elastic

Leveraging Elastic to power your data security compliance

Executive summary

As the cybersecurity threat landscape grows increasingly sophisticated — with cyber attacks becoming more frequent, targeted, stealthy, and technically advanced — the imperative for robust and comprehensive data security has never been more critical. The legal requirements and potential liabilities related to cybersecurity are likewise becoming more complex and demanding, making a risk-based approach to security an absolute necessity.

To keep up with the ever-expanding list of security-related regulatory requirements, prevent potentially devastating business disruptions and guard against the risk of costly lawsuits from security breaches, companies should adopt a holistic, strategic approach to cybersecurity. Failure to do so not only exposes businesses to significant legal and financial consequences, but also irreparable operational and reputational harm.

This white paper explores how organizations can use Elastic to meet their security obligations and build a truly resilient defense against cyber threats. Elastic's powerful, flexible, and scalable solution helps enterprises to meet varied, multifaceted compliance and operational cybersecurity needs, including:

- Increased visibility and searchability of data across attack surfaces
- Simplified data pulls for compliance requests
- Streamlined detection and automation to remediate threats
- Monitoring and demonstration of your security posture
- Enriched threat intelligence

Below, we provide an overview of foundational security concepts that are common across legal frameworks; review the potential consequences of failing to implement these concepts in a risk-based, compliant manner; and illustrate how organizations can use Elastic's platform and solutions to help meet compliance obligations and mitigate security risks.

Please note: *This white paper is provided for informational purposes only and is not intended to constitute legal advice. Please consult your legal counsel for legal advice.*

Foundational security principles and related compliance obligations

The modern security compliance landscape consists of a patchwork of jurisdiction-specific, industry-specific, and data-specific requirements. Organizations' responsibilities will therefore differ depending on where they are located, where they do business, what data they process and how, including the sensitivity of that data and the nature of that business.

For instance, a global financial institution could be simultaneously subject to the US federal Gramm-Leach-Bliley Act ("GLBA"), the New York Department of Financial Services ("NYDFS") Cybersecurity Regulation, the EU Digital Operations Resiliency Act ("DORA"), and the EU Network and Information Security Directive 2 ("NIS2 Directive"), among other laws.

A publicly traded, US-based retailer, on the other hand, might be subject to a different array of requirements, such as the PCI Data Security Standards ("PCI-DSS") for payment card security, Sarbanes-Oxley ("SOX") requirements for the security of financial reporting systems, and US state breach notification laws. Without of course forgetting privacy laws and their information security requirements for the protection of personal information.

On top of these mandatory requirements, many companies also maintain voluntary certifications to a variety of different third-party security frameworks, such as ISO 27001, SOC 2, NIST CSF, or the UK Cyber Essentials.

Despite these differences, statutory, regulatory, self-regulatory, and industry frameworks — as well as general security best practices — largely converge around a core set of security principles. Below, we review the key parts of these principles and provide examples of how they align with various frameworks.

Data inventory, mapping, and classification

Organizations cannot deploy risk-based security controls without first understanding what data they have (a process known as data inventory), where it resides (data mapping), and the sensitive nature of that data (data classification).

These processes are also critical in the event of a data breach incident so that companies can better understand whether impacted data will trigger statutory, regulatory, or contractual breach notification obligations. For these reasons, data inventory, mapping, and classification are either explicitly required by, or a necessary prerequisite to, complying with multiple frameworks. For example:

- The *FTC Safeguards Rule* (16 CFR § 314), which implements requirements for certain financial institutions subject to the GLBA, requires covered financial institutions to identify and assess the sensitivity of customer information as part of their risk assessment process.
- The *HIPAA Security Rule* (45 CFR § 164.308) similarly obligates covered entities to inventory and protect electronic protected health information ("ePHI").
- Under Article 30 of the EU General Data Protection Regulation ("GDPR"), organizations must maintain a record of processing activities, effectively requiring a data inventory and mapping to demonstrate compliance.
- Each US state's breach notification obligations are typically triggered only if certain types of sensitive personal data relating to residents of that state are compromised. Accordingly, in a data breach scenario, companies must be able to determine what categories of data are included in a compromised dataset.
- Frameworks like NIST SP 800-53 and the CIS Controls emphasize data classification to ensure that protections are aligned with the sensitivity of the data. By establishing a clear inventory and classification scheme, companies can more confidently implement access controls, monitor sensitive data flows, meet regulatory obligations, and reduce the risk of unauthorized disclosure.

Role-based access controls

Role-based access controls ("RBAC") are measures designed to ensure that individuals have access only to the systems and data that they need in order to perform their responsibilities (a concept also known as "least privilege"). Consistently applied RBACs reduce the risk of unauthorized access by malicious insiders and can help to limit the scope of an intrusion. Many legal and industry frameworks explicitly require or strongly recommend RBAC:

- Under the EU GDPR, only duly authorized persons with a need-to-know may access personal data. Going even further, the regulation defines unauthorized access as a case of data breach.
- Massachusetts' Standards for the Protection of Personal Information, 201 CMR 17.04, requires companies that do business in Massachusetts to implement secure access control measures that restrict access to records and files containing sensitive personal information to those who need such information to perform their job duties.
- The HIPAA Security Rule mandates that access to ePHI be limited to those with a legitimate need to know.
- Article 9(4) of the EU's DORA requires covered financial institutions to implement policies that limit the physical or logical access to assets to what is required for legitimate and approved functions and activities only.
- Industry standards like NIST SP 800-53, ISO/IEC 27001, and the CIS Controls (e.g., CIS Control 6) also emphasize RBAC as a foundational access management practice.

Logging and monitoring

Security event logs are among the most important resources that companies have to detect security incidents. Logs reflecting information such as dates and times of access, actions performed, and the user who performed those actions are essential for verifying whether system access was authorized and investigating potential unauthorized activity. Monitoring logs in real time or near real time is also key to detecting and addressing threats on a timely basis.

Log management can be a challenge, though, for organizations with complex, diverse systems that can generate large volumes of logs every day. Such organizations must rely on technical solutions to effectively aggregate logs and monitor them for anomalous activity. Legal and industry frameworks emphasize the importance of logging and monitoring:

- The Payment Card Industry Data Security Standard (PCI-DSS) requires all companies that store, transmit, or process payment card data to log and monitor all access to system components and cardholder data.
- The HIPAA Security Rule mandates audit controls to record and examine activity in systems containing ePHI.
- SOX Section 404 requires management and auditors to assess and report on the effectiveness of public companies' internal controls over financial reporting. Such auditors evaluate those controls against frameworks such as COBIT, which require audit logging of user activity, access to financial systems, and changes to financial data.
- The "Detect" component of the NIST CSF specifies that companies should log security events and maintain continuous security monitoring, which is also indispensable for the timely reporting of incidents notifiable under, for instance, EU GDPR Article 32, EU NIS2 Article 23, or EU DORA Article 19.

Intrusion detection and response

It is an unfortunate fact that in today's threat landscape, every organization is a potential target for cyber attack. Organizations must maintain intrusion detection systems and processes for responding to security incidents in the inevitable event of an attempted intrusion. Such systems are critical to allow companies to quickly identify and respond to an attack before it escalates into a serious incident. However, intrusion detection systems and incident response processes are rarely effective out of the box; rather, companies must establish a baseline of activity and tailor alerting criteria to the company's unique attributes. This tailoring increases the accuracy of alerts and helps to ensure that incidents are appropriately triaged and addressed in accordance with their criticality. Intrusion detection and response is central to numerous legal and industry frameworks:

- US federal, state, and international breach notification laws require data breaches to be reported within specific timeframes. While it is often thought that the GDPR imposes the shortest timeframe for reporting (within 72 hours of determining that a reportable data breach has occurred), it is worth noting that DORA requires major Information and Communication Technology ("ICT")-related incidents to be reported within four hours of discovery.
- The NYDFS Cybersecurity Regulation Section 500.16 requires regulated entities to have incident response plans to promptly respond to, and recover from, cybersecurity incidents.
- DORA also requires regulated financial institutions to develop detailed incident response plans.
- The NIST CSF specifies that companies maintain detailed "Detect" and "Respond" controls to detect and respond to security incidents.

The cost of non-compliance

Failing to implement compliant and effective security controls can expose companies, their leadership, and their boards of directors to significant legal, financial, and reputational risks. From a practical standpoint, organizations with ineffective monitoring tools or processes risk prolonged unauthorized access, which can allow an attacker to conduct reconnaissance on a company and to more closely mimic authorized activity, all while leaking data or setting the groundwork for a ransomware attack. Incomplete logging can also make it impossible to determine whether suspicious or unexpected activity was authorized, which can lead to both over-and under-notification.

In the event of a data breach or cybersecurity incident, inadequate data mapping and inventory can lead to difficulties in identifying impacted data. This can result in delays in notifying impacted parties and regulators. Such delays, in turn, increase the potential damage suffered by victims, violate regulatory reporting timelines, and compound the immediate burden of recovery and remediation with additional damages claims, regulatory sanctions, and further enforcement and litigation costs. For business-to-business vendors, it can also make it harder to identify which customers were impacted by an incident.

Failure to comply with affirmative security requirements such as those imposed by privacy laws to protect personal information can result in substantial penalties, fines, and other legal liability. All businesses also face the risk of negligence, breach of contract, or other lawsuits (often in class actions) from plaintiffs whose information was breached in an incident. Notably, the California Consumer Privacy Act (CCPA) establishes a private right of action for plaintiffs whose sensitive data was breached as a result of a company's failure to maintain "reasonable" security measures. Sanctions and damages under regulations like HIPAA, CCPA, or the EU GDPR may quickly fetch in the seven digits.

Beyond direct compliance penalties, reputational damage from poor security can also be severe. Companies that suffer a breach or fail to comply with security regulations may lose customer trust, face public backlash, experience significant business disruption, and suffer long-term impacts on their brand value. Publicly traded companies also run the risk of impact to share price in the wake of widely publicised security failures. Risks include customer churn and possible demands for compensation for failing to protect customer data adequately, leading to loss of business and revenue. In light of these significant consequences, companies should take security seriously by investing appropriately in compliance obligations and mitigating security risks.

Leveraging Elastic for compliance

The Elasticsearch Platform is the foundation for Elastic's two out-of-the-box solutions, Elastic Observability and Elastic Security. Organizations can use Elastic's open and flexible platform to meet their compliance obligations and address key cybersecurity risks across multiple channels. Most importantly, Elastic's solutions are inherently agile and scalable; they can be deployed on and collect data from a wide variety of systems and platforms, and their search capabilities can be leveraged for countless use cases. Below are just a few examples of how Elastic can be used to support core tenets of a security program:

Data mapping and classification

Elastic can support data mapping efforts by indexing structured and unstructured data across environments, giving organizations centralized visibility into the types and locations of their data. Using custom tags, metadata, and machine learning, Elastic can help identify patterns in data (e.g., personal data, financial records, system logs), making it easier to classify data based on sensitivity or regulatory obligations. While Elastic is not a dedicated data classification engine, its powerful search and analytics capabilities can be integrated into broader data governance programs to help track and inventory data across cloud and on-prem systems.

Role-based access control (RBAC)

While Elastic is not an RBAC tool, the platform can ingest logs across an organization's systems to help identify gaps in permission management. Organizations can analyze access patterns to identify systems that user groups may or may not need access to and use that to inform assignment of access privileges. Elastic also helps our customers to ingest group access policies from across systems, enabling companies to generate reports from that data to demonstrate enforcement of access rights in audits or compliance investigations. And Elastic contains built-in RBAC features in its Elastic Security and Kibana interfaces. Admins can define roles that limit user access to specific indices, dashboards, or actions (like viewing versus editing), supporting least-privilege access principles.

Logging and monitoring

One of Elastic's core strengths, and most common use cases, is in aggregating, storing, and analyzing logs at scale. Using Elastic Agent, companies can ingest logs from endpoints, servers, cloud services, and applications. These logs are indexed in Elasticsearch, allowing for real-time analysis and visualization in Kibana. Elastic supports long-term log retention, alerting, and anomaly detection, making it an ideal log aggregation and security monitoring solution, as well as an effective compliance reporting tool. Its observability suite also provides application performance monitoring (APM), metrics, and uptime monitoring for holistic infrastructure visibility.

Many regulations, such as M-21-31 for US federal government agencies, require organizations to store logs for a set period of time. Elastic's data tiering structure enables data to be stored cost-effectively based on how often and quickly it needs to be accessed and used. Elasticsearch logsdb index mode **reduces the storage footprint of log data by up to 65%**, increasing visibility and compliance while keeping all data immediately accessible for analysis.

To cite just one example, the University of York transitioned its security information and event management (SIEM) system to Elastic Security to enhance cybersecurity capabilities, improve operational efficiency, and reduce costs. By deploying approximately 9,000 Elastic agents across servers, desktops, and laptops and collecting logs from across the university's hybrid cloud infrastructure, including Google Cloud, AWS, Azure, and on-premises servers, the University ingests 500 gigabytes of data per day, with 35 terabytes of logs in storage. It also connects with security tools like Palo Alto Networks firewalls, Cloudflare, and Duo, ensuring comprehensive monitoring across various platforms. This setup enables swift searches across vast amounts of data, reducing query times from hours to seconds.

Intrusion detection and response

Elastic Security includes endpoint detection and response (EDR) capabilities and integrates threat intelligence feeds to support intrusion detection. It enables security teams to monitor for known and unknown threats using behavioral analytics, attack mapping, and custom detection rules. With centralized logging, analysts can rapidly correlate events across systems, investigate alerts in context, and orchestrate response workflows. Elastic also supports automated responses through integrations with third-party security orchestration, automation, and response (SOAR) platforms, making it a powerful tool for improving incident response readiness and threat hunting. These advanced capabilities reduce the likelihood of a breach and speed response time in the event of a successful intrusion, which in turn mitigate potential legal liabilities associated with an incident.

AHEAD, a leading digital platform and transformation provider, significantly enhanced its intrusion detection and response capabilities by integrating Elastic Security into its managed security services. AHEAD now ingests client security data into Elastic running on Elastic Cloud where the data is enriched, aggregated, and connected to threat intelligence feeds. Elastic is also the data source for the organization's SOAR system. AHEAD security analysts can also leverage AI-driven alarms that highlight relevant information within security events, reducing the time needed to manually sift through vast amounts of data and helping to reduce the burden of false positives.

Conclusion

As the cybersecurity threat landscape continues to pose sophisticated challenges for organizations, complying with the ever-expanding list of security and data privacy-related regulatory requirements and reducing risk also becomes more complex. Failure to do so not only exposes businesses to significant legal and financial consequences, but also operational and reputational harm. Elastic can help CIOs and CISOs enhance their organizations' compliance with these various legal requirements, especially in the areas of data mapping and classification, RBAC, logging and monitoring, and intrusion detection and response.

