Hewlett Packard Enterprise

Business white paper

Meeting Data Residency and Compliance Challenges in Global Enterprises

Innovative Security Solutions Enhance Business Agility and Reduce Risk

Table of contents

Why Data-centric Security?
A data-centric approach to security provides a new method of protecting data: at the data level itself, wherever the data goes. Legacy approaches focus on securing infrastructure elements such as servers, databases, and networks. These methods leave the actual data exposed and at risk in the event of a breach. With data-centric security, the data is protected as soon as it is captured by an application. That makes the data useless to attackers, while preserving its format for the business processes that depend on it. Data-centric security approaches protect the data over its complete lifecycle—at rest, in motion, and in use.

Data Security: A Competitive Advantage

In today's global business environment, companies are increasingly finding their employees, business practices, and IT systems stretched across international boundaries. However, one element of a global enterprise remains surprisingly local: how to effectively manage data residency requirements and data privacy regulations.

Governments, regulatory bodies, and consumers are concerned about data privacy and what steps organizations should take to ensure the protection of data. Many jurisdictions and authorities have constructed an expanding array of guidance and laws to address security issues such as:

- Which information can be collected
- How data can be stored
- Where and how data can be transmitted
- Which security practices must be applied
- Actions that are required in the event of a data breach

Addressing data residency, protection, and privacy concerns requires an understanding of both international and domestic regulations. Companies that do business in Europe must understand the implications of regulations such as the European Data Protection Law as well as local data mandates in places such as Switzerland, Luxembourg, Singapore, and the Channel Islands.

In the United States, every state has applicable data protection laws and regulations. These laws vary widely from one state to another. Yet some rules apply to business conducted across state lines. For example, a company operating in Texas that owns data on customers residing in Massachusetts and California must comply with the disclosure and breach mandates of all three states.

Data protection and compliance, therefore, has become a highest common denominator issue, with the most aggressive laws driving corporate strategy. To meet these regulations, organizations need an information security solution that delivers comprehensive protection across all of their data and supports compliance with regulatory, standards, and policy requirements.

A data-centric security approach offers the most effective way to protect data as it is used, stored, or moved across data centers, cloud services, or mobile devices. But how can compliance directors and security officers choose the most effective, manageable, and affordable solutions for their enterprises?

This paper examines information privacy and data residency solutions that can help multinational businesses meet their data protection goals. It focuses on U.S. interstate and federal regulations, and European Union requirements as they apply both in the EU as well as in other jurisdictions, where regulations such as the U.S. Patriot II Act mandate can create conflicting requirements. We will also explore how two large global enterprises have leveraged data-centric security solutions from HPE Security—Data Security. These case studies describe how customers can cost-effectively meet compliance requirements and grow their business in regulated markets—using their legacy IT applications and infrastructure and existing processes and administrative staff.

Global Business Operations, Local Data Security Challenges

For many international companies, digital technologies have contributed to dramatic business growth and brand awareness. By gaining the ability to electronically transmit data, transfer funds, and collaborate efficiently across all time zones and geographies, many enterprises have successfully established a global footprint in their markets.

Yet making these connections opened up a myriad of new security issues. With more widespread electronic data transmission comes the need to protect these digital assets from various threats and dangers. As a result, organizations face a number of increasingly critical data protection challenges.

Regulatory issues

Many governments and regulatory authorities—both local and international—have developed data residency laws. For example, in Europe, financial regulator Commission de Surveillance du Secteur Financier (CSSF) prohibits the transmission and storage of personally identifiable information (PII) of nationals outside their home country. In order to do business in countries such as Luxembourg, companies must comply with this regulation and demonstrate the appropriate controls.

In addition, the European Data Protection directive establishes many strict data protection requirements. "Data collectors," those persons or entities that collect and process personal data, must respect the privacy and data protection rights of those individuals whose personal data is entrusted to them. According to the law, data collectors must "protect personal data against accidental or unlawful destruction, loss, alteration and disclosure, particularly when processing involves data transmission over networks." Furthermore, customers whose privacy has been breached must be notified within 24 hours[1]. This law has received a great deal of attention, because it threatens to fine violators up to 5% of their annual revenue, making it similar to existing anti-trust fines.

[1] New European Data Protection Law—A First Look; SNR Denton; **dentons.com/en/insights/articles/2012/january/9/privacy-and-data-security**

"Consider encryption. If an organization is sophisticated enough to ensure the reliable use of encryption, then it can avoid confidentiality risk in the public cloud whenever it is practical to encrypt data before uploading it to the cloud. As long as the organization has sole access to the encryption keys, there should be reduced concern about unauthorized access to the data on the part of law enforcement agencies, service provider administrators or hackers. In the unlikely event that law enforcement agencies seize the data, they would be unable to use it without coming back to the organization for the key. At that point the investigation would no longer be secret."

- Who's Afraid of the Patriot Act: Law Enforcement and Service Providers March 19th 2012 Gartner Inc.

Changing Data Security Issues

NEW DATA CHALLENGE	SAMPLE MANDATE
Data in a country where it cannot leave	Offshore banking rules in countries such as Switzerland, Luxembourg
Data in a state with new or changing regulations	California data breach law
Data related to a person who resides where data residency or privacy laws apply but where data is actually managed in another state or country	Massachusetts law that applies to the data of any state resident, no matter where in the U.S. it is processed

Data security breaches and regulatory non-compliance are not only caused by those seeking to do harm. In many cases, companies and employees with the best intentions can inadvertently violate regulations. In the United States, the International Traffic in Arms Regulations (ITAR) prohibit companies and individuals from importing or exporting defense-related information and materials But when data travels through electronic networks, companies can unknowingly share protected information, risking national security and heavy corporate fines.

Obviously this emerging collection of laws and requirements places a greater compliance burden on multinational organizations. Meeting these mandates requires an intensified focus on formal information access policies, privacy by design, a clearly articulated governance structure, and the appointment of data protection officers.

Threat environment

The threat environment is growing increasingly hostile. Financial data and associated PII present an attractive target to a broad class of threat actors, including organized cybercrime, malicious insiders, and hackers.

Cybercrime organizations are well-funded, financially motivated groups. They have at their disposal a variety of advanced attack methodologies, monetization networks, and constantly evolving tactics. According to the 2012 Data Breach Investigation Report[2] by Verizon, 83% of breaches were designed for financial gain by threat agents affiliated with organized crime.

Malicious insiders are also often financially motivated. In addition, these former trusted associates understand an organization's business processes and infrastructure weaknesses. With this knowledge, they create increased liability. Hackers—who have varied motivations for their activities—present continuous challenges, primarily for weak links in the overall system. "Hacktivism" from politically motivated groups can be a significant concern. For example, a group called Byzantine Candor, identified as China's preeminent hacker collective, infiltrated the European Union computers in the summer of 2011. According to Bloomberg Businessweek, these hackers are infiltrating systems and vacuuming up the proprietary data of U.S. corporations. The Verizon Data Breach Investigation Report notes that the incidence of hacktivism grew rapidly in the past year, accounting for 58% of all records breached.

Integration with the existing application and compute environment

Nearly all enterprises have already made a major investment in IT infrastructure, application development, and ongoing operations and compliance processes. To protect this investment, any data protection approach must integrate seamlessly with the existing IT ecosystem.

Data protection solutions must also support a user experience that facilitates an efficient, transparent workflow. Once sensitive data is captured by the front-end application, a security environment must handle any subsequent back-end processing in mainframe and data warehouse systems. The solution must handle this processing without changing the data format or negatively impacting overall throughput and latency.

[2] 2012 Data Breach Investigations Report; **verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf**

With organizations moving to cloud-based solutions—including private cloud, public cloud, and hybrid cloud solutions—data protection strategies must embrace this change and solve the regulatory challenges that go with it. A data-centric security approach does exactly that. The key to success is making sure the data-centric security approach is simple, consistently applied to any type of data, and able to be deployed across corporate systems. These criteria are critical whether the chosen solutions use mainframes or mobile technologies, and whether they are deployed on-premise or on-demand.

Traditional Data Protection Approaches Don't Measure Up

Meeting these security, privacy, and compliance challenges can be a time-consuming, costly struggle for companies. Chief security officers have invested in many traditional forms of security, hoping to ward off data breaches, meet compliance mandates, and enhance sustainability efforts.

But as the bad guys meet every new security approach with a more sophisticated data breach strategy, executives can feel like they are engaged in an unwinnable digital security arms race. What's more, the challenge of protecting data becomes even more complex when viewed in light of emerging trends such as mobility, big data, and cloud-based computing. For example, think of the new questions raised by mobility, where data moves both physically and logically. To determine whether data access should be allowed or denied, companies must be able to determine the context of access.

Hoping to stay ahead of this rapidly changing security landscape, many companies are taking action. Some organizations have deployed data centers in each country where they operate, hoping to keep data confined within legal boundaries by allowing customers to choose the specific data center where their data is stored. But since data can be accessed from anywhere, this approach is ineffective. A multi-data center strategy also creates unnecessary management costs and overhead.

Facing the challenges of cloud-based computing, some organizations consider putting all data through a single gateway. However, this strategy creates impossible latency issues. Others have opted for database-oriented tokenization strategies. This approach is effectively a step backward, creating a need to sync vast data repositories across long path networks.

Table 1: Evaluating Current Data Protection Approaches

DATA PROTECTION APPROACH	STRENGTHS	CONSIDERATIONS
Encrypt data in transit; SSL	Offers familiar, well-understood solution	Protects only data in transit
Encrypt data at rest; storage encryption	Provides minimal application and process impact	Protects only data at rest
Application encryption; internal project with cryptography toolkit	Addresses risk factors	Requires significant time, cost and implementation risk
Application encryption with data-centric security	Addresses risk factors and provides minimal application and process impact	Offers low risk and low cost of ownership

The Solution: Data-Centric Security

To adequately protect corporate and customer data, meet regulatory mandates, and reduce risk, businesses need to deploy solutions that can address these critical requirements:

- **Build security policy into the technology—**Bolt-on solutions are insufficient to meet company's unique security requirements, because they cannot accommodate corporate security policies.
- **Recognize reality of data lifecycle—**Data travels, among states and countries, users, within your value chain and outside it. Additionally, data now travels across different IT systems and end-user devices. No company can hope to contain data within traditional boundaries.
- **Stand up to scrutiny—**Without published proofs of security, protected data may not be as secure as one might think. In fact, unproven methods could mean violation of data security compliance requirements.
- **Scalable to meet business and IT requirements—**Data protection solutions should be architected to match the growth of the business and its data. Otherwise, business could be impacted.
- **Low impact and low TCO—**The success of the company and its data protection solution is dependent on easy deployment and low cost of operation. Low implementation complexity and cost means faster time-to-production.
- **Simpler is better—**Users must be shielded from the complexity of data security regulations and the need for access control. Otherwise, adoption is deterred and the security initiative will be stalled.

- **Secure structured and unstructured data—**The types of data that run a company are varied (structured and unstructured), and the data protection solution needs to secure them all the same while providing access to the authorized party as needed.
- **Support legacy systems—**IT environments today are heterogeneous, with new technologies working alongside legacy systems. Data protection solutions need to work with these legacy systems without extensive and complex re-engineering.
- **Support new technologies—**On the other hand, data protection solutions also need to work with new, cutting-edge technologies, including cloud and mobility, without rip-and-replace.
- **Support existing compliance processes—**Companies have archiving and e-discovery processes that cannot be disrupted due to compliance requirements. Data protection solutions need to enable these processes without extensive and complex re-engineering.

A data-centric approach to security can address each of these key requirements by supporting a new method of protecting data: at the data level itself. With data-centric security, the best defense is a good offense. As soon as data is captured by an application, data-centric security takes action. Using new methods of encryption, tokenization, and masking, the data is made useless to attackers without compromising its value to the business processes that depend on it.

This approach also protects data over its complete lifecycle—at the moment it is captured and stored, as it travels, and as it is used. Data can only be decrypted, detokenized, or unmasked by authorized users on a need-to-know basis, with access dictated by highly controlled, centrally-managed policies.

Data-centric security also simplifies compliance with privacy mandates and regulations. The data is useless to non-authorized parties who might accidentally access it, so it can be stored wherever is convenient for the customer and the business. As a result, companies are able to mitigate the risk of data breach while avoiding collision with data privacy regulations. They can also reduce the cost of protecting their most important assets: customer and corporate data.

HPE Security—Data Security offers innovative data encryption technologies such as HPE Identity-Based Encryption (IBE), HPE Format-Preserving Encryption (FPE), HPE Page-Integrated Encryption (PIE), and HPE Stateless Key Management that are easily integrated into existing security frameworks. With these technology advantages, data-centric solutions from HPE Security—Data Security provide dramatic business benefits:

- Reduce implementation and operational costs
- Easily scale data protection to meet business and IT needs
- Minimal implementation disruption to business and IT, as well as user productivity

- Ability to support data protection in new technologies such as cloud applications, big data, and mobility
- Extend the investment in existing IT systems and compliance processes
- Confident in proven security for sensitive data

Let's review two companies that addressed their data security challenges with data-centric security solutions.

Case study: Solving a data residency and privacy compliance challenge
A western European banking corporation with operations in 23 countries needed to meet the latest industry security mandates. Because it operates in Luxembourg, the bank was subject to the requirements of the CSSF. As a result, the bank was prohibited from transmitting, processing, or storing certain classes of data about Luxembourg nationals and from allowing sensitive data from leaving the country's boundaries.

The bank had already deployed Alnova Financial Solutions, a core banking application. Any security solution would need to integrate with and leverage the Alnova solution. Vendors proposed several security architectures to meet this need, including SSL links between the Luxembourg offices and the bank's data centers, as well as data-at-rest encryption solutions while the data was stored. All of these solutions were failed by CSSF reviewers.

The bank's partner Global Systems Integrator (GSI) demonstrated the use of the HPE SecureData architecture and solution. The GSI team identified three business processes, demonstrating the integration of HPE SecureData into the complex Alnova banking application. The process showed how the bank could encrypt and decrypt identified sensitive data using the HPE Format-Preserving Encryption technology, all without requiring any application changes. Each of the other solutions demonstrated to the bank required considerable customization of the Alnova application to handle traditional encryption approaches.

The bank chose to initially deploy the HPE SecureData solution within its Luxembourg location. HPE SecureData key servers are located within the jurisdictional boundaries of Luxembourg and managed by nationals employed by the bank. With this solution, sensitive data is encrypted at the point of capture within Luxembourg. It remains encrypted throughout its life, even when transmitted or stored outside Luxembourg. Sensitive data can only be decrypted against a local active directory, making it easy to process or view in clear text.

Case study: Protecting client-identifying data

A financial institution with headquarters in Switzerland provides services to private, corporate, and institutional clients. The company is present in all major financial centers, has offices in more than 50 countries, and employs more than 65,000 people around the world. The organization's businesses include wealth management, global asset management, and investment banking for a clientele of high net worth and ultra high net worth customers.

To meet Swiss banking laws, country-specific privacy laws, as well as client contractual obligations, the financial institution needed to protect critical privacy data, referred to as client-identifying data. To meet these needs, the company began evaluating products that would mask critical privacy data. The firm wanted an enterprise solution that would address cloud security, client confidentiality, and protection of both test and development data. A solution that could be supported as a central service would help cut costs by reducing the number of solutions used across the lines of business.

In its evaluation, the bank focused on HPE SecureData and its underlying HPE Format-Preserving Encryption technology. The HPE Security—Data Security team organized a proof of concept driven by a comprehensive business use case, which helped the company understand how it could use the solution for production-level data masking. During the proof of concept, the team fully tested simple API, CL ("Command Line"), and Web services interfaces.

The financial institution selected the HPE SecureData solution for an enterprise-wide deployment. To support the initial use case, developers from the bank are using HPE Security—Data Security solutions to write a middle layer that masks data as it moves from production to test systems. The bank is expanding the deployment to protect production data in the cloud, as well as in internal systems across the enterprise.

For More Information

HPE Security—Data Security provides a broad collection of innovative solutions, including data-centric encryption, tokenization, data-masking, and key management technology that can help businesses address today's complex security challenges and combat new and emerging security threats.

Table 2: HPE Security–Data Security provides data-centric security and stateless key management for protecting data, from mainframe to mobile

HPE Security—Data Security Product	FEATURES
HPE SecureMail Cloud	Provides services and applications for encryption and key management that are built on a cloud scale, multi-tenant infrastructure hosted by HPE Security—Data Security.
HPE SecureMail	Employs proven encryption technologies and innovations that enable global scale deployments of end-to-end email protection that are simple to manage and administer, for enterprises of all sizes, from desktop to mobile.
HPE SecureData Enterprise	Provides a comprehensive data protection solution uniting end-to-end encryption, tokenization, and masking for PCI cardholder data and all other sensitive information, with minimal impact to business process, work flow, and applications.
HPE SecureData Payments	Provides complete end-to-end data protection for payment transactions, from the point of capture to authorization, settlement, and beyond.
HPE SecureData Web	Protects payment information at the browser and keeps it protected all the way through the transaction system in the payment processor; shields the data from theft in all of the merchant and intermediate systems; and also reduces the footprint subject to PCI requirements.
HPE SecureFile	Provides encryption to protect files and documents used by individuals and groups, regardless of whether those files are on the desktop, network share, or collaboration portal.

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

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-0217ENW, April 2016, Rev. 1