Encryption at Rest for Elasticsearch: The Complete Series

Daniel Gleim · 2026-07-16

Encryption at Rest, start to finish

Over three articles we worked through Encryption at Rest from the ground up: what it is and why it matters, where it shows up across industries, and how it maps to the compliance standards teams actually get audited against.

If you run Elasticsearch or OpenSearch in production and encryption at rest is on your list this year, this is the whole series in one place, plus a short FAQ for the questions that come up most on demo calls.

Part 1 · Why Encryption at Rest Matters for Your Business

Encryption at rest protects data while it sits on storage, whether that is a drive, a database, a file server, or cloud storage. If someone reaches the storage layer without the keys, the data stays unreadable.

Part 1 makes the practical case. Encryption at rest minimises data exposure in a breach, mitigates insider risk, protects data on lost or stolen devices, builds customer confidence, and enables secure data disposal, since deleting the keys renders the data unrecoverable. It also covers the mechanics: common algorithms such as AES-256, why secure key management is the part that actually matters, and how Search Guard's Encryption at Rest brings this to modern search deployments while helping meet requirements under frameworks like PCI, ISO, and SOX.

Read Part 1: https://search-guard.com/blog/why-encryption-at-rest-matters-for-your-business/

Part 2 · Real-World Use Cases and Industry Applications

Part 2 moves from theory to the floor: where encryption at rest earns its place, and why treating it as a compliance checkbox misses the point.

It walks through three sectors. Healthcare protects medical histories, lab results, and personal identifiers under HIPAA. Finance protects card numbers, transaction records, and customer profiles under PCI-DSS, and for investment firms, proprietary trading algorithms worth millions. E-commerce and retail protect payment details, shipping addresses, and purchase histories under GDPR and CCPA.

It also puts numbers on the risk. IBM's 2024 Cost of a Data Breach Report put the global average breach at $4.88 million, and breaches involving encrypted data tend to cost less because the stolen data stays unusable. Encrypted environments can often keep running during an investigation instead of shutting down entirely.

The article closes on modern practice: encryption built into the pipeline through DevSecOps, field-level and transparent database encryption, encryption for containers and microservices, and cross-border data protection where keys are kept in the country of origin. The point running through it is that mature organisations treat encryption as a business enabler rather than a burden.

Read Part 2: https://search-guard.com/blog/encryption-at-rest-real-world-use-cases-and-industry-applications/

Part 3 · Compliance and Future-Ready Security

Part 3 ties the series to compliance and to where security is heading.

On compliance, it maps encryption at rest to the standards teams get audited against: PCI-DSS for cardholder data, GDPR (where encryption is explicitly recommended, and properly encrypted data may in some cases fall outside the definition of personal data, reducing reporting obligations), SOX for financial reporting integrity, and ISO 27001. On the economics, GDPR fines can reach 4% of global annual turnover while encryption costs a small fraction of an IT budget, and organisations with mature encryption programs often see smoother audits and lower cyber-insurance premiums.

On what is coming, it covers cloud and hybrid environments and the shared-responsibility model (where customer-managed encryption keys are becoming best practice), ransomware and how encryption cuts an attacker's leverage in double-extortion attacks, rising regulatory scrutiny, IoT and edge devices, zero-trust architecture with identity-based encryption, and the automation of key management and compliance reporting. It closes on a clear point: encryption at rest is a strategic pillar for compliance, resilience, and trust, not only a technical safeguard.

Read Part 3: https://search-guard.com/blog/encryption-at-rest-compliance-and-future-ready-security/

Frequently asked questions

What is encryption at rest?
Encryption at rest is the practice of encrypting data while it is stored, on a disk, database, file server, or in cloud storage, so that anyone who reaches the storage layer cannot read the data without the decryption keys.

How is encryption at rest different from encryption in transit?
Encryption in transit protects data as it moves across the network. Encryption at rest protects data once it has been written to storage. You need both. In transit covers the easier half; at rest covers the half that auditors and attackers both care about.

Which compliance frameworks does encryption at rest support?
It supports requirements across PCI-DSS, GDPR, SOX, and ISO 27001, among others. GDPR in particular explicitly recommends encryption as a technical measure for protecting personal data.

Can encryption reduce GDPR reporting obligations?
In some cases, yes. Under GDPR, properly encrypted data may not be treated as personal data, which can reduce reporting obligations and regulatory impact after an incident. The specifics depend on the situation, so treat this as a strong reason to encrypt, not a blanket exemption.

Which encryption standard is used?
AES-256 is the industry default across regulated sectors and the standard reference point for encryption at rest. The harder question is key management, not the algorithm.

Who should manage the encryption keys?
Customer-managed encryption keys are a best practice, especially across multiple cloud providers, so you keep control over who can access your data even when it sits on third-party infrastructure. Secure key management is what separates "encrypted" from "only you can read it".

Does encryption at rest help against ransomware?
It reduces the damage. Modern ransomware often combines encryption with data theft and extortion. If your data is already encrypted before an attacker reaches it and they do not have the keys, its value drops sharply, which cuts their leverage.

Is encryption at rest worth the cost?
IBM's 2024 Cost of a Data Breach Report put the global average breach at $4.88 million. Encryption typically costs a small fraction of an IT budget, encrypted breaches tend to cost less, and encrypted environments can often stay operational during an investigation. Weigh the cost of encryption against the cost of a breach or a failed audit.

Ready to see it on your cluster?

If encryption at rest is on your roadmap this year, the fastest way to see how Search Guard handles it is a short walkthrough on your own setup.

Book a 20-min Encryption at Rest demo: [CALENDLY-URL]

This article was published on the Search Guard blog: https://search-guard.com/blog/encryption-at-rest-series/
Search Guard is Security and Alerting for Elasticsearch and Kibana — search-guard.com · Start a free trial