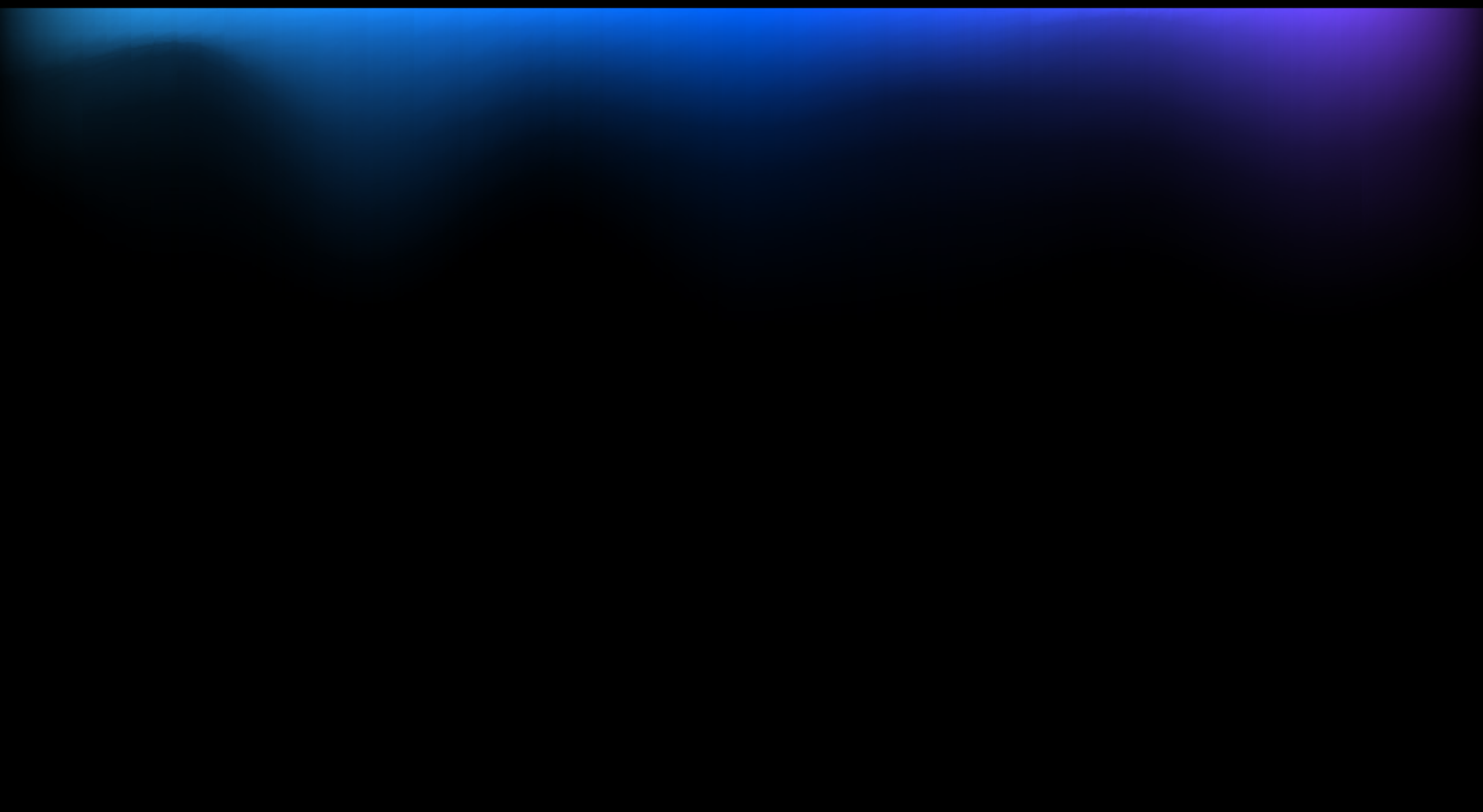
IBM Security

February 2020

Encryption: Protect your most critical data

Learn how encryption can help safeguard your data against threats and address compliance



IBM

Contents

Introduction

Encryption is all around us. Our emails can be encrypted. Our video conferences can be encrypted. Even our phone calls can be encrypted. It's only natural then to assume our most sensitive business data should also be encrypted. Yet according to Ponemon Institute's 2019 Global Encryption Trends Study, the average rate of adoption of an enterprise encryption strategy is only 45 percent for those surveyed.[1]

How can you be sure that all your sensitive data is encrypted? First, you need to know where it is located. With siloed databases, cloud storage and personal devices in the mix, there's a good chance that at least some of your sensitive data is exposed. A data breach could lead to the worst kind of exposure — the kind where you notify millions of customers that you failed to protect their privacy and their personal information.

But that doesn't have to be your reality. The right encryption strategy will not only help protect your data, it can help strengthen your compliance posture. IBM Security Guardium helps identify your sensitive data — on premises and across hybrid multicloud — and helps to protect it with robust encryption and key management solutions. Plus, IBM Security's strategic consulting can work with you to align your encryption strategy with business goals.

Encryption for a world in motion

The most successful businesses are driven by data and analytics. A recent study from Forrester found that such businesses, on average, grow at least seven times faster than global GDP[2] — and driving implies movement. Your data can move between clients and servers. It can move over secure and non-secure networks. It can move between databases in your network. It can move between clouds. Safeguarding your sensitive data on these journeys is critical. Customers expect it and many regulatory agencies require it. So why doesn't every business do it?

Many organizations simply don't have the skills and the resources needed to effectively protect all the critical data in their business. Maybe they have a general security strategy but have not dedicated the time and effort to creating a data encryption strategy. It's a common problem, and one that cybercriminals prey upon by extracting unencrypted data and gaining unauthorized access to under-protected encryption keys.

What can you do to help protect your business? **You can start by encrypting your sensitive data, implementing strong access controls, managing your encryption keys securely and aligning your encryption efforts with the latest compliance requirements.** Without these safeguards in place, your data might not be as protected as it could be.

IBM Security Guardium helps identify your sensitive data — on premises and across hybrid cloud — and helps to protect it with robust encryption and key management solutions.

Is your critical data protected?

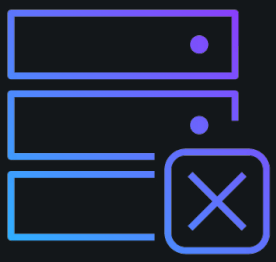
Security professionals — tasked with preventing data breaches, stolen passwords and internal espionage — should be concerned about the level of protection of their data, since data is the lifeblood of their businesses. Encryption can help to make data unusable in the event it is hacked or stolen. Think of it as the first and last line of defense that can help protect your data from full exposure.

There are steps you can take to protect your organization's data. A good place to start is identifying what data needs to be protected and where it is located. (The answer: more data than you realize and in more places than you expect.) Customer and financial data are obvious choices for encryption, but many companies fail to realize that even older, seemingly non-critical data can contain sensitive information, partly because the definition of what constitutes personally identifiable information (PII) has broadened considerably in the last decade.

Controlling and monitoring data access represents an important part of any data encryption strategy. It's something that organizations need to balance with frictionless access to data. You want to make sure the right people have quick access to the data they need, while blocking the access privileges of unauthorized users. This is where security best practices can be invaluable:

- Keep your encryption keys stored in a safe and separate location from your data
- Rotate your encryption keys frequently and align your key rotation strategy with your industry's best practices for key rotation
- Always use self-encrypting media to help protect data on your devices
- Layer file and database encryption on top of media encryption to provide granular control over access and cryptographic erasure
- Use techniques such as data masking and tokenization to anonymize PII data that you share with outside parties

Encryption can help to ensure that data is unusable in the event it is hacked or stolen.



Use encryption to defend against threats

Most security professionals are aware of the threats of data breaches and ransomware. They're on the news, they're on their minds and stopping them is at the top of most companies' strategic imperatives. So why do data breaches still occur? Because, for cybercriminals, data breaches and ransomware attacks still work.

Ransomware attacks and data breaches are on the rise, so businesses should be prepared for these types of threats.[2] It's important to note that preparation is different from protection. You can try to protect against network attacks and insider threats 100 percent of the time, but you won't always be successful. There are simply too many variables, too many chances for human error and too many cybercriminals looking to exploit those vulnerabilities to stop everything. This is why preparation is important — because you actually can encrypt your most sensitive data and render it useless in the event of a breach.

Encryption should be your first and last line of defense against attacks. It protects your data and your organization against internal and external threats and helps safeguard sensitive customer data. But encryption isn't your only line of defense. Secure and consistent access controls across all your environments — on premises and in the cloud — as well as secure key management is important for keeping sensitive information out of the wrong hands.

Secure and consistent access controls across all your environments — on premises and in the cloud — as well as secure key management is important for keeping sensitive information out of the wrong hands.

Use encryption to help address compliance

Security professionals aren't the only ones concerned with data protection. Countries, states and industry consortiums are entering the privacy picture with increasing frequency. For example, in 2019 and 2020 respectively, Europe's Global Data Protection Regulation (GDPR) and the California Consumer Protection Act (CCPA) introduced new security requirements that can levy heavy fines for non-compliance.

Keeping up with regulations can be difficult work. **Understanding what data is impacted by specific regulations in each jurisdiction, the reporting requirements and even the penalties for non-compliance can be a full-time job.** And in a world where full-time compliance experts are in scarce supply, many organizations have much to do before achieving compliance readiness.

Encryption, to borrow an expression, can cover a multitude of security sins. It can help to make your critical and sensitive data — what cybercriminals desire — worthless to would-be thieves. In many cases, compliance regulations mandate data encryption on some level. But beyond basic encryption, there are additional measures that every organization can take to protect their data. For example, using pseudo-anonymization strategies such as data masking and tokenization to selectively hide sensitive data as it's being shared with partners can help make your data productive and protected. Using self-encrypting media on any device that stores data is another important safeguard that can help to prevent unauthorized parties from gaining access to data on stolen or salvaged devices.

How IBM Security Guardium can help protect your data

IBM Security Guardium can provide you with advanced and integrated solutions that help your organization identify, encrypt and securely access your most sensitive data.

In addition, IBM Security offers security services and expertise to help your organization develop effective, efficient data protection strategies. At the heart of our encryption solutions are the IBM Security Guardium Data Encryption family of products and IBM Security Guardium Key Lifecycle Manager (GKLM).

IBM Security Guardium Data Encryption (GDE) helps protect critical data across all your data environments, helping to address compliance with industry and government regulations. The integrated family of products that make up GDE feature encryption for files, databases, applications and containers, as well as centralized key and policy management. GDE also provides data masking and tokenization, in addition to integration with third-party hardware security modules.

IBM Security Guardium Key Lifecycle Manager (GKLM)* helps deliver a secured, centrally managed encryption key management solution that supports the Key Management Interoperability Protocol (KMIP) — the standard for encryption key management — and features multi-master clustering for high availability and resiliency. GKLM can help organizations follow industry best practices for encryption key storage, access, security and reliability. GKLM simplifies encryption key management, synchronizes encryption keys between on-premises and cloud environments and automates many encryption functions, including self-encryption for storage media.

To learn more about how IBM Security can help you protect critical data against threats and address compliance through our encryption solutions, follow the links below.

IBM Security Guardium Data Encryption
IBM Security Guardium Key Lifecycle Manager
IBM Security Guardium

*Formerly Security Key Lifecycle Manager (SKLM)

Sources

1. Ponemon Institute, 2019 Global Encryption Trends Study.
2. Forrester Research, Inc., Insights-Driven Businesses Set The Pace For Global Growth, October 19, 2018.

IBM Security

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
February 2020

IBM

JYBMP8LZ