kyndryl

Breaking the sprawl tax

The hidden cost of cybersecurity complexity

by Kris Lovejoy

Global Practice Leader, Cyber Resilience, Kyndryl

Key takeaways

Complexity has become the enemy of security. Years of reactive, best-of-breed buying has created fragmented architectures with weakened defenses and inflated costs.

Tool sprawl starves AI of the data it needs to work well. Disconnected systems produce messy, siloed information that blinds security teams and prevents AI from learning, correlating, and responding effectively – and potentially exposes attack surfaces.

The fix isn't another tool — it's consolidation. Simplifying around unified, intelligent platforms cuts cost and clutter, improves visibility and speed, and unlocks the full potential of AI-driven defense.

Introduction

Artificial intelligence is reshaping cybersecurity — used by attackers to find openings and by defenders to close them just as quickly.

But organizations racing to use AI to bolster their defenses are encountering a serious obstacle of their own making: a fragmented security architecture that often undermines rather than enhances their security posture.

This fragmentation didn't happen overnight. It's the result of years of reactive, best-of-breed buying, defensive patching against emerging threats, and decentralized decision-making across the enterprise — each logical in isolation, but together creating a complex, disconnected quagmire.

Over time, layer by layer, tool by tool, many enterprises assembled a patchwork of point solutions in pursuit of greater resilience. The result isn't a unified defense — it's an accidental architecture: sprawling, redundant, and increasingly unsustainable. This isn't just operational clutter; it's a crisis of complexity that imposes a costly "sprawl tax" on budgets, performance, and security itself. The shift to remote and mobile work only compounded the problem, with employees introducing new tools — so-called "shadow IT" — without approval and expanding the unseen edges of the IT estate.

This tangled web of overlapping, underused tools obscure visibility for security teams, and expands the very attack surface they were meant to protect. More critically, the complexity itself has become a barrier to adopting AI as a true defense strategy. To realize the full potential of AI-driven security, organizations must simplify — consolidating fragmented toolsets into a unified, intelligent architecture.

31%

of leaders report feeling completely ready to manage external business risks

22%

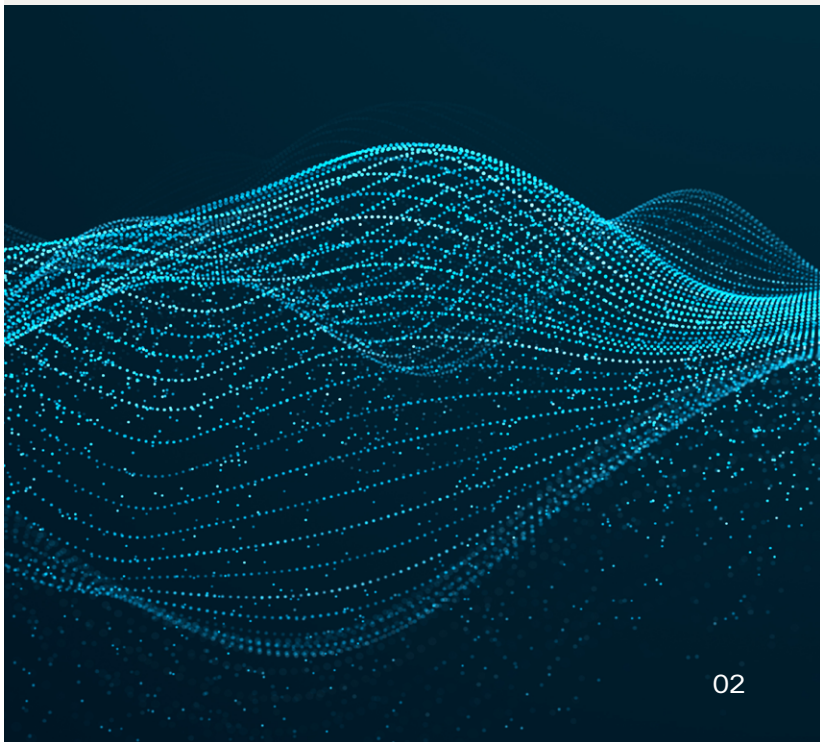
of leaders say technical debt holds them back from strategic initiatives

75%

of leaders investing in AI-powered cybersecurity solutions — more than any other AI capability

Source: Kyndryl Readiness Report, 2025

The path ahead isn't another tool — it's a rethink. Security teams need to move from scattered point products to a connected, intelligent platform that learns and adapts. Simplifying the stack doesn't just cut clutter; it drives clarity, unlocks the potential of AI, and gives organizations the resilience to stay ahead of what's next.



Data that can't connect

Security ecosystems are becoming increasingly complex. The issue, however, runs deeper than software. At its core, it's a problem of both product sprawl and data sprawl.

Product sprawl arises when organizations accumulate a growing number of tools and vendors — each with its own licensing agreements, support contracts, and communication channels. Managing this patchwork consumes valuable time and resources, creating administrative drag that undermines efficiency.

Data sprawl compounds the challenge. Every security tool produces its own alerts and telemetry, often in incompatible formats. Without strong integration, that information remains siloed, preventing security teams from seeing the complete picture. The result is fragmented visibility, inconsistent policy enforcement, and critical blind spots across the threat landscape.

How tool sprawl starves AI

The promise of AI in cybersecurity is immense, offering the ability to detect, withstand, and respond to threats at new speeds and scales. However, AI's effectiveness is entirely dependent on one critical resource: data. AI works best when it's trained on clean, connected data that helps it distinguish real attacks from harmless behavior.

Security tool sprawl creates the exact opposite of this ideal environment. It produces a collection of small, siloed, and inconsistent datasets — the equivalent of feeding an elite athlete a diet of junk food and expecting peak performance. This data fragmentation has several debilitating effects on AI initiatives.

Each tool generates information in isolation, leaving critical context trapped within its own silo. An AI model analyzing endpoint data alone can't connect it to network anomalies or suspicious cloud logins happening at the same time, creating blind spots that attackers can exploit.

The problem runs deeper than missing context. Messy data forces security teams to spend enormous effort cleaning and normalizing it before it can be used. The result is AI that underperforms — models overwhelmed by noise, prone to false positives, and unable to detect complex attack patterns. In short, tool sprawl doesn't just complicate security operations; it actively weakens the intelligence meant to strengthen them.

And that weakness matters more than ever. Today's adversaries aren't simply trying to disrupt business for financial gain — they're targeting the very systems that enable recovery. Attacks are designed to erode trust, corrupt data, and prolong downtime, turning disruption into destabilization. When AI defenses are fragmented, recovery slows, and the ripple effects spread far beyond the initial breach.

The cost of over-tooling

The "sprawl tax" represents a very real drain on financial and human capital. Its impact shows up in two ways: direct costs that hit the budget line and the hidden ones that quietly erode productivity and focus.

- **The direct costs are easy to spot.** They include overlapping software licenses, annual maintenance contracts, and the hardware or cloud infrastructure needed to run each product. On paper, each expense looks justified. Together, they add up to an ecosystem that costs far more than the protection it provides.
- **The hidden costs are where the real damage lies.** Redundant functionality means organizations often pay two or three times over for the same capabilities, without realizing it. Every new tool demands specialized expertise — training, certification, and ongoing maintenance — which turns security teams into tool operators instead of strategists. That creates a time tax. Security professionals can spend significant time switching between applications and managing tool sprawl, which amounts to time lost on tool management instead of threat detection, vulnerability management, or proactive risk reduction. Finally, the integration burden can be relentless. Making dozens of incompatible tools work together requires custom engineering and constant upkeep. These integrations are often fragile, breaking whenever a vendor updates its software — consuming even more time and money to repair.

Taken together, these costs form a self-perpetuating cycle of inefficiency: every new tool meant to solve a problem adds another layer of complexity to manage. Over time, the financial drain of tool sprawl becomes not just a budget issue, but a strategic one — diverting energy and investment away from true security outcomes.

60%

of leaders report feeling their IT is not ready to manage future risk

28%

of leaders say stronger cybersecurity posture is critical to proving ROI on digital transformation

42%

of leaders list upgrading their IT infrastructure as a top action to mitigate external business risks

Source: Kyndryl Readiness Report, 2025

The strategic imperative

Addressing the systemic issues of tool sprawl requires more than simply reducing the number of tools; it demands a fundamental shift in strategy. Organizations must move from a tactical, tool-centric approach to a strategic, platform-centric one. It's a process of rationalization and consolidation.

Platformization over point products

The first step is to launch a deliberate and comprehensive audit to discover every security tool in use, identify functional overlaps and capability gaps, and make informed decisions about which tools to consolidate, which to keep, and which to retire.

This rationalization process naturally leads to a platform-centric approach, often referred to as "platformization." A security platform is defined as the integration of multiple, previously disparate security functions into a unified framework. This is not about finding a single tool to do everything, but rather about building a cohesive architecture where different security capabilities work together natively, leveraging a common data model, shared threat intelligence, and integrated workflows. This is particularly important for enterprises looking to integrate modern AI and machine learning into their security.

Driving multi-faceted ROI

Adopting a consolidated, platform-based approach to security yields significant and measurable returns across multiple dimensions of the business.

- **Enhanced visibility and centralized control:** The most immediate benefit of consolidation is the creation of a "single pane of glass" — a unified platform that provides security teams with a holistic, correlated view of their entire security posture across the network, cloud, endpoints, and user identities from a single dashboard. This eliminates the blind spots created by data silos and enables the consistent application and enforcement of security policies across the entire enterprise.
- **Improved operational efficiency:** By reducing the number of interfaces, automating cross-domain workflows, and minimizing context switching, consolidation dramatically improves the efficiency of the security team. It frees analysts from the drudgery of manual data correlation, allowing them to focus on higher-value, strategic tasks such as hunting for threats, vulnerability management, and risk reduction.
- **Unlocking AI-powered defense:** A consolidated platform provides the clean, correlated, and context-rich data AI and machine learning algorithms need to function effectively. This "AI-ready data" enables more accurate threat detection, predictive analytics, and sophisticated automated responses that are impossible to achieve with fragmented data sources.
- **Accelerated threat detection and response:** Integrated platforms are designed to share data and threat intelligence. This enables superior data correlation, which, when combined with AI and machine learning, results in faster and more accurate threat detection. Furthermore, the automation capabilities inherent in these platforms can trigger coordinated response actions across different security layers instantly, reducing the Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) and minimizing the potential damage from a breach.
- **Significant cost savings and optimized TCO**: Consolidation offers a compelling financial case by lowering the Total Cost of Ownership (TCO) of the security stack. It achieves this by eliminating redundant tools and overlapping vendor contracts, which in turn reduces software licensing fees, annual maintenance costs, and the need for specialized training for multiple products.
- **Strengthened security posture and risk management:** Ultimately, the goal of any security initiative is to reduce risk. Consolidation achieves this by directly addressing the root causes of weakness in a fragmented environment. It reduces the overall attack surface by minimizing the number of tools, mitigates the risk of misconfiguration through centralized policy management, and closes the security gaps that exist between siloed solutions. Research indicates that 65% of organizations believe that consolidating their security vendors would improve their overall risk posture.

Conclusion

The next frontier of cybersecurity won't be defined by more tools. It'll be defined by smarter architecture. Enterprises that consolidate now will not only cut cost and complexity, but create the unified, AI-ready foundation needed to stay ahead of tomorrow's ever-evolving threats.

The time to simplify is now — before complexity becomes the biggest vulnerability of all.

kyndryl