standards to protect your hybrid infrastructure—a partner that brings security experts together to establish security best practices, a partner that strives for transparency and community involvement. HPE engineers lead the OpenStack® security team, contribute to the Payment Card Industry Data Security Standard (PCI DSS) organization and encourage community collaboration with HPE Threat Central. With a standards-based security philosophy, HPE is as visible as possible in every aspect of hybrid cloud security and continuously works to protect your hybrid cloud from the constantly changing security threat.

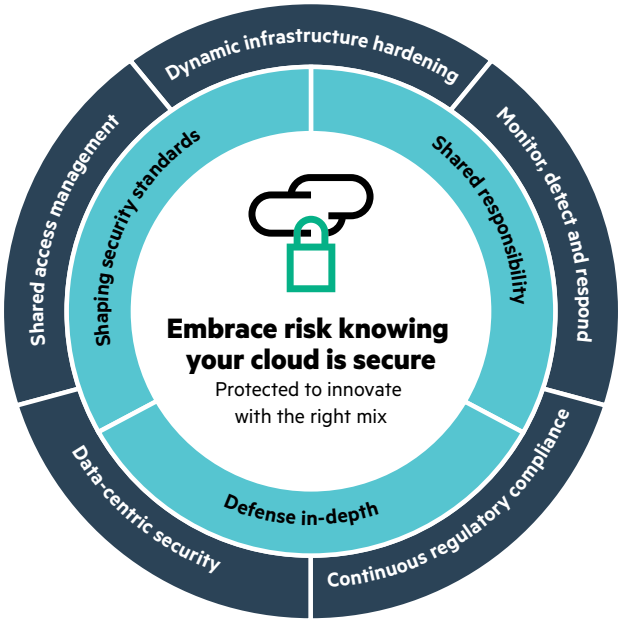


Figure 3: HPE strategy for securing hybrid clouds

Shared responsibility: HPE believes in shared responsibility for information security—finding the right mix of involvement for customers and their security challenges. Shared responsibility means both the vendor and customer are responsible for certain aspects of security. The IT vendor develops products and services with best-in-class, standards-based, security features. Customers then define security policies and manage them from within the cloud, following security best practices.

Defense in-depth: HPE supports a defense in-depth model for integrated, built-in security. Most security vendors provide a single point solution, addressing only one aspect of security or compliance. The hybrid cloud security of HPE provides multiple layers of security controls, creating security redundancies. For example, internal network protections exist on top of host layer protection, which exist on top of application and data layer protection—no single breach can circumvent all the layers of security within the environment. HPE security solutions are built-in, not added on later. Moreover, with an integrated approach, you can use the same security tools to protect your private cloud, public cloud and traditional IT, reducing the number of tools and the complexity of securing your hybrid infrastructure.

Five key hybrid cloud security capabilities

The three security-first principles provide a foundation for five key hybrid cloud security capabilities that HPE focuses on to ensure a secure hybrid cloud environment: data-centric security; dynamic infrastructure hardening; monitor, detect and respond; continuous regulatory compliance; and shared access management. These core capabilities are built-in to HPE Helion products and services, delivering enterprise-grade security for a hybrid cloud environment.

Data-centric security ensures unified data protection across private cloud, public cloud and traditional IT. Confidential data should be secure at all times, at rest, in motion and in use. The typical approach to encryption is to encrypt and decrypt data at each stage, in storage, in transit over networks and in databases. As an example, sensitive data is typically encrypted when it's stored in a storage device. When it's retrieved, the data is decrypted. When that data is transmitted, it is encrypted, transmitted and then decrypted. Next, the data is used by the application. This process creates gaps where the data is not secured (see figure 4).

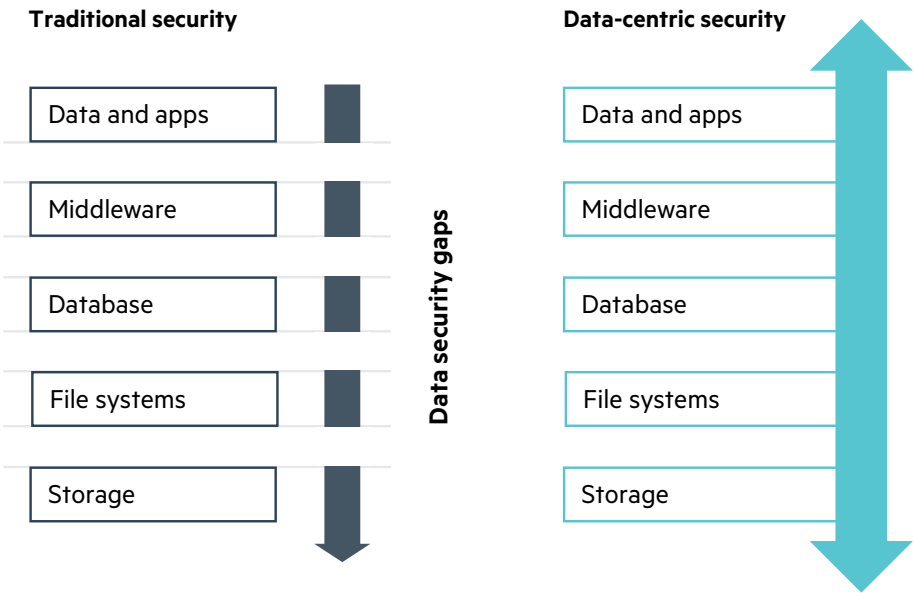


Figure 4: Gaps in traditional security vs. data-centric security

The HPE data-centric security approach is different. We provide encryption when the data is first received. The data continues to be encrypted throughout its use to ensure there are no security gaps. HPE employs unique security technologies, including Format-Preserving Encryption (FPE), Secure Stateless Tokenization (SST), Stateless Key Management and multiple layer encryption to ensure sensitive data is protected at all times.

Public cloud data and private cloud data should be protected seamlessly while maintaining the formats and structure of the data. Encryption keys need to be safeguarded with a highly scalable key management system. In addition, both application and user generated data must be protected. HPE security products provide these capabilities to protect your sensitive data.

Protection with dynamic infrastructure hardening involves several aspects of IT security best practices to reduce the overall attack surface. By eliminating unnecessary operating system components, the exposed IT footprint is reduced, thereby offering fewer opportunities for hackers to exploit.

Perimeter security should no longer be the core of corporate security that it once was. However, it is still important to continue implementing properly managed intrusion detection and firewalls as a component of an overall security strategy. While more and more attacks are occurring from within the enterprise firewall, attacks are still being successfully implemented externally.

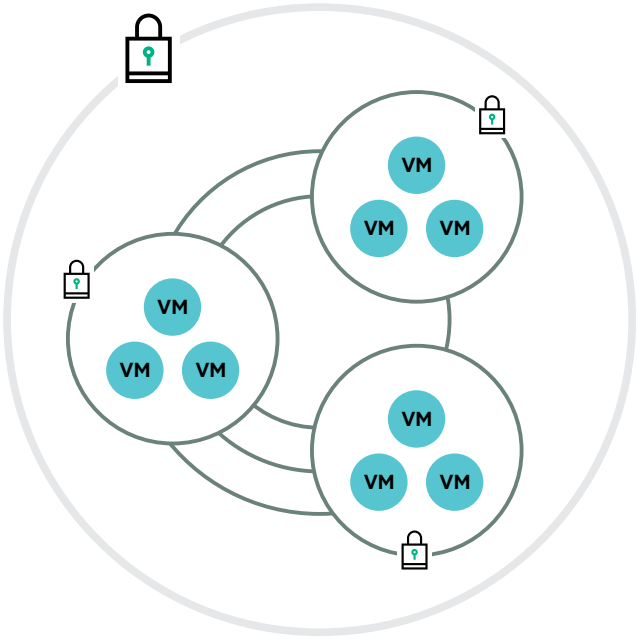


Figure 5: Protecting your dynamic infrastructure with micro-segmentation

Network separation at both the physical and logical level and securing virtual machine (VM) to VM traffic to create secure domains is extremely important. Opportunities for both deliberate and inadvertent breaches are greatly reduced. When a breach does occur, it is "containerized" and limited in scope. The HPE cloud strategy helps enterprises configure their infrastructure with security zones to provide additional layers of protection using micro-segmentation to prevent hackers from getting access to all services and infrastructure.

Critical security patches must be applied as quickly and as automatically as possible, while causing the least disruption possible to the clients. The cloud operating system and supported hypervisors must be properly configured and managed to prevent hypervisor breakouts otherwise known as Virtualized Environment Neglected Operations Manipulation (VENOM). HPE provides critical security patches to ensure customer's cloud environments are protected from the latest attacks and hardens the underlying operating system to reduce the attack surface.

An enterprise needs to be protected, with complete visibility, by proactively **monitoring, detecting and responding** to threats. A typical data breach response takes 46 mean days to resolve without proper controls or tools. With the proper implementation of tools and procedures, data breaches can be quickly detected and responded to in hours.

Figure 6: Protect your hybrid cloud by monitoring, detecting and responding to threats

A quick response time to a breach requires collecting logs from private cloud, public cloud and traditional IT environments. HPE industry-leading security information and event management tools unify data logs from multiple sources into a single format. They enable administrators to search through millions of events in seconds for anomalies, making it possible to quickly detect break-ins. Years of unified data can be retained, archived and compressed for future forensic use. The resulting large amount of archived information requires a big data solution to manage the data and requires the right tools to make use of it. Analysis, reporting and alerting needs to be automated for IT operations, IT security and IT governance, risk and compliance (GRC) teams.

Hybrid infrastructure also needs to be **protected with continuous regulatory compliance**, which is unified with policies and best practices across the hybrid IT environment. Enterprises need to have a consistent compliance model across private cloud, public cloud and traditional IT assets. Keeping data within the required country/region requires policy-based deployment, using consistent out-of-the-box templates for regulatory standards, which creates a solid regulatory compliance IT foundation.

Figure 7: Protect your hybrid cloud with continuous regulatory compliance

Checking continuously for compliance drift, along with automated scanning and remediation, allows administrators to identify and fix non-compliancy issues quickly. Implementing consistent, regular, auditing and reporting processes give the enterprise the supporting documentation necessary for required "proof of compliancy." A unified, continuous regulatory compliance strategy is a huge benefit to the bottom line by directly reducing auditing compliancy costs. HPE provides tools to make it easier to ensure compliance to regulatory requirements and to run reports and analyze environments for compliance drift. These capabilities greatly reduce the time and effort required for auditing.

The enterprise hybrid cloud needs to be **protected with shared access management**. IT management policies need to maintain and enforce consistent access policies across all environments, both internal and external. Properly implemented access policies ensure people do not get access to things that they shouldn't.

Figure 8: Protect your hybrid cloud with shared access management

HPE cloud management tools support role-based access and access control. Users can be limited to only ordering cloud services they should have access to. Administrative management has separate access controls to prevent users from accessing administrative controls. Multiple catalogs can be created for different audiences to help control which users have access to services—and integration with enterprise directory services simplifies access management.

Customer examples

Thousands of customers around the world are using HPE security products for protection. Examples of enterprises making full use of cloud resources, while simultaneously managing the associated risk and security issues, are numerous. They include some of the most successful and fastest growing enterprises in the market.

A top-five retailer had an older homegrown tokenization system with multiple security solutions, making it difficult to provide a truly secure environment. They needed to move to an end-to-end security solution that was maintainable, scalable and cost effective. They have since moved to a data-centric security model that employs the unique HPE Secure Stateless Tokenization technology that encrypts every captured card at purchase and tokenizes all stored cards. Customer card data is now completely protected, from web browser to data center, with no security gaps from end to end.

With this new security model, the enterprise no longer needed to synchronize token databases across multiple data centers. They now have a highly scalable point of sale system supporting 100 million transactions annually. Due to this upgrade, the retailer removed 600 servers from PCI compliancy requirements and saved $1 million USD annually in compliancy savings.

In response to market and customer needs, **a "new style" financial firm** wanted to use Amazon AWS and Microsoft® Azure services to increase agility, without increasing risk to the enterprise or their clients. They had more than 30 sensitive data types to secure across 100 million customers, while still meeting complex regulatory issues for personally identifiable information (PII), mobile data and residency rules. Their solution was to use HPE security products to encrypt and tokenize sensitive data in Amazon AWS and Microsoft Azure public cloud services, but retain policy enforcement on-premises, not in public cloud, using a single platform. This allowed them to use on-premises virtual appliances for security operations, along with audit and key management.

This solution resulted in a unified architecture that streamlined compliance and risk control and allowed the financial firm to quickly meet third-party data protection mandates and audits. Sensitive data exposure was minimized within Amazon AWS and Microsoft Azure. They were also able to cut application costs, while creating an agile business strategy using public cloud.

Conclusion

The move to hybrid cloud can be properly secured using products, tools and processes that are available today, but an integrated approach is required. The key to creating a secure hybrid cloud infrastructure is to treat security as something that should be built into the IT cloud strategy and its design, not just bolted on as an afterthought.

The enterprise needs to define their security with the right strategy, power their security with the right products and optimize their security with the right tools and processes.

Hewlett Packard Enterprise advocates this integrated approach to hybrid cloud security, one that starts with a single, comprehensive view of risk across the enterprise and is driven by the enterprise's priorities and goals. HPE offers unique security technologies, such as Format-Preserving Encryption (FPE) and Secure Stateless Tokenization (SST), industry-leading security products and extensive security expertise and experience. By focusing on the business-critical digital assets, and the interactions between them, businesses can implement a more proactive and effective enterprise-wide approach to security and risk management that balances regulatory requirements, threats, asset protection and recovery. The results include fixing vulnerabilities in days instead of weeks, responding to threats in hours instead of days and an 85 percent reduction in IT outages.[5]

Finding your right mix, backed by a security-first mindset, allows you to take full advantage of both private and public cloud technologies. Thousands of customers across a variety of market segments have built their hybrid infrastructure with Hewlett Packard Enterprise security concepts and products. HPE Helion allows you to **embrace risk knowing your cloud is secure**.

Learn more at
hpe.com/helion

[5] Based on HPE internal study.

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-4577ENN, March 2016