Your Business Will Be Attacked. How Safe is Your Most Valuable Asset?

Data protection solutions must keep pace with new technologies and emerging data sources.

01.17 EB7214 DATA SECURITY

Hewlett Packard Enterprise

TERADATA.

Table of Contents

Organizations' network data are under constant attack. The data can be used by hackers to blackmail or embarrass companies, exploit or sell customer financial information, or steal company trade secrets and intellectual property to sell as their own.

To protect the data, businesses must keep it secure, regardless of where it's used, stored, or transferred. This requires a strategy to keep data safe while allowing it to be used by the business and to make sure it complies with privacy regulations. With data in constant motion and facing unrelenting attacks from inside and outside the enterprise, organizations must have end-to-end protection, from the moment of capture across the information lifecycle, including testing and production.

The risks have never been higher. Companies have more data than ever before, and hackers are more sophisticated and determined to get it. Businesses that fail to keep their data safe face customer loss, reputational damage, legal actions, and starting May 25, 2018, enormous penalties from the European Union (EU) for non-compliance with the General Data Protection Regulation (GDPR). The good news is that innovative, data-centric security solutions such as strong format-preserving encryption and tokenization technologies can keep even the most sensitive data safe.

New Data Uses Call For New Protections

Businesses need to make full use of their data and analytics, and subject that data to more applications and uses. Many security technologies and strategies limit data access. This runs counter to the business need for free movement and broad authorized access to data in order to leverage its maximum value and insights. Today, this data is companies' most precious asset.

Data security can present challenges when using new ecosystems that rely on data lakes and Internet of Things (IoT) data. As companies implement unified architectures that include Hadoop data lakes, and ingest and leverage IoT sensor data, the information must be safe in these environments. Big data, Hadoop, and IoT have increased the complexity of security requirements. Today the aggregate attack surface is significantly larger than just three to five years ago as more devices, places, connections, and networks are operational for hackers to target.

When companies tap into new solutions and data sources, they must have a data security strategy in place. Data protection measures are much more effective when they're implemented as new technologies and applications are added, not bolted on later with limited capability. Ideally, data is protected as close to its source as possible. Encryption, tokenization, and data masking protection techniques are key components of a layered defense security strategy for protecting data in new and existing technologies.

More At Stake For Businesses

Companies have more at stake with data security than at any time in their histories. EU data protection regulations regarding security, privacy, and breaches (effective May 2018) are posed to have a far-reaching impact on organizations worldwide. Under GDPR:

- Data protection processes must be compliant
- Breaches must be reported within 72 hours
- Organizations face a fine of up to 4% of their global annual revenues—enough to put many companies out of business

GDPR affects any company doing business in the EU or involving EU citizen information. This means almost every large company doing international business will be impacted. For example, a telecommunications company in America with customers holding dual citizenship in the U.S. and a European country are covered under GDPR. So are businesses with offices in the EU and those with customers who are European citizens.

In addition to meeting regulations, companies need to safeguard their data to protect their reputations, customers, intellectual property, and confidential information. Securing data could even save lives. A hacker taking over a self-driving car, for instance, could kill the driver, occupants, and bystanders.

Best Practices Offer Protection, Negate Risks

Most data breaches, 84 percent[1], happen at the application layer or in gaps between levels when data is potentially exposed. Fundamental security controls dramatically reduce the likelihood of a successful attack. Data-centric security, for example, can provide protection from the moment data is ingested, throughout analysis, and to back-end data storage.

Robust format-preserving encryption offers substantial protection benefits. It uses pseudonymization—actual data is replaced with artificial identifiers—to minimize exposure of personal data and eliminate the ability to identify consumers and employees. As a result, this encryption mitigates risks inherent in data processing. It may even remove the requirement in GDPR to notify people of a data breach since strongly encrypted data is virtually useless to a hacker. While GDPR does not specify technologies to use to enable compliance, it does encourage encryption and pseudonymization to protect sensitive data.

With format-preserving encryption, even if a security system is breached, encrypted data is worthless to hackers because today's algorithms and keys would require enormous time and effort, maybe even years, to compromise. However, because encrypted data looks like the real thing, data scientists and business intelligence experts are able to use it to identify patterns, make discoveries, and run queries without having to decrypt it. This enables deep insights in less time than with

5 Essentials for Data Protection

Companies can reduce 80% of data vulnerabilities with:

- Hardware management
- Software management
- Malware defense
- Configuration management
- Vulnerability management

traditional encryption, while preserving the referential integrity required between real and encrypted data. It also allows data sets to be mobile between systems, databases, and around the globe while protected.

Protection Across Platforms

A single breach is all it takes to severely damage a company, or even put it out of business. That's why security requires solutions that protect the data without limiting its use. With the right solutions, including a data-centric approach applying format-preserving encryption, tokenization, and data masking protection, companies can keep their data safe and secure across all platforms while leveraging the information to enhance their business.

For More Information

Teradata solutions allow businesses to leverage all of their data across all applications and uses to gain maximum value. The solutions should be part of security plan that relies on big data analytics to provide intelligence about threats and optimize cyber defense strategies, and an integrated data warehouse (IDW) to reduce the dispersion of data storage throughout an organization, increasing the overall effectiveness and manageability of a comprehensive security program. When data is in an IDW, security efforts can be focused and easily monitored and maintained without the risk of weaknesses in a single uncontrolled database exposing the entire enterprise environment to risk.

Teradata advocates for a comprehensive approach to information security that includes an orchestrated combination of technology and best practice processes. Teradata helps protect data while empowering companies to achieve high-impact business outcomes. For more information, visit **Teradata.com**.

End-to-End Data Security Solutions

Protecting data isn't easy. Many organizations quickly discover the complexities and management challenges inherent in traditional security approaches. Hewlett Packard Enterprise (HPE) provides innovative and effective solutions. It offers the fastest National Institute of Standards and Technology (NIST) certified format-preserving encryption for a highly granular and scientifically vetted approach to encryption that facilitates field-level protection. Business functionality is also preserved, meaning that normal data processing activities and analytics are maintained even though data is encrypted.

HPE Stateless Key Management facilitates robust encryption even at high volumes. The company's **HPE Secure Stateless Tokenization** is also an advanced, patented data security technology that offers a new approach to protect payment card data. **HPE SecureData** unites market-leading **HPE Format-preserving Encryption** with tokenization, data masking and key management to protect sensitive information in a single comprehensive solution.

HPE SecureData offers continuous data protection to reduce threats from insiders, malware and advanced external attacks to systems. Its solutions provide end-to-end data security in databases, mission-critical mainframes and applications while the information is in use, motion and storage.

Cyber Crime by the Numbers

1.9 Number of successful attacks per week on organizations[2]

46 Days needed to resolve a cyber attack (up from 14 days in 2010)[2]

59 Percent of employees who steal proprietary corporate data when they quit or are fired[3]

93 Percent of breaches that take minutes or less to compromise a system[4]

63 Percent of confirmed data beaches that leverage a weak, default or stolen password[4]

$2.1 trillion
Estimated cost of data breaches by 2019[5]

End Notes

1. Verizon's 2016 Data Breach Investigations Report: **www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf**
2. Ponemon Institute, "2015 Cost of Cyber Crime Study: Global," HP-commissioned study, October, 2015, **itnewsafrica.com/hp/IT%20management%20and%20monitoring/HPE_security.pdf**
3. Heimdal Security, "10 Alarming Cyber Security Facts that Threaten Your Data." May, 2016, **heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety**
4. Office of the Secretary of Defense, memo, Sept. 30, 2015, Verizon, "2016 Data Breach Investigations Report," April, 2016, **www.verizonenterprise.com/verizon-insights-lab/dbir**
5. Juniper Research, "Cybercrime Will Cost Businesses Over $2 Trillion By 2019," May, 2015, **www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion**

10000 Innovation Drive, Dayton, OH 45342 **Teradata.com**

01.17 EB7214

Hewlett Packard Enterprise

TERADATA