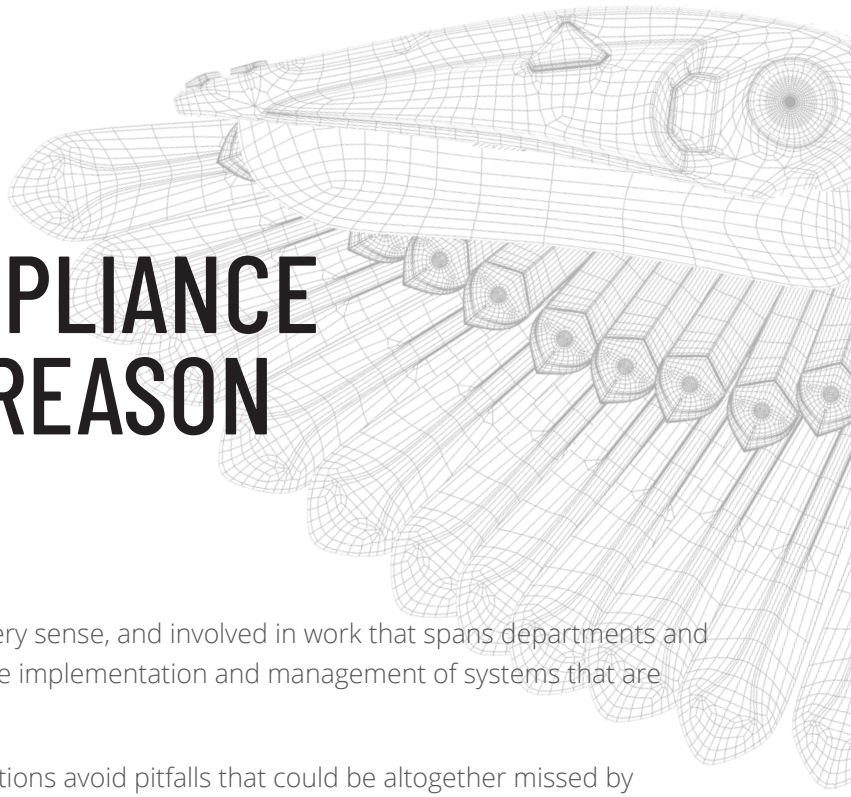
cybereason



ADDRESSING COMPLIANCE GAPS WITH CYBEREASON TECHNOLOGY

Information security teams are cross-functional in every sense, and involved in work that spans departments and functions. Security leaders are a key component in the implementation and management of systems that are compliant and communicate in compliant ways.

Adherence to compliance frameworks helps organizations avoid pitfalls that could be altogether missed by bringing more structure and proven practices into the security program. Compliance mandates often exist for a reason, and will lead to better hygiene which helps to ultimately avoid breaches and their undesirable impact to business continuity.

At times, the penalties for non-compliance can be more severe and costly than a breach or other security incident itself. British Airways was initially handed an eye popping **£183.39 million** fine for the failure to disclose a security incident to the ICO in 2018 as required under GDPR. The fine was later reduced to £20 million, still an impressively high number, and a warning to organizations in the future who intentionally fail to disclose events that meet the GDPR threshold for reporting.

Fulfilling Compliance Requirements with Cybereason

Address compliance needs dictated by mandates like GDPR, PCI-DSS, FINRA and others with compensating controls

Regulatory compliance often intersects with responsibilities of the Information Security team.

Some examples:

- **GDPR (General Data Protection Regulation) Article 33**

  Notification of a personal data breach to the supervisory authority

  "In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority"

  Information Security teams are ideally tasked with preventing a breach, but defenses aren't always bulletproof against targeted attacks and sophisticated operations. When a breach does occur, teams are responsible for quickly becoming aware of the situation, disclosing the details to relevant regulators and authorities, and then taking action to respond and recover.

  How Cybereason Enables GDPR Compliance: To maintain compliance with GDPR, time is of the essence. Cybereason enables you to understand the full scope of an attack with minimal-to-no manual investigation, enabling you to contain an attack, resolve it - and when necessary - report the incident as quickly as possible.

- **PCI-DSS (Payment Card Industry Data Security Standard)**

  PCI-DSS dictates that organizations protect stored cardholder data, use and regularly update antivirus software, maintain secure systems and monitor network data.

  How Cybereason Enables PCI-DSS Compliance: Multi-layered and fileless prevention capabilities available with Cybereason provides Defenders a wide array of protection that reduces the volume of threats that bypass less-capable defenses, which frees up more time to detect, investigate and remediate. Cybereason prevents zero-day threats by detecting malicious operations early based on suspicious chains of behavior followed by automated responses to end cyber attacks before they can become serious breach events.

- **FINRA (Financial Industry Regulatory Authority)**

  FINRA is a private regulatory body that helps to ensure the integrity of the financial system, and operates under the supervision of the SEC. FINRA works to enforce rules relevant to the financial sector and audits firms for compliance, at times levying penalties or other recommendations for non-compliance.

  FINRA calls specifically for security teams to perform asset inventory and risk assessments of a given environment, and work to protect against malware infections.

  How Cybereason Enables FINRA Compliance: Assess risk across the enterprise via cyber posture assessments to create a clean-slate environment that is simple to maintain on an ongoing basis, and identifies gaps in coverage and any embedded vulnerabilities. The cybereason Defense Platform comprehensively detects and definitively remediates threats, setting up a security posture that prevents malware infections.

Cybereason technology fulfils environment sweep requirements and allows Defenders to answer relevant questions, like:

- What was the scope, timeline and root cause of the attack?
- Which users, machines and systems were impacted?
- What was the context of the threat and any relevant tactics, techniques and procedures that were used?

Understand the environment - both past and present - with sweeps and IOC scanning. A commonality between several compliance mandates is the requirement to audit for occurrences of specific threats that are live or have occurred in the last 12 months in a given environment. This auditable trail creates a cache that can be recalled as needed in the event of an unforeseen breach or incident.

The data retention period available with Cybereason is industry-leading, and includes options for retention of enterprise data in periods of months or years. This data cache is incredibly useful to surface subtle threats over a protracted period of time, and produces an auditable log of environment activity to ensure compliance. Defenders should be cautious of solutions that require data filtering from the endpoint, as this reduces visibility and leads to gaps in coverage.

Data localization standards are a new commonality across multiple compliance mandates. Organizations are required to adhere to data privacy and data sovereignty protections that are specific to certain regions. For example, under GDPR, all data collected from citizens of the European Union must be stored in the EU and under the jurisdiction of EU regulators. From a technology perspective, vendors must account for this and operate with data centers that keep data in-region.

Cybereason technology separates the UI from the storage and collection of endpoint data. This means that Defenders can deploy detection servers in-region to maintain compliance to data localization requirements and simultaneously deploy aggressive prevention, detection and response capabilities.

Adhere to and enforce compliance mandates relevant to information security with Cybereason

Implement best-in-class threat prevention to protect data and assets

Validate technology and performance

Retain data without limits for threat hunting and environment sweeps

Streamline operations and response automation

Correlate detections that tie the wholeattack story together

Regulatory Compliance vs. Compliance to Security Best Practices

Compliance to certain industry-standard and proven frameworks is a wise decision, even without the looming threat of regulators that levy penalties for noncompliance.

MITRE ATT&CK

MITRE Engenuity has developed a knowledge base known as MITRE ATT&CK (adversarial tactics, techniques and common knowledge) that catalogs advanced attacker behaviors into an easily digestible framework. Mapping detection and response efforts to the MITRE ATT&CK framework is not mandatory, but makes an organization better able to identify sophisticated attacker operations early in the process and take decisive action to avoid a data breach altogether. Security teams looking to uplevel their abilities should consider adoption of MITRE ATT&CK in their processes.

Cybereason delivered front-runner results in the most recent MITRE ATT&CK evaluations, where vendors were tested for their detection effectiveness against the key behaviors identified in the framework. Notable results from the evaluation include 100% detection and prevention of Linux-based attacks - meaning Defenders using Cybereason technology can reliably prevent and comprehensively detect based on MITRE ATT&CK, even on nonstandard systems and in cloud configurations.

NIST Framework (National Institute of Standards and Technology)

The NIST Cybersecurity framework is a well-known and voluntary framework that helps to institute basic security practices. Cybereason provides technological capabilities that align to NIST and support critical functions prescribed by NIST, including:

IDENTIFY
Inventory assets and ensure visibility and coverage across the enterprises. Shore up vulnerabilities with personal firewall controls and vulnerability assessment.

PROTECT
Aggressively prevent threats and malicious behaviors that are indicative of adversaries, including zero-day threats based on indicators of behavior.

DETECT
Sophisticated adversaries operate subtly. Discover and investigate suspicious attacker activity in a correlated view that deconstructs the malicious operation.

RESPOND
Remediate impacted systems, isolate endpoints to contain lateral spread, and kill malicious processes. Reset impacted registry keys and remediate memory-based attacks.

RECOVER
Restore trust to impacted systems and return to a state of business continuity. Avoid the recurrence of partially resolved threats with better endpoint hardening, threat intelligence, new policies and prevention fed by previous detections.