SmarterD

IT & Security Data Convergence: Breaking Down Silos for Modern Business Resilience

Alan Boehme
SmarterD Technical Advisory Board Member

Table of Contents

Executive Summary

Organizations are facing unprecedented challenges as disconnected and fragmented IT and security tool setups become the new standard of operation. As a result, stakeholders are seeing significant collaboration disruption, inefficiencies, and potential organizational failure as threats and challenges surface.

Unfortunately, this problem will not be resolved without intentional approaches that manage the dysfunction in a sustainable way. Continuing to use siloed tools for IT operations (such as service desk management, incident response, and patching) results in critical blind spots and friction that can dismantle an organization from the inside out.

This problem isn't uncommon, either. Survey results from Dark Reading show "51% of IT professionals struggle with identifying critical risks due to data silos."

These silos create complexity. Complexity creates risk to the business and is the enemy of security and resilience. The interconnectedness of your tools and data silos has become table stakes to reduce risk and improve resiliency. Teams and stakeholders can limit the consequences and restrictions of a siloed approach by adopting a "single pane of glass" view that unifies and contextualizes the data within their data convergence platforms. This data convergence approach facilitates unified visibility and connected intelligence, enables seamless collaboration, and automates workflows, improving efficiency, data accuracy, and consistency-allowing your tools and data to work together harmoniously.

Read on to learn how your organization can limit risks that come from fragmented tools and siloed data, and how you can benefit from SmarterD's holistic approach.

"Data convergence is the catalyst for a new era of connected enterprise intelligence. At SmarterD, we're building a platform where IT, security, and executives don't just share data—they operate from a unified, intelligent core. By combining context, automation, and agentic AI, we enable organizations to transform complexity into clarity, and fragmented operations into resilient, data-driven action."

— Founder and CTO of SmarterD, Vijay Sundhar, says.

IT & Security Data Convergence: Breaking Down Silos for Modern Business Resilience

Organizations know that IT and security management facilitate business growth and resilience. However, the management of these critical functions is siloed and isolated in disconnected tools — limiting effectiveness and possibly compromising the entirety of the business. While it may seem frustrating or inconvenient on the surface, this fragmentation goes deep — creating significant obstacles that limit collaboration, breed inefficiency, and ultimately erode an organization's ability to remain competitive against risks and competitors alike.

Could your business be at risk? Take a moment and consider any average company that's similar to yours in size and stature. The IT team is likely juggling multiple platforms, yet another for project management, while the security team is trying to use other specialty tools to detect and neutralize threats. While each tool functions well, there's no central directorial "hub." And therein lies the problem.

The Case of the Silent Breach: A Scenario of Disconnected Tools

The Scenario:

A mid-sized financial services firm, Capital Reserve Management, prides itself on its robust security posture and efficient IT operations. However, beneath the surface of seemingly well-functioning departments lies a common yet critical challenge: a fragmented and unintegrated tool landscape.

The IT operations team at Capital Reserve relies on a patchwork of systems. Their network infrastructure is monitored by one platform, server patching is handled by another, the internal service desk runs on a third, and project management for IT initiatives lives in yet another application. Each tool is managed by different team members, often with limited visibility into the others.

Meanwhile, the security team operates in its own distinct silo. They use a cutting-edge threat detection system, a separate vulnerability scanner that runs on a weekly schedule, a dedicated incident response platform, and a Security Information and Event Management (SIEM) system that aggregates logs but lacks deep integration with the operational tools.

The Incident

The Incident:

One Tuesday morning, the security team's threat detection system flags a series of suspicious outbound connections from a seemingly ordinary file server. An alert is generated within the security team's incident response platform. The security analyst investigating the alert notes the IP address of the server and creates a ticket in their system.

However, the security platform doesn't automatically link this IP address to the server's name, its function, or who is responsible for it within the IT operations team. To get this information, the analyst has to manually log into the infrastructure monitoring tool used by IT, search for the IP, and identify the server details. This takes crucial time.

Simultaneously, the IT operations team is dealing with a surge of service desk tickets related to slow network performance – an unrelated issue they are troubleshooting using their network monitoring and service desk tools. They are unaware of the security alert firing on the file server because their tools don't pull information from the security platforms.

The security analyst, having finally identified the server, checks the vulnerability scanning tool's last report for that server. The report is a week old and doesn't show any recent critical vulnerabilities that would explain the suspicious activity. What the vulnerability scanner doesn't know is that a new, critical vulnerability was disclosed just two days prior, and the patch management system, while aware of the new patch, hasn't yet deployed it to this specific server due to it being in a lower-priority patching group based on outdated information in the infrastructure monitoring tool.

As the security team delves deeper, they find evidence of data exfiltration. The attacker exploited the newly disclosed vulnerability, which the vulnerability scanner missed due to its outdated scan, and the patch management system hadn't addressed it due to the lack of real-time vulnerability and asset criticality information from the security and monitoring tools.

The critical delay in correlating the security alert with the server's operational context, its patching status, and the latest vulnerability intelligence — all trapped within separate, uncommunicative tools — allowed the attackers valuable time to extract sensitive data before the breach was fully understood and contained. *The lack of interconnectedness between IT operations and security transformed a potentially containable incident into a significant data breach, highlighting the critical blind spots created by their disconnected toolsets.*

Obstacles Created by Siloed IT and Security Tools

Additional risks organizations run by failing to have a unified approach to IT and security management include:

Lack of Unified Visibility

When IT and security operate in separate tools, critical understanding and collaboration gaps surface — possibly leading to catastrophic effects on a business's cybersecurity posture.

Consider this example: A business's security team might be drowning in a sea of alerts from its intrusion detection systems (IDS), vulnerability scanners, and threat intelligence feeds. While each alert is a data point, the overall flow of information lacks context about the underlying IT infrastructure. While IT could speak to this, they may not if they are unaware that a problem is present. This is where the interconnectedness of a "single pane of glass" view holds particular value.

While it may require upfront investment and effort, it's incredibly difficult for security analysts to gauge the true severity and potential impact of a threat without a total holistic view and intentional collaboration with complementary teams, like security team members. They see what might be happening, of course, but not where it is happening in a meaningful business context (or the possible customer and team implications).

Conversely, the IT operations team is focused on maintaining system uptime, managing performance, and implementing changes using their own set of monitoring and management tools. They might see unusual network traffic or server load spikes, but without input from security tools, they might dismiss these as routine operational fluctuations rather than potential indicators of a security incident.

The result? The data-driven decision-making that should be happening is distilled down into educated guessing and conjecture. Additionally, resources — both human and technical — often go completely misallocated, focusing on lower-priority issues while critical threats go unaddressed.

"63% of [polled] organizations report that siloed data decreases their security response times."

Delayed Incident Response

Every minute of downtime or unchecked malicious activity increases the potential for financial loss, data compromise, operational disruption, and reputational damage.

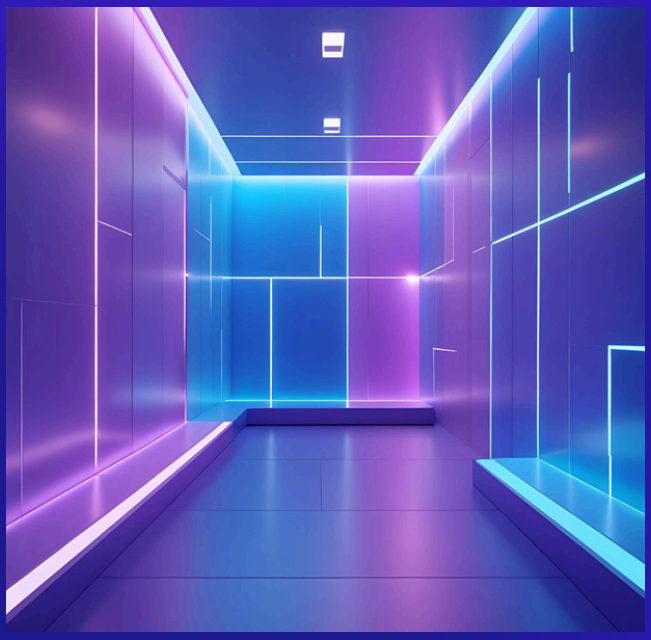
In organizations where IT and security tools and data are disconnected, the very process of understanding what is happening, how it happened, and which systems are affected becomes a cumbersome manual investigation that spans multiple platforms. It's such a prevalent issue that Help Net Security found that "63% of [polled] organizations report that siloed data decreases their security response times."

This constant "swivel chair" effect — manually logging into different systems, exporting data, correlating timestamps, and trying to piece together a coherent timeline — is a massive time sink during a crisis and increases risk while killing resiliency. It's like trying to solve a complex puzzle where half the pieces are in one room and the other half are in another, and you must run back and forth to compare them. This effect significantly hinders the teams' ability to quickly identify the root cause of any risk, accurately assess the full scope of the impact across the IT environment, and formulate an effective containment and recovery plan.

Inefficient Communication and Collaboration

When IT and security teams operate with entirely separate sets of tools (i.e., different ticketing systems, chat platforms, and reporting structures), the communication channels themselves become fragmented, and data loss becomes more of a risk.

Since 41% of organizations struggle to collaboratively manage cybersecurity due to data silos, it's clear that removing the digital "walls" associated with a fragmented approach and building interconnectedness through data convergence should be a top priority for teams and stakeholders.



Duplication of Effort and Inconsistent Data

A common and damaging outcome of a fragmented approach is the independent collection and maintenance of overlapping datasets.

This isn't just inefficient; it actively creates "multiple sources of truth" that inevitably diverge over time — ultimately breaching data pool integrity and throwing data-based red herrings into strategy discussions and decision-making.

Beyond the obvious inefficiency and risk in this process, the other more pressing concern is the lack of trust that surfaces when data becomes unreliable. Your team may wonder: Which version is correct? Is the list complete? Who will be the decision-maker if data does not match across sources, determining which is the "most true?"

This uncertainty makes it difficult to base critical decisions on the available information, leading to hesitancy and missed opportunities for teams as they work to secure the cyber landscape.

Difficulty in Prioritizing Risks

A high technical severity score doesn't always equate to the highest business risk. Teams need input from both IT and security to accurately determine what does.

The problem: In organizations with siloed tools, the security team's vulnerability data resides in their security scanners or vulnerability management platforms; while the IT team's data on asset criticality, business ownership, and function typically resides in their Configuration Management Database (CMDB), asset inventories, or business continuity planning documentation. These systems remain generally disconnected from the security tools, if they even exist at all.

This separation means inefficiency if there is ever collaboration with the IT team for remediation after a breach, as the crucial context about *which* assets are most vital to the business are missing or difficult to access alongside the vulnerability data.

Hindered Strategic Planning

Developing robust, forward-looking strategies for IT and security programs requires teams to maintain an understanding of the current state. A single pane of glass, 360-degree view helps them anticipate future challenges and plan investments and initiatives that will protect and enable the business long-term.

Encourage teams and stakeholders to consider several interconnected factors as they build workflows, such as:

- **The Technology Landscape:**
  What hardware, software, applications, and services does the organization currently use? Where are they located? How are they interconnected? What is their lifecycle?

- **The Threat Surface:**
  Where are the organization's vulnerabilities? What threats are most likely to target them? What is the potential impact of a successful attack? What security controls are currently in place, and how effective are they?

- **Operational Capabilities:**
  What are the IT team's strengths and weaknesses in managing the infrastructure? How efficient are the processes? What is the capacity for change or incident response?

- **Business Objectives:**
  What are the organization's strategic goals (e.g., expand to new markets, launch new digital products, improve customer experience)? How does technology support these goals and are they mission-aligned? What are the key risks to achieving them?

When IT and security data and workflows are trapped in siloed tools, getting this holistic view becomes incredibly difficult. As a result, strategic plans are often developed in isolation or based on incomplete information. *This leads to strategies that are not truly cohesive, may leave critical gaps, result in wasted investment, and fail to adequately enhance the organization's resilience against future threats and operational challenges.*

Increased Operational Overhead

Beyond the direct costs of licensing and maintenance for each individual tool, managing a siloed IT and security stack introduces a host of hidden, but significant, operational overheads that shouldn't be ignored as you run the numbers.

Consider the most pressing areas of cost below as you plan your pivot:

- **Administrative Burden:**
  Each tool requires its own administrative tasks — think installation, configuration, updates, patches, user management, backups, and troubleshooting. This multiplies the administrative workload for IT and security operations teams.

- **Training Costs:**
  Personnel need to be trained on the unique interfaces, workflows, and quirks of every single tool they use. This increases training time and complexity, especially for individuals who need to interact with systems on both the IT and security sides.

- **Context Switching:**
  Users constantly have to switch between different applications, each with its own login, interface, and data model. This context switching is inefficient and increases the likelihood of errors.

- **Manual Processes:**
  As highlighted earlier, siloed tools require manual processes for correlating data, transferring information, and coordinating workflows between teams. These manual steps are time-consuming and prone to error.

- **Redundant Infrastructure:**
  Maintaining separate tools often requires redundant underlying infrastructure, databases, and monitoring systems.

- **Troubleshooting Complexity:**
  When something goes wrong that involves multiple systems (e.g., a security alert that points to a performance issue), troubleshooting becomes a multi-system investigation across disparate logs and dashboards.

The Value of a Single Pane of Glass through Data Convergence Platforms

The solution to the challenges posed by siloed tools lies in adopting a "single pane of glass" approach, often facilitated by data convergence platforms. These platforms are designed to integrate data from various IT and security tools, bringing it together into a unified, centralized view. *Data convergence platforms break down the walls between IT and security by:*

- **Providing Unified Visibility:**
  By aggregating data from disparate sources, these platforms offer a holistic view of the IT infrastructure, security events, vulnerabilities, and operational metrics. This allows both IT and security teams to work from the same, accurate information.

- **Enabling Seamless Collaboration:**
  A single pane of glass provides a shared platform for communication, incident response, and project management related to IT and security. In this format, teams can easily share information, assign tasks, and track progress within a unified environment.

- **Automating Workflows:**
  Data convergence platforms can automate workflows based on integrated data. For example, a critical security alert can automatically trigger the creation of an IT incident ticket with all relevant context attached, streamlining the response process.

- **Improving Data Accuracy and Consistency:**
  By acting as a central repository, these platforms help ensure data consistency and reduce the likelihood of errors caused by manual data correlation.

- **Facilitating Risk Prioritization:**
  By linking security data with IT asset information and business criticality, data convergence platforms enable more informed risk assessment and prioritization, allowing teams to focus on the most critical threats.

Data Convergence Platforms and Increased Organizational Resilience

The adoption of a single pane of glass through data convergence platforms directly contributes to increased organizational resilience in several impactful ways.

- **Faster and More Effective Incident Response:**
  With unified visibility, an organization is better equipped to withstand disruptions, whether they are caused by cyberattacks, system failures, or other unforeseen events. The improved collaboration and visibility offered by data convergence platforms are crucial for maintaining business continuity.

- **Proactive Threat Mitigation:**
  By having a clearer picture of the threat landscape and vulnerabilities in the context of their IT infrastructure, organizations can proactively identify and mitigate potential risks before they are exploited.

- **Improved Security Posture:**
  Enhanced collaboration and unified visibility lead to a stronger overall security posture. Security policies can be more effectively enforced, and vulnerabilities are less likely to fall through the cracks.

- **Better Resource Utilization:**
  By eliminating duplicate efforts and streamlining workflows, organizations can optimize the use of their IT and security resources, allowing teams to focus on higher-value activities.

- **More Informed Decision-Making:**
  Access to comprehensive and accurate data empowers leaders to make better-informed decisions regarding IT investments, security strategies, and risk management.

- **Enhanced Business Continuity:**
  A resilient organization is better equipped to withstand disruptions, whether they are caused by cyberattacks, system failures, or other unforeseen events. The improved collaboration and visibility offered by data convergence platforms are crucial for maintaining business continuity.

"Knowledge workers spend an average of 12 hours a week chasing data due to silos."

Managing IT and security projects in siloed tools is a relic of the past that actively undermines an organization's ability to operate efficiently and securely. The costs are simply too high to accept this as your reality. The obstacles this creates in terms of visibility, collaboration, and incident response are significant. A commissioned study conducted by Forrester Consulting on behalf of Airtable found that "Knowledge workers spend an average of 12 hours a week chasing data due to silos."

By embracing the concept of a single pane of glass through data convergence platforms, organizations can break down these silos, foster seamless collaboration between IT and security teams, and ultimately build a more resilient and future-ready enterprise capable of navigating the complexities of the digital age.

Work Cited

- https://www.darkreading.com/vulnerabilities-threats/survey-findings-show-link-between-data-silos-and-security-vulnerabilities
- https://www.helpnetsecurity.com/2024/05/28/data-silos-problem-for-organizations/
- https://venturebeat.com/data-infrastructure/report-data-silos-cause-employees-to-lose-12-hours-a-week-chasing-data/

Get Started Today!

SmarterD's powerful data convergence platform provides IT and security teams with the necessary tools to connect data from disjoined systems, automate responses, and optimize risk prioritization — ultimately resolving the common concerns that siloed teams face.

Unlike traditional GRC platforms that primarily focus on governance frameworks, SmarterD delivers a truly integrated and converged platform specifically designed for IT and security risk management.

The platform's AI-driven intelligence and automation capabilities eliminate the reliance on error-prone spreadsheets and manual processes that consume valuable team resources.

Instead, SmarterD's unified approach breaks down the silos currently existing in adjacent teams; creating a single source of truth that empowers collaboration and a transition from reactive and fractional action to proactive risk management.

Ready to experience the difference a foundation of convergence can make? Experience the power of complete visibility and interconnected, intelligent automation firsthand with SmarterD. Connect with us today to secure your demo.

Schedule a Demo Today