

The Infrastructure Security Paradox: Breaking SIEM Trade-offs

When ransomware took down [Colonial Pipeline in 2021](#), and then JBS just weeks later, cybersecurity officially became a national security issue. These weren't just isolated corporate IT events. They disrupted fuel distribution and food supply chains across the U.S., spotlighting just how vulnerable critical infrastructure had become.

Three years later, that threat hasn't faded, it's only grown. [FBI data](#) shows that ransomware attacks targeting critical infrastructure rose another 9% in 2024. Nearly half of all complaints involved industries like manufacturing, healthcare, finance, government, and IT.

Now, the policy response is catching up faster than many organizations are prepared to handle.

From Guidelines to Mandates

Within days of the Colonial Pipeline breach, the White House issued Executive Order 14028, initially drafted in response to [SolarWinds](#). Since then, the federal government has only intensified its stance. In early 2024, the [Transportation Security Administration](#) issued a Notice of Proposed Rulemaking requiring mandatory cyber risk reporting and controls for surface transportation operators.

The era of optional security best practices is ending. But here's the problem: even well-intentioned teams are struggling to meet these new standards, not because they lack effort, but because their tools lock them into false choices.



The Trap: SIEM Trade-Offs That Don't Scale

SOC teams today are being forced into trade-offs that weaken both compliance and defense.

Take log retention. New mandates require long-term data availability for forensics, but traditional SIEMs still use volume-based licensing. That means many organizations cut “non-essential” logs to stay under budget, only to find out too late that DNS data or Proxy Logs held the clues they needed to trace an incident.

Detection adds another layer of complexity. Regulations call for continuous monitoring, but more detections mean more alerts. To stay sane, teams disable rules, creating the very blind spots those mandates were meant to prevent. When it comes to response, security leaders are forced to choose between rigid SOAR workflows that break under pressure or AI copilots that act without context or consistency.

One [\\$30 billion energy company](#) faced this exact dilemma. Their legacy tools couldn't deliver the speed or flexibility needed for mission-critical infrastructure while meeting evolving compliance demands. They needed full retention and full control without volume-based cost penalties. They got there by rethinking how they handled data ownership and the alignment of data to analytics to meet their use cases.



Moving Past the False Choices

The organizations staying ahead aren't just upgrading tools, they're rejecting the trade-offs.

Instead of choosing between log volume and cost, they're splitting the workload. Critical logs go to fast-access hot storage, while everything else is routed to cost-efficient data lakes, retaining full visibility without breaking the budget.

They're also rethinking how they detect threats. [One telecoms provider](#), for example, built custom detection logic by correlating API activity and login events across systems. Rather than chasing isolated alerts, they mapped behavioral chains that reflected actual adversary tactics, boosting alert fidelity and tying signals together based on risk.

Platforms like Graylog are helping teams do this with automated campaign detection and data lake routing. Instead of tuning down detection rules to reduce noise, which [59% of SOC teams admit to doing](#), these organizations scale detection based on use cases, not license tiers.

The Infrastructure Reality Check

This challenge isn't limited to massive enterprises. A Canadian construction firm needed full visibility across dozens of distributed sites, mobile devices, and hybrid cloud systems — without blowing up the budget or requiring vendor-specific deployments.

Their solution was a flexible hybrid architecture that unified logging and detection across environments. Structured workflows guide their incident response, while contextual AI surfaced relevant actions without the unpredictability of black-box automation.

They didn't compromise between structured procedures and usability. And they didn't have to.

A SIEM Without Compromise

The security landscape is evolving. And traditional SIEMs, built around trade-offs, aren't keeping up. They force teams to choose between:

- Visibility and cost
- Detection and alert fatigue
- Automation and adaptability
- The teams thriving under pressure aren't necessarily the biggest or most resourced. They're the ones rejecting those limitations.

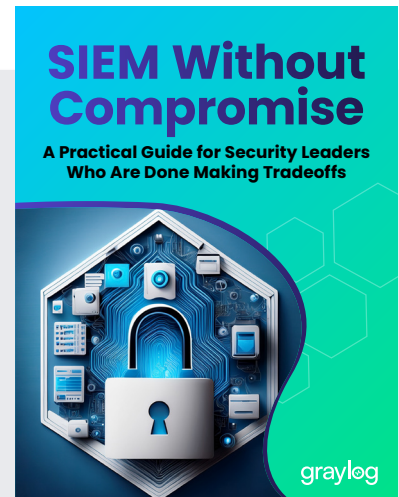
They're operating a SIEM aligned with how real data flows and SecOps teams work:

- Smart log routing that preserves data access without runaway costs
- Automatically corroborating evidence for accuracy, not disparate alert noise
- Workflows that are structured, adaptable, and backed by explainable AI

The technology exists. The mandate clock is ticking. And the next attack isn't waiting.

Looking for guidance on how to get started? Read: ["SIEM Without Compromise — A Practical Guide for Security Leaders Who are Done Making Tradeoffs"](#)

Learn more about [Graylog Security](#) >



ABOUT GRAYLOG

Graylog delivers a SIEM that works the way teams actually need: full visibility, real detection, and faster investigations—without blowing the budget. Trusted by 50,000+ organizations worldwide, Graylog helps analysts skip the noise and get to what matters. Automate the heavy lifting. Stay focused on real threats. Learn more at graylog.com.