# SIEM Without Compromise

## A Practical Guide for Security Leaders Who Are Done Making Tradeoffs

graylog

# Security, Without the Strings

Security leaders operate under pressure. You need full visibility, consistent performance, and team trust while managing cost and complexity. Most SIEMs just add more weight.

Licensing models punish growth. Detections flood your team with noise. Response workflows feel either locked down or all over the place. Over time, your platform ends up driving strategy more than the threats do. These issues slow more than technology. They impact how your team works, how fast you move, and how much risk you carry. But here's the shift: the old tradeoffs are no longer necessary.

This guide breaks down the friction points legacy SIEMs create, and what forward-thinking teams can (and should) expect from a platform that keeps up.

# The Trade-Offs That Shouldn't Exist

## 1. Ingest Limits That Undercut Strategy

### The challenge:

Send only what your budget can handle, or drop valuable logs and lose context. That choice is a risk multiplier. When you cap visibility, incident response and audit readiness take the hit. For many teams, retention has become a financial negotiation, not a security priority.

By 2026, 80% of SIEM buyers will prioritize flexible ingest over feature parity. The market is shifting toward models that remove constraints, not reinforce them.

### What to expect instead:

**Modern SIEMs let you:**

- Send priority logs to fast storage for real time search
- Store everything else in cost-free data lakes
- Preview archived logs without having to fully reload them

### The result:

Your visibility should scale with your environment, not with your license key.

## 2. Detection or Fatigue

### The challenge:

More detections mean more alerts. More alerts mean burnout. Teams are stuck choosing between catching threats or keeping their heads above water.

In a recent study, 59% of SOC teams admitted they had disabled detection rules just to reduce alert volume, even knowing the risk that comes with it. This is not just about false positives. The real issue is disconnected detection logic that cannot correlate across signals.

### What to expect instead:

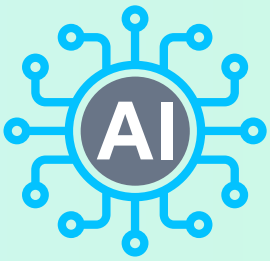
**Detection engines that:**

- Connect alerts across time, assets, and tactics
- Score threats with business and vulnerability context
- Detect long dwell time threats by matching past activity to current signals

### The result:

Less alert fatigue. More true positives. And a team that can focus on what matters.

## 3. Rigid Playbooks or AI That Cannot Be Trusted




### The challenge:

Static workflows slow response. Generative AI offers speed but no accountability. Neither one gives analysts the support they need in real time. The average analyst loses 30 to 45 minutes per incident switching between tools, digging for evidence, and retyping notes.

That delay is not just inefficient, it is dangerous.

### What to expect instead:

- Built in guidance that follows live investigations
- AI that summarizes and explains rather than guessing or hallucinating
- Structured evidence capture that speeds up audits and reduces rework

### The result:

Response workflows that flex with the situation. Not ones that leave your analysts scrambling.

# Scaling Without Losing Control

### Performance That Keeps Up

Search should stay fast and accurate as your data grows. Whether logs are old or fresh, you should be able to search them together without delay or workarounds.

### Deploy Where It Works

Cloud is not always the best option. Some teams need hybrid or on premises deployments due to regulatory, operational, or security requirements. Your platform should support that without forcing tradeoffs.

### Connect All Signals

By 2025, 50% of security incidents will involve assets outside traditional IT—across APIs, SaaS, OT, and cloud-native environments. A modern SIEM needs to normalize and correlate that entire surface.

### What to expect

- Ingest normalization across sources and formats
- Real time correlation that connects signals from across your stack
- One view that shows your full threat story, not just pieces of it

# What “Without Compromise” Really Means

You should not have to choose between visibility and cost, speed and accuracy, automation and control.

## Expect a platform that lets you:

- ✓ Ingest all your data without financial penalties
- ✓ Detect faster without sacrificing clarity
- ✓ Respond in the same platform where detection happens
- ✓ Search old and new logs in the same interface
- ✓ Scale across environments without breaking workflows
- ✓ Deploy based on your needs, not your vendor’s preference
- ✓ Operate the system without hiring a build team

This is not a stretch goal. This is the new normal.

# Signs Your SIEM Is Holding You Back

You may be overdue for a change if any of these feel familiar:

- Logs get dropped just to avoid ingest limits
- Analysts mute alerts to keep from falling behind
- Response processes are stitched together across tools
- You spend more time managing licenses than improving detection
- You are not sure whether your SIEM helps or just hangs on

In 2024, 63% of security leaders reported actively reassessing their SIEM investments, with most citing misalignment between platform capabilities and how their teams actually work. The shift is clear: organizations are moving toward systems that reduce operational drag, not add to it.

# Where You Go From Here

Legacy SIEMs made you choose between visibility, speed, and control. That era is over.

## Graylog delivers:

- ✓ Unlimited data access — without ingest penalties
- ✓ Context-rich detections — not alert overload
- ✓ Streamlined response — no tool-hopping, no delays

# Why Graylog Wins

| What Matters | Graylog | Most SIEMs |
|---|---|---|
| **Proof of Concept** | ✓ Live in hours | X Weeks or more |
| **Pricing** | ✓ Transparent, predictable | X Hidden costs, ingest caps |
| **Ease of Use** | ✓ No SIEM team required | X Complex, resource-heavy |

## ABOUT GRAYLOG

Graylog is the no-nonsense SIEM that cuts through noise and complexity. It delivers what security teams need most: full visibility, faster investigations, and smarter detection—without trade-offs or surprise costs. From automated workflows to correlation and anomaly detection, Graylog helps analysts move faster and stay focused. With a product suite spanning Graylog Enterprise, Security, API Security, and Open, we support everyone from large enterprises to lean teams. Trusted by over 60,000 organizations around the world. Learn more at graylog.com or connect with us on Bluesky and LinkedIn.

www.graylog.org
info@graylog.com