Futurum®

brinqa

Vulnerability Management at Scale: Moving from Telemetry Overload to Orchestrated Remediation

MAY 2026

Introduction: Strategic Imperative & Key Business Challenges

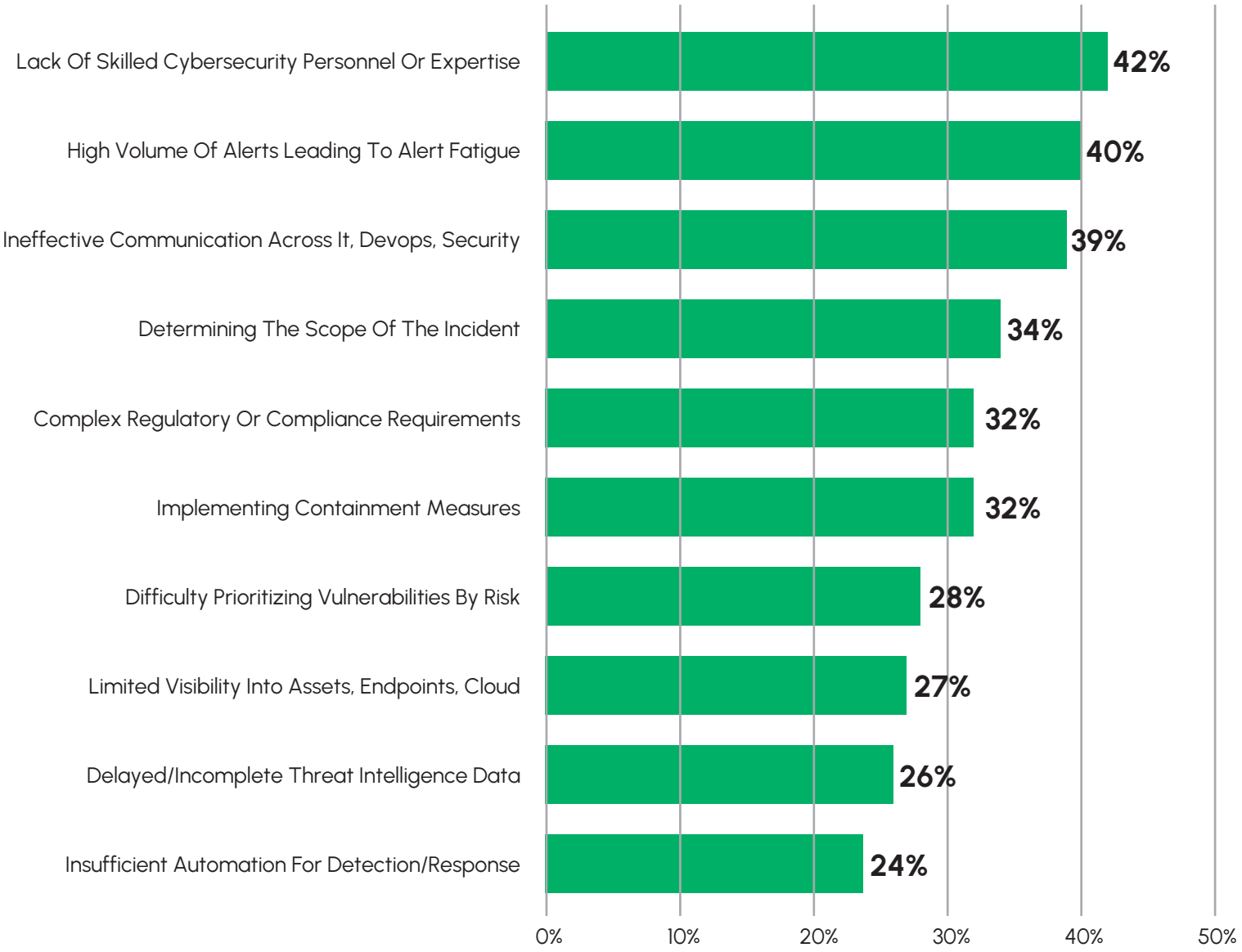
Even before the AI surge, enterprise cybersecurity demands shifted considerably, particularly around vulnerability management. Security teams have been moving from reactive vulnerability discovery to a more proactive Continuous Threat Exposure Management (CTEM) approach.

In modern, highly distributed environments, the goal is to measure vulnerability management by continuous, quantifiable metrics of business resilience and not by the technical metric of "flaws found." Organizations prioritizing investments in continuous exposure management and automated routing will be better positioned to deliver the resilience businesses need.

However, the market is currently constrained by the structural and organizational limitations of legacy security practices. Traditionally, enterprises invested in standalone vulnerability scanners focused on detecting flaws across their infrastructure. The operational reality is that this approach of compiling endless lists of vulnerabilities largely fails the business because it dumps disconnected data into silos with limited, if any, contextualization methodologies. This older model overwhelms IT operations with unactionable alerts and blinds executive leadership to operational risk. The market is shifting away from basic vulnerability management toward contextualized, enterprise-wide exposure management.

The data distinctly reflects this failure. According to Futurum's 2H25 Cybersecurity Decision Maker Survey, the primary hurdles to resolving security vulnerabilities are not technology limitations, but human bottlenecks. Respondents cited a high volume of alerts leading to analyst fatigue and ineffective communication across IT, DevOps, and security teams as their top operational hurdles (see Figure 1).

Figure 1. SOC Burdens



Source: Futurum Research, Cybersecurity Decision Maker Survey, 2H 2025.

The financial and operational friction caused by this disconnect is severe, and the urgency to resolve it isn't decreasing. As a recent example, the industry is digesting the implications of Anthropic's Project Glasswing: while there is considerable confusion about the specifics of Anthropic's new Mythos model, the industry's consensus is that the barrier to executing increasingly sophisticated cyberattacks continues to lower. Since malicious actors can now increasingly automate complex exploits with ease, addressing the existing market failures of analyst alert fatigue and delayed Mean Time To Resolve (MTTR) has become even more important. Without contextualized data to enforce cross-team accountability and accelerate remediation, organizations will face compounding technical debt and a systemic inability to execute a functioning CTEM cycle in the face of this evolving threat landscape.

Critical Insights and Decision-Making Criteria

To bridge the gap between security telemetry and business risk, cybersecurity decision-makers must evaluate their exposure management strategies against three critical operational realities.

The Necessity of Relationship-Driven Data

Executive leaders must recognize the structural divide between legacy vulnerability management and modern CTEM. Standard vulnerability platforms attempt to combine discovery, assessment, and prioritization workflows into a single silo, fundamentally failing to account for the complex enterprise realities. Specifically, two key issues exist:

- On a technical level, enterprises traditionally relied on more relational database architectures not well-suited for complex relationship mapping.
- They often need to account for strong heterogeneity of signals and tools in complex enterprise environments.

The use of more graph-based architectures has emerged as a key component of modern vulnerability management offerings, as those are much better suited for mapping complex relationships.

This need amplifies in complex environments, where different parts of the organization may rely on different security tooling to achieve similar results. The growing criticality of cybersecurity as a board-level conversation pressurizes teams to harmonize results across the organization, even as traditional tooling may lag.

The Integration Trap

To compensate for the lack of unified platforms, enterprises often build their own data normalization engines. This exposes a hidden, undifferentiated burden on the organization, one that likely falls outside its actual business goals. Organizations end up with budget demands to support internal engineering teams building and maintaining custom API integrations, primarily to deduplicate security data from a rotating stack of scanning tools and to bring some level of business context to the process.

Futurum's survey data validates this friction: assessing integration complexity is currently considered the second-biggest challenge in evaluating new security offerings. Furthermore, when selecting platforms, buyers indicated prioritizing integration and operational efficiency over feature specialization by a meaningful two-to-one margin. To overcome the resource drain from custom-built normalization efforts, enterprises require a scalable, automated data abstraction layer that natively enables support for different scanning technologies without breaking downstream operational workflows.

The Danger of "Black Box" Automation

Automation capabilities, increasingly reliant on AI, are now all but required to manage the massive scale of modern threat telemetry; however, they cannot operate autonomously without strict oversight. The interest in different flavors of automation, including autonomous operation, is understandable, but in some cases, it may introduce unacceptable risks to organizations managing mission-critical systems. To ensure that risk-acceptance and remediation decisions are defensible to the board and external auditors, decision-makers should ensure their vulnerability management tools have robust guardrails for AI. AI ingestion and deduplication must utilize user-defined confidence thresholds, maintain human oversight, and provide transparent audit trails that connect any unified finding directly back to their original source data.

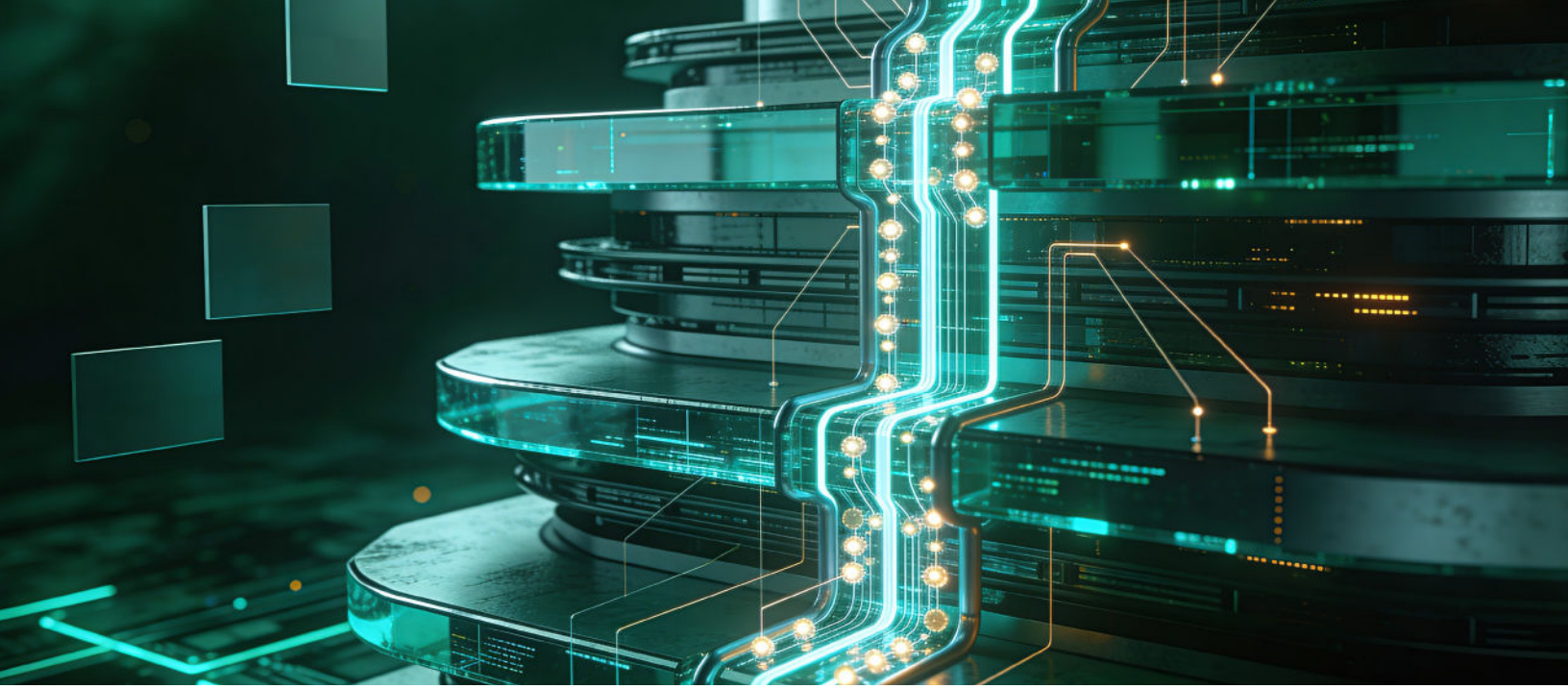
Strategic Recommendations for Exposure Management

Based on these factors, organizations are highly encouraged to consider the following recommendations in relation to their exposure management programs:

- **Decouple Intelligence from Execution**. Organizations, particularly larger enterprises, are strongly encouraged to modularize the key functions of their exposure management program – detection, analysis, execution. In this model, vulnerability detection uses a variety of tools to identify potential vulnerabilities, followed by a dedicated analysis layer that ingests, normalizes, deduplicates, and prioritizes risk. The analysis layer is the ideal place to apply modern AI capabilities. The execution layer then consists of the IT and DevOps tools that actually apply the patch or mitigation. Coupling these layers creates operational bias. By decoupling them, organizations create a more objective, centralized routing engine that ensures remediation tickets are sent to the correct asset owner with the exact context required to fix the issue.

- **Institute Policy-Based Automation**. Enterprises should move aggressively to eradicate ad hoc manual ticketing and spreadsheet-driven vulnerability tracking. To bridge the documented, historical divide between InfoSec, IT Ops, DevOps, and AppSec, organizations should implement continuous automation workflows. These workflows, which can benefit from more consistent vulnerability analysis and better alignment with business objectives through enhanced use of business context, can then route mitigations strictly based on predefined, approved risk policies, reducing friction and ensuring MTTR SLAs are enforced automatically.

- **Move Toward Cyber Risk Quantification (CRQ)**. The increased strategic importance of cybersecurity necessitates that security programs be grounded in robust risk management practices, so they can be more easily discussed with senior leadership. To that effect, organizations should consider a broader move toward CRQ. Specifically on the topic of vulnerability management, reporting on the "number of vulnerabilities closed" is a legacy metric that fails to translate technical debt into financial risk. Leadership must work toward reporting on the "reduction of business exposure." Executing this requires, among other things, investing in enterprise-grade data lakes capable of multi-year historical data retention to support long-term strategic trend analysis, regulatory compliance auditing, and defensible board-level reporting.

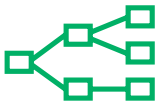


Brinqa as the Orchestration Layer: Enabling a Coordinated Vulnerability Response

Our analysis shows that Brinqa reflects the shift from fragmented visibility to orchestrated, scalable execution in vulnerability management, aligning closely with the core operational requirements outlined in this brief.

Support for Contextualized Data: Brinqa addresses the requirement for contextualized risk data through its underlying graph database architecture. By replacing flat relational tables with a relationship-driven model, the platform natively maps the complex connections between technical assets, real-world threat intelligence, and business criticality to accurately reflect true organizational exposure.

Scale and AI Guardrails: To address integration challenges, Brinqa uses an elastic compute architecture that ingests and normalizes hundreds of millions of signals across 240+ native integrations. Furthermore, its implementation of AI for data deduplication and attribution operates within recommended strict guardrails. It requires user-defined confidence thresholds and structurally maintains a verifiable audit trail from the unified data model back to the original source telemetry, ensuring data defensibility.



Orchestration and Quantification: In alignment with the recommendation to decouple intelligence from execution, Brinqa does not execute remediation actions directly. Instead, it functions purely as the centralized routing engine. It utilizes continuous, policy-based automation to trigger workflows in downstream ITSM and DevOps systems. Finally, Brinqa utilizes a dedicated, cloud-native data lake to provide the multi-year data retention required for complex regulatory auditing and executive-level CRQ.

Important Information About This Report

AUTHORS

Fernando Montenegro
Vice President & Practice Lead, Cybersecurity & Resilience | The Futurum Group

PUBLISHER

Futurum Research

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

brinqa

ABOUT BRINQA

Brinqa empowers enterprises to understand and reduce technology risk by delivering full visibility into exposures that impact the business. The Brinqa platform consolidates and normalizes data from across your security stack, enriches it with business and threat intelligence, and prioritizes remediation based on actual risk. Trusted by the world's leading organizations, Brinqa transforms traditional vulnerability management into a strategic risk management capability - driving faster remediation, improved security posture, and measurable reductions in business risk.

Futurum®

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.