# BTR: Mid-Market Firms Grapple with Cybersecurity Fragmentation as Tool Sprawl Exposes Risk

WASHINGTON, DC, UNITED STATES, November 13, 2025 /EINPresswire.com/
-- For mid-sized businesses, cybersecurity is increasingly defined by a paradox: the more tools they deploy, the more vulnerable they may become.

> The more solutions organizations stack, the more seams they create — and those seams are where adversaries thrive."
>
> *Manoj Srivastava, Blackpoint Cyber*

Industry analysts estimate that more than 3,000 enterprise security solutions are now available. While large enterprises often have the staff and governance structures to integrate disparate tools, companies with 500 to 5,000 employees typically do not. The result is a patchwork of overlapping products that create blind spots, inflate costs, and complicate risk management.

"The more solutions organizations stack, the more seams they create — and those seams are where adversaries thrive," said Manoj Srivastava, Chief Technology and Product Officer at Blackpoint Cyber, during a recent BizTechReports Vidcast interview.

Tool Fragmentation as a Systemic Challenge

Mid-market firms often purchase security tools tactically rather than strategically, adding point solutions in response to emerging threats. Yet without integration, these tools generate silos of data that executives cannot easily translate into meaningful risk assessments.

Srivastava described the effect as the "barnacle problem" — solutions that accumulate over time but slow organizations down and create vulnerabilities where they intersect. "The conversation should not be about how many tools you have, but about dwell time, response speed, and quantifying risk," he said.

This view aligns with global market research. IDC projects that worldwide security spending will rise 12.2% in 2025, driven largely by integrated approaches such as cloud-native application protection, identity and access management, and security analytics.

The Shifting Role of Managed Service Providers

Many mid-market organizations turn to Managed Service Providers (MSPs) to assemble and operate their security stack. But MSPs are also facing an inflection point. Historically positioned as technology resellers, they now must evolve into risk advisors capable of translating technical signals into business language.


Manoj Srivastava, Blackpoint Cyber

“MSPs need to move from saying, ‘Here’s a firewall,’ to saying, ‘Here’s your security posture, and here’s how it aligns with your business strategy,’” Srivastava said.

This mirrors broader industry findings. BizTechReports has reported that MSPs are undergoing consolidation and operational discipline, with the next wave of growth hinging on delivering outcomes rather than just tools

Discovery and Context

Any path toward rationalized security spending begins with discovery: identifying assets, users, and applications that form the attack surface. Srivastava stressed that automated fingerprinting, coupled with user input, creates the unified data model required to contextualize risk.

“You can’t secure what you don’t know you have,” he said. “Visibility is the first step in building a realistic risk profile. But it is a challenge for organizations that lack the resources associated with large enterprise organizations.”

Because mid-market firms have already invested heavily in security tools, demanding wholesale replacement is impractical. Instead, Srivastava advocates for integration: layering on platforms that consolidate and contextualize existing tools, creating a unified view without discarding sunk investments.

Integration, he added, is not only a technical necessity but also a financial one. Each additional tool creates hidden costs — licensing fees, integration challenges, and staffing requirements. “It’s not only the price of the product,” he said, “it’s the people and processes needed to stitch everything together.”

## Economics of Sprawl

These hidden costs accumulate quickly, and over time they reshape the economics of cybersecurity. What begins as a series of tactical purchases to address specific threats can evolve into a sprawling architecture that is both expensive and inefficient. The economics of tool sprawl are clear: redundancy, inefficiency, and wasted effort. Security budgets balloon as firms attempt to plug gaps with more products, but the outcomes often fail to match the investment.

IDC's forecast underscores this tension. Security software is expected to remain the largest and fastest-growing segment globally, but growth will concentrate in platforms that unify posture rather than isolated point solutions.

## From Technical to Business Conversation

The challenge is as much cultural as it is technical. Business leaders care about resilience, compliance, and cost. Security teams often speak in logs, vulnerabilities, and patches. MSPs and vendors that can translate between these languages — turning technical alerts into business posture — will increasingly define the competitive landscape.

"Owners of mid-sized firms aren't focused on security; they're focused on running their business," Srivastava said. "They need partners who can bridge that gap."

## Strategic Implications

Blackpoint Cyber has positioned itself to address these realities by focusing on integration, visibility, and translation. Its managed detection and response roots provide the speed and human expertise needed to counter active threats, while its new Compass One platform aims to unify disparate signals into a single posture framework. By giving MSPs and mid-market executives a common language for risk, the company is seeking to shift security conversations from tool deployment to business resilience.

As threats intensify, mid-market firms risk falling behind if they continue to rely on fragmented defenses. Attackers are targeting them precisely because they sit between well-defended enterprises and smaller, less attractive targets.

For vendors and MSPs, success depends on adapting to this environment. Technical expertise alone will not suffice. What matters is the ability to rationalize tools, integrate data, and present security posture in business terms.

"The future of cybersecurity isn't just about buying more," Srivastava said. "It's about unifying what you have, prioritizing what matters, and making security decisions in the language of business."

Click here to read the Q&A based on this interview.

Airrion Andrews
BizTechReports
email us here