

Why Encryption at Rest Matters for Your Business

Daniel Gleim · 2025-04-22



ENCRYPTION AT REST: WHAT IT IS AND WHY YOUR BUSINESS NEEDS IT



Encryption at Rest: What It Is and Why Your Business Needs It

In today's digital landscape, businesses generate and store large volumes of sensitive data—customer records, financial transactions, intellectual property, and proprietary business information. With cyber threats continuing to evolve, it's more important than ever to ensure that stored data is protected from unauthorized access.

One of the most effective strategies for protecting stored data is **Encryption at Rest**. In this article, we'll explore what Encryption at Rest is, how it works, and why it's an essential part of a modern data security strategy.

What is Encryption at Rest?

Encryption at Rest refers to the process of encrypting data while it is stored on a physical or virtual storage medium, such as a hard drive, solid-state drive, database, file server, or cloud storage system. This means that even if someone gains access to the storage device, they won't be able to read or use the data without the proper decryption keys.

Why is Encryption at Rest Essential for Businesses?

Minimizes the Risk of Data Exposure

When a data breach occurs, the main concern is often the exposure of sensitive information. Encryption at Rest helps reduce this risk by ensuring that any stolen or leaked data remains inaccessible without the correct keys.

For example, if an attacker manages to gain access to a cloud storage bucket, encrypted files will remain unusable unless they can also obtain the decryption keys.

Mitigates Insider Risk

Not all threats come from the outside. Sometimes employees or contractors may unintentionally or deliberately access information they shouldn't. With Encryption at Rest, even users who have access to storage systems won't be able to view sensitive data unless they have the appropriate decryption keys.

Builds Customer Confidence

People are becoming more aware of how their data is handled. Businesses that take proactive steps to protect sensitive information—like implementing Encryption at Rest—can strengthen their relationships with customers and partners by demonstrating a commitment to data privacy and security.

Protects Data on Lost or Stolen Devices

Portable devices such as laptops or external drives can easily be lost or stolen. If those devices contain unencrypted data, it could fall into the wrong hands. Encryption at Rest ensures that the data on these devices is protected, even if the hardware itself is compromised.

Enables Secure Data Disposal

When it's time to retire or repurpose storage devices, Encryption at Rest makes it easier to securely dispose of data. Simply deleting the encryption keys renders the data unreadable, eliminating the risk of it being recovered later.

How Encryption at Rest Works

Encryption at Rest uses cryptographic algorithms to convert readable data (plaintext) into an unreadable format (ciphertext). Only users or systems with the correct decryption key can access the original data. The basic process includes:

1. Choosing an Encryption Algorithm – Common choices include AES-256 or RSA.
2. Managing Encryption Keys Securely – Key management is essential to maintain access control and prevent unauthorized decryption.
3. Applying Policies and Access Controls – Organizations decide which data needs to be encrypted and under what conditions access is granted.

Implementing Encryption at Rest with Search Guard

Search Guard introduced a dedicated **Encryption at Rest** solution designed for modern search technologies. This capability will help businesses protect stored data and ensure it remains inaccessible to unauthorized users—even in the event of a storage compromise.

With Encryption at Rest from Search Guard, organizations can:

- **Improve data security** across their deployments, ensuring their sensitive information remains secure even when stored on disk in public cloud environments

- **Streamline compliance** with data protection regulations meeting requirements of PCI, ISO, SOX, and similar regulations with Encryption at Rest's advanced encryption capabilities
- **Demonstrate responsible data practices** to customers and stakeholders

Search Guard's approach is focused on making encryption easy to implement and manage—ensuring that your security posture keeps pace with your business needs. Click this [link](#) to learn more!

Conclusion

Encryption at Rest plays a key role in helping businesses protect sensitive data, maintain compliance, and build trust. Whether data is stored on-premises or in the cloud, encrypting it ensures that even if someone gains unauthorized access, the information remains secure.

Search Guard's Encryption at Rest solution will provide a reliable and user-friendly way to secure stored data. It's a smart step forward in any organization's data protection strategy.

Looking to strengthen your security posture? Contact us or check out this [link](#) to learn more!

This article was published on the Search Guard blog: <https://search-guard.com/blog/why-encryption-at-rest-matters-for-your-business/>

Search Guard is Security and Alerting for Elasticsearch and Kibana — search-guard.com · [Start a free trial](#)