ANOMALI

Infographic

10 WAYS TO CUT SECURITY SPEND

If you haven't actualized the Agentic SOC yet, here's what the delay is costing you.

Only **32%** of organizations use security AI and automation extensively, per IBM's 2025 Cost of a Data Breach report. What holds them back is fragmentation: data trapped in silos, alerts no one can clear, and tools that were never built to talk to each other. None of it takes a rip-and-replace to fix. It takes a common data layer underneath the stack you already own.

1 KEEP EVERY TOOL

Unify what they produce. A large enterprise r**uns dozens of security tools, 45 on average**, by one cybersecurity report's count. What drains the budget is the analyst time spent stitching their output together by hand, plus the blind spots that open in the gaps between them. A shared data layer beneath the stack removes that integration tax, with no rip-and-replace and no new concentration risk.

2 STOP PAYING TO STORE NOISE

Deduplicate and strip low-value events at ingest, before they reach the SIEM. You stop paying ingest and long-term retention on data no analyst will ever act on.

3 SPLIT HOT STORAGE FROM COLD

Keep roughly 30 days hot in the SIEM and move long-term, searchable history to a lake. Full-fidelity retention stops carrying SIEM-tier pricing.

4 TAKE FALSE POSITIVES OFF ANALYSTS' DESKS

In the 2025 SANS Detection and Response Survey, **73% of teams named false positives** their top detection challenge, and **more than 60% encounter them frequently or very frequently**. Analyst hours are the largest recurring cost in most SOCs. Scoring and enrichment at ingest means fewer false positives reach a person.

5 END THE COST OF SPLIT DATA

IBM's 2025 report found **30% of breaches** involved data spread across multiple environments, at an average cost of $5.05 million. Silos cost you twice: on the breach itself, and on the analyst time spent pivoting between tools to reconstruct one event.

6 ENRICH ONCE, AT INGEST.

Fuse vetted intelligence into every event as it lands, instead of an analyst querying the threat intel platform case by case. Context arrives with the data, hours earlier than a manual lookup.

7 REDEPLOY TRIAGE HEADCOUNT INSTEAD OF HIRING

Organizations using AI and automation extensively contain breaches **80 days faster and pay $1.9 million less, yet only 32% do it**, according to IBM. Freed triage time becomes capacity you already pay for, redirected to hunting.

8 WRITE DETECTIONS ONCE

OCSF normalization gives you one schema across all telemetry. Write a detection a single time and it runs everywhere, with no rule rebuilds per source.

9 SHRINK DWELL TIME, SHRINK BREACH COST

Breaches that run past **200 days cost $5.01 million, against $3.87 million when caught sooner**. Attackers now break out in 29 minutes on average, and 27 seconds at the fastest, per CrowdStrike's 2026 Global Threat Report. Human-speed triage cannot close that gap.

10 PAY ONLY WHEN ANALYTICS RUN

Decoupled compute and storage means queries draw resources on demand. Between investigations, there is no always-on bill for warm infrastructure you are not using.

Anomali unifies telemetry, threat intelligence, and AI-powered judgment so security teams can act at machine speed.

Find out how to build the foundation for the agentic SOC and help drive down security spend while improving governance and security outcomes.

ANOMALI