

Encryption at Rest – Real-World Use Cases and Industry Applications

Daniel Gleim · 2025-08-25



ENCRYPTION AT REST—REAL-WORLD USE CASES AND INDUSTRY APPLICATIONS

As digital systems grow more complex and interconnected, the need to store data securely has become critical. While encryption at rest is widely recognized as a best practice, many organizations still treat it as a compliance checkbox rather than a strategic tool for reducing risk, protecting reputation, and simplifying regulatory efforts.

In our previous article, we explained what Encryption at Rest is and how it protects stored data from unauthorized access. In this follow-up, we'll look at how organizations apply it in practice and why it's becoming increasingly important in the face of emerging threats and technologies.

How Organizations Use Encryption at Rest: Real-World Applications

Encryption at Rest isn't limited to one specific industry. It's used anywhere sensitive data needs protection—whether that's patient records, financial transactions, or customer information. Below are several common use cases across sectors where Encryption at Rest plays a critical role.

Healthcare

Hospitals, clinics, and healthtech companies handle a wide range of highly sensitive data, including medical histories, lab results, treatment plans, and personal identifiers. This information is protected under stringent privacy regulations like **HIPAA** (Health Insurance Portability and Accountability Act), which mandates robust safeguards to ensure the confidentiality, integrity, and availability of patient data.

Encryption at Rest plays a pivotal role in meeting these requirements. By encrypting patient data when stored on servers, cloud platforms, or external devices, healthcare providers can ensure it remains inaccessible to unauthorized users—even in the event of a breach or physical device loss. Beyond regulatory compliance, encryption also builds patient trust, as individuals increasingly expect their

healthcare providers to prioritize data privacy and security. With rising concerns about cyber threats targeting the healthcare sector, adopting Encryption at Rest is no longer optional but a critical part of a comprehensive data protection strategy.

Finance

Banks, insurers, and investment firms are prime targets for cyberattacks, given the sensitive nature of the data they handle—credit card numbers, transaction records, customer financial profiles. These organizations must comply with strict standards like **PCI-DSS**, which mandates strong protections for stored cardholder data.

Encryption at Rest ensures that financial information remains secure, even if systems are breached. Encrypted data is unusable without decryption keys, making it far less valuable to attackers. Investment firms face unique challenges when protecting proprietary trading algorithms and market analysis data—information that represents competitive advantage worth millions. By adopting this practice, financial institutions not only safeguard their data but also demonstrate a commitment to privacy and security, which is critical for building customer trust in an increasingly digital economy.

E-commerce and Retail

E-commerce platforms and retail businesses manage an extensive amount of sensitive customer information—ranging from payment details and shipping addresses to purchase histories and loyalty program data. These organizations are frequent targets of cyberattacks due to the high volume of transactions and the potential for financial gain. Data breaches in the retail sector are not only costly but can also result in severe reputational damage.

Regulations such as the **General Data Protection Regulation (GDPR)** in the EU and **CCPA** (California Consumer Privacy Act) in the US require retailers to safeguard customer data and be transparent about how it is handled. **Encryption at Rest** is crucial for protecting sensitive customer information during storage, ensuring that even if a hacker gains access to a retailer's systems or databases, the encrypted data remains unusable without the decryption keys.

Additionally, Encryption at Rest helps maintain the integrity of customer data, reducing the risk of identity theft, payment fraud, and financial loss. By implementing strong encryption practices, retailers can demonstrate their commitment to data privacy, which not only helps with compliance but also builds consumer trust—a vital asset in a competitive market where customers are more concerned than ever about the security of their personal information.

The Hidden Costs of Unencrypted Data

According to IBM's 2024 Cost of a Data Breach Report, the global average breach cost reached \$4.88 million. However, breaches involving encrypted data tend to be significantly less costly, as the stolen information remains unusable to attackers.

Unencrypted data breaches typically force organizations to shut down systems entirely while they assess the extent of the exposure. In contrast, encrypted environments can often remain operational during investigations, reducing both business disruption and revenue loss. Breaches also tend to erode

customer trust, leading to customer loss—a costly outcome, as acquiring new customers is significantly more expensive than retaining existing ones.

Encryption in Modern Development

Modern software development has fundamentally changed how organizations approach data protection. With DevSecOps practices gaining traction, security measures—like encryption—are now integrated directly into the development pipeline, embedding protection from the earliest stages.

Today's applications often employ layered encryption strategies. At the field level, sensitive data such as social security numbers or credit card information is secured using column-level encryption. In parallel, transparent data encryption (TDE) protects entire databases without requiring changes to application logic.

As containerized applications and microservices become standard, encryption strategies must evolve. Container images commonly contain sensitive elements such as API keys, configuration files, and certificates—all of which must be securely stored. At the same time, development pipelines themselves manage valuable resources like source code and deployment credentials, which must also be encrypted throughout the software delivery lifecycle.

Cross-Border Data Protection

In a global economy, data frequently crosses national borders—and with it, regulatory boundaries. Some countries require that sensitive data remain within their jurisdiction. Encryption can help meet these rules, especially when encryption keys are retained within the country of origin.

But effective encryption isn't just technical—it's cultural. Employees must understand why it matters. Ongoing training and awareness programs help build a security-first mindset. Organizations should also test their ability to respond to encryption-related incidents, such as key compromise or backup recovery scenarios.

Conclusion

From hospitals to online retailers, government agencies to emerging technology companies, Encryption at Rest proves to be a foundational element in protecting sensitive data and maintaining stakeholder trust. The real-world applications demonstrate that encryption is not just a technical requirement but a business enabler that allows organizations to innovate while maintaining security and compliance.

Modern organizations that view encryption as a strategic investment rather than a compliance burden are better positioned to compete in data-driven markets. They can pursue new business opportunities, adopt emerging technologies, and build customer trust more effectively than organizations that treat encryption as an afterthought.

In our next article in this series, we'll explore how Encryption at Rest supports compliance with major standards like PCI-DSS and GDPR, and why it's gaining importance in response to emerging threats like ransomware and cloud vulnerabilities.

This article was published on the Search Guard blog: <https://search-guard.com/blog/encryption-at-rest-real-world-use-cases-and-industry-applications/>

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