# Platform Consolidation for ROI

This article is part of a series expanding on the themes explored in **Executive Brief: The Meditology 2026 Healthcare Security Outlook**. Each installment takes a deeper look at the strategic priorities shaping healthcare cybersecurity in 2026, drawn from executive interviews with CISOs and senior security leaders across the industry.

MEDITOLOGY SERVICES

## EXECUTIVE SUMMARY

- **Metric Shift:** Security performance shifts from number of tools deployed to level of integration, data consistency, and operational efficiency.
- **The Goal:** Moving from “Do we have the best tools?” to “Are our tools working together to reduce risk, cost, and response time?”
- **The Bottom Line:** Organizations that consolidate platforms reduce the complexity tax, improve visibility and response, and create the foundation for scalable operations and AI readiness.

Healthcare security teams are not short on tools. They are drowning in them.

Some organizations report managing as many as 76 separate security products,[1] each purchased at different times for different reasons. While the average enterprise typically runs 45 cybersecurity tools,[2] the result is rarely more security. Instead, we see a complexity tax with more integration gaps, analyst fatigue, and a fragmented view of risk.

In 2026, economic math caught up with this sprawl. Global cybersecurity spending has climbed to $240 billion, a 12.5 percent increase over 2025.[3] Healthcare organizations operating on razor-thin margins see diminishing returns from that investment. Budget growth is being consumed by the overhead of maintaining disconnected tools rather than by improving security outcomes.

# The Operational Liability of Tool Sprawl

Tool sprawl was cited across interviews as both a budget drain and an operational liability. The problem is not that individual tools are ineffective; it's that they do not naturally interoperate. Each tool identifies assets differently and captures data in its own format. Correlating this data requires manual effort and specialized expertise that most teams simply do not have the bandwidth to sustain.

As one security leader noted, when over half your security tools work by deploying independent sensors, you end up with half a million vulnerabilities that look alarming in aggregate, but no coherent narrative for the board.

The operational consequences compound quickly. Analysts toggle between consoles instead of investigating threats, leading to alert fatigue that erodes response quality and the team's capacity to triage. And when a critical incident occurs, the lack of a unified view slows the response at precisely the moment speed matters most.

> "The technology is only as effective as the team behind it."
>
> — David Finkelstein, St. Luke's University Health Network

# The Strategic Pivot: Best Integrated Over Best of Breed

In our executive interviews for the 2026 Healthcare Security Outlook, a clear shift emerged: the era of best of breed point solutions is giving way to a strategic push for best integrated.

The goal is not to reduce capabilities, but to reduce integration points. By gravitating toward platform solutions like ServiceNow, Microsoft's security ecosystem, or Epic-native tooling, organizations are creating a single system of record.

This unification eliminates duplicative interfaces and inconsistent security controls, normalizes data feeds so that a SIEM can produce better detections from integrated platforms than from 20 disconnected tools, and accelerates incident response by allowing workflows to operate within a single console.


The same logic applies to the GRC layer as well, where risk management and compliance programs should run on shared control libraries and single systems of record rather than parallel tool stacks and duplicate evidence collection. The consolidation argument is not about sacrificing capability. It is about making the capabilities you already have actually work together.

One CISO framed the challenge in business terms: healthcare security teams cannot continue to have a proliferation of tools and resources that they keep adding. The question is how to create more effectiveness and efficiency in the way the team operates, taking waste out of the system the same way the broader organization manages its margins.

# Proving ROI in the Language of the Board

**Consolidation is ultimately a financial conversation.**
Security has historically been perceived as a cost center, but Boards in 2026 are demanding reduced costs, minimized risk, and smarter resource allocation.

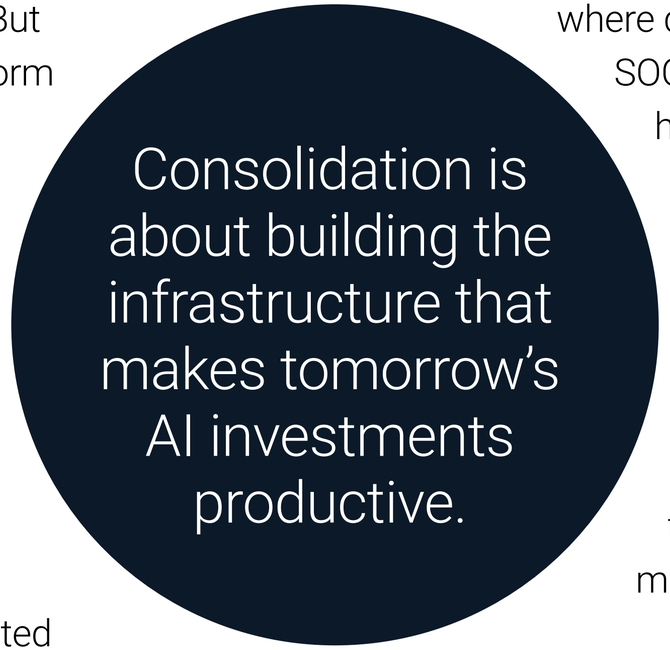
A request for a new security tool is viewed as an IT expenditure. However, a proposal to consolidate overlapping platforms reduces Mean Time to Detect (MTD) by 40% and frees staff from maintenance work is a business efficiency initiative. When you reduce 30 tools to 12, the savings are tangible, and the case for improved detection quality becomes a compelling ROI story.

# The Foundation for AI and Workforce Resilience

**Beyond immediate ROI, consolidation is a prerequisite for the next generation of security.**

The ROI case for consolidation is strong on its own. But there is a second, equally important dimension: platform consolidation creates the data normalization layer that is prerequisite to effective AI enablement.

As explored in Article 3 of this series, AI maturity in healthcare security sits at the top of a five-stage ladder that begins with standardized operational processes and structured data capture. Organizations that attempt to deploy AI-driven automation on top of fragmented, inconsistent data will get noise, not insight. The organizations moving fastest toward AI readiness are those that have invested in the foundational work of normalizing their security telemetry onto consolidated platforms.




This is not a theoretical connection. The area where AI is delivering the most measurable value today, security operations, is also the area where data is most commonly structured and normalized. SOC telemetry from an integrated platform produces the high-quality, consistent input that AI models require. By contrast, AI applied to fragmented data from 20 disconnected tools produces unreliable outputs that analysts learn to ignore, undermining the very efficiency gains the technology was meant to deliver.

Consolidation, in other words, is not just about today's ROI. It is about building the infrastructure that makes tomorrow's AI investments productive.

# Relieving Constrained Teams

**Security staffing remains deeply constrained across healthcare.** Small GRC teams support massive, complex ecosystems. Specialized roles in TPRM, cloud security, and medical device security are particularly difficult to fill, and the broader cybersecurity talent shortage shows no signs of easing. Reducing the number of tools directly reduces the operational burden on stretched staff. It is the difference between asking five analysts to manage 40 consoles versus 15; the same people, but with more time to think, investigate, and respond.

This workforce reality reinforces every other strategic theme in the Outlook report. Platform consolidation reduces tool management overhead. Co-managed TPRM models extend vendor assessment capacity. AI augmentation accelerates triage. And operational discipline, through standardized processes, structured data, and evidence reuse, reduces the manual effort that burns out the professionals who remain. The organizations that acknowledge the talent constraint as structural rather than temporary are making better investment decisions.

# From Sprawl to Strategy

Platform consolidation is not just a migration project; It's a strategic reorientation. The organizations that get this right will not just spend less on security; they will get more from every dollar they spend.

**Take the Next Step**

The "Complexity Tax" is a choice. You can continue to manage sprawl, or you can begin the transition to a high-ROI, integrated security architecture.

- **Download the Full Report:** Explore all five themes of the 2026 Healthcare Security Outlook: The Shift to Operational Resilience.
- **Assess Your Stack:** Contact our advisory team for a Security Tooling Consolidation Assessment to identify overlapping costs and integration gaps in your current environment.

# About Meditology Services and this Research

Meditology Services is a healthcare-exclusive cybersecurity advisory firm. As the facilitator of this research and a trusted partner to hundreds of healthcare organizations nationwide, Meditology translates peer insights into actionable programs that accelerate security program maturity.

To execute on the strategic priorities outlined in this report, Meditology partners with healthcare organizations across critical areas:

### Operationalize Resilience & Third-Party Risk (TPRM)

Transition from reactive vendor assessment to proactive supply chain resilience through architectural risk reviews, continuous monitoring, and vendor integration into business continuity planning.

### Achieve Industry-Standard Certifications

Pursue HITRUST certifications and SOC 2 attestations to provide validated proof of security maturity to partners, patients, and regulators.

### Validate Security Through Continuous Technical Testing

Replace point-in-time assessments with continuous testing and ethical hacking to ensure controls remain effective against an evolving threat landscape.

### Establish AI & Emerging Technology Governance

Proactively manage the risks of AI adoption through AI risk program and governance frameworks that ensure innovation does not outpace security.

**This executive report is based on in-depth executive interviews conducted during January and February 2026** with CISOs and senior cybersecurity leaders representing multi-state integrated delivery networks, academic medical centers, regional and community health systems, health plans, and health technology companies.

Discussion areas included enterprise risk prioritization, budget strategy, vendor governance, security operations, regulatory readiness, and emerging technology risk. All findings are reinforced by Meditology's proprietary data derived from hundreds of healthcare cybersecurity engagements conducted annually.

**Participants included:**

- Gillian Lockwood, Director, Information Security, Mass General Brigham
- Matthew Webb, AVP, Cyber Risk Management, HCA
- Zishan Siddiqui, CISO, Sentara Health
- David Finklestein, CISO, St. Luke's University Health Network
- Raj Raju, CISO, Integra Connect
- Denis Tanguay, CIO, Sturdy Health
- Paul Curylo, CISO, Inova Health System
- Among others who requested anonymity.

All insights are presented in aggregate to reflect industry-wide themes rather than the position of any single organization.

# Citations


1 Palo Alto Networks, “5 Trends Shaping Healthcare Cybersecurity in 2025,” January 2025. https://www.paloaltonetworks.com/blog/2025/01/5-trends-shaping-healthcare-cybersecurity-in-2025/

2 Cycore, “Top 8 Cybersecurity Takeaways for 2025 and Trends for 2026,” December 2025. https://www.cycoresecure.com/blogs/cybersecurity-takeaways-2025-trends-2026

3 Gartner, Global Cybersecurity Spending Forecast 2026. Referenced in Elisity, “Cybersecurity Budget 2026: Benchmarks & Spending Trends,” March 2026. https://www.elisity.com/blog/2026-cybersecurity-budget-complete-enterprise-planning-guide

## About This Series

*This article is the fourth in a series of deep dives from the* **Executive Summary Brief: The Meditology 2026 Healthcare Security Outlook**. *Previous installments include Article 1: The Rise of Operational Resilience, Article 2: Third-Party Risk as Operational Accountability, and Article 3: AI Governance Before Enablement.*

MEDITOLOGY SERVICES

To access the full report or to speak with our team, visit **www.meditologyservices.com**.