Encryption at Rest – Compliance and Future-Ready Security

Daniel Gleim · 2025-09-09

In our previous article, we explored how Encryption at Rest is used across industries like healthcare, finance, and e-commerce to protect sensitive data and meet customer expectations. In this article, we'll dive deeper into how Encryption at Rest supports compliance with international data protection standards and examine why it's becoming more essential than ever in response to new cybersecurity challenges.

Compliance: Meeting Global Standards with Encryption at Rest

As businesses operate in an increasingly regulated landscape, compliance with data protection laws is more critical than ever. Whether it's about securing personal information or demonstrating accountability to customers, organizations must adopt practices that meet both local and international standards. **Encryption at Rest** is one of the most effective and widely accepted ways to achieve this.

PCI-DSS (Payment Card Industry Data Security Standard)

For companies handling payment card information, **PCI-DSS** mandates strict security controls to protect cardholder data. Encryption at Rest is central to meeting these requirements, ensuring that payment information—such as credit card numbers and transaction records—remains protected even if systems are compromised. Failure to comply can lead to heavy penalties and the loss of payment processing privileges.

GDPR (General Data Protection Regulation)

The **GDPR** requires organizations operating in or serving the EU to secure the personal data of EU citizens and encryption is explicitly recommended as a technical measure to protect this data. With Encryption at Rest, personal details like names, contact information, and payment history are secured

against unauthorized access—even during a breach. In some cases, properly encrypted data may not be considered personal data under GDPR, reducing reporting obligations and regulatory impact.

SOX (Sarbanes-Oxley Act)

The **Sarbanes-Oxley Act (SOX)** requires public companies in the U.S. to maintain strict internal controls over financial reporting and data integrity. Encryption at Rest helps fulfill these controls by protecting stored financial data against unauthorized changes or disclosure, supporting audit readiness and compliance.

ISO 27001

ISO 27001 outlines best practices for building and managing an information security management system (ISMS). Encryption at Rest is one of the recommended controls under this standard, ensuring that sensitive data remains protected wherever it's stored—on-premises or in the cloud.

The Economics of Compliance

While GDPR fines can reach up to 4% of global annual turnover, implementing robust encryption typically requires only a small fraction of an organization's IT budget. Organizations with mature encryption programs often experience smoother compliance audits, and many cyber insurers offer premium discounts for comprehensive encryption strategies.

Industry Trends and Emerging Threats

As technologies evolve and attackers become more sophisticated, encryption is no longer a "nice to have"—it's an essential safeguard.

Cloud Adoption and Hybrid Environments

The growing shift to cloud environments reinforces the shared responsibility model: while cloud providers secure the infrastructure, organizations remain responsible for protecting their own data. Encryption at Rest provides strong protection in multi-cloud and hybrid environments, giving organizations control over who can access what, even in third-party infrastructure.

Managing encryption keys across multiple cloud providers adds complexity, which is why customer-managed encryption keys (CMEKs) have become a best practice for cloud-based security.

Rise in Ransomware Attacks

Ransomware continues to evolve, often combining encryption with data theft and extortion. While traditional ransomware encrypts your data, newer variants also threaten to leak it unless a ransom is paid.

Encryption at Rest helps mitigate this risk. If data is encrypted before attackers access it—and they don't have the decryption keys—then its value drops dramatically. In other words, encryption doesn't just protect systems; it diminishes the attacker's leverage.

Increased Regulatory Scrutiny

From **GDPR** and **CCPA** to national cybersecurity laws and sector-specific regulations, organizations face growing expectations around how they protect data. Encryption at Rest provides a transparent, defensible control that satisfies auditors and demonstrates proactive risk management.

IoT and Connected Devices

The rapid growth of IoT devices means they often store or process data locally—sometimes in physically insecure environments. Encryption at Rest ensures that even if a device is lost or stolen, the data on it remains protected.

To truly secure data across these networks, organizations must implement **end-to-end encryption**—securing data from the edge all the way to backend systems.

Zero-Trust Architecture and Encryption

In a zero-trust environment, nothing is trusted by default—not devices, not users, not internal systems. Every request must be verified.

Encryption at Rest plays a key role here. It acts as a final line of defense if identity verification or access control fails. Advanced zero-trust implementations may also include identity-based encryption, where only specific users or services can decrypt specific data, further reducing exposure.

Automation and Encryption Management

The growing adoption of encryption has made automation a critical factor in managing it efficiently. Organizations are increasingly deploying:

- **Policy engines** to apply encryption based on data classification and location
- **Key management systems** that automatically handle key generation, rotation, and expiration
- **Automated compliance reporting** to generate real-time visibility into encryption status

Together, these systems reduce human error, improve scalability, and simplify audit processes.

Organizational Success Factors

Even with the right tools in place, encryption programs only succeed when supported by culture and leadership. Executive sponsorship ensures that encryption remains a business priority, not just a technical task.

Cross-functional collaboration between security, development, operations, and compliance teams ensures encryption is implemented in ways that support—not hinder—business goals.

Success metrics might include:

- Percentage of sensitive data encrypted at rest
- Reduction in breach impact
- Improvements in audit outcomes and reporting efficiency

Conclusion

Encryption at Rest is no longer just a technical safeguard—it's a strategic pillar for compliance, resilience, and trust in today's data-driven world. As businesses face an evolving landscape of regulation, cyberthreats, and digital transformation, proactive encryption practices offer a clear path forward.

The organizations that succeed in the coming decade will be those that view encryption not as a burden, but as an enabler of innovation and growth. By implementing comprehensive encryption strategies today, businesses position themselves to adapt quickly to new challenges and opportunities while maintaining the trust of customers, partners, and regulators.

To learn how SearchGuard's Encryption at Rest solution can help your organization protect stored data and simplify compliance, click here.

This article was published on the Search Guard blog: https://search-guard.com/blog/encryption-at-rest-compliance-and-future-ready-security/