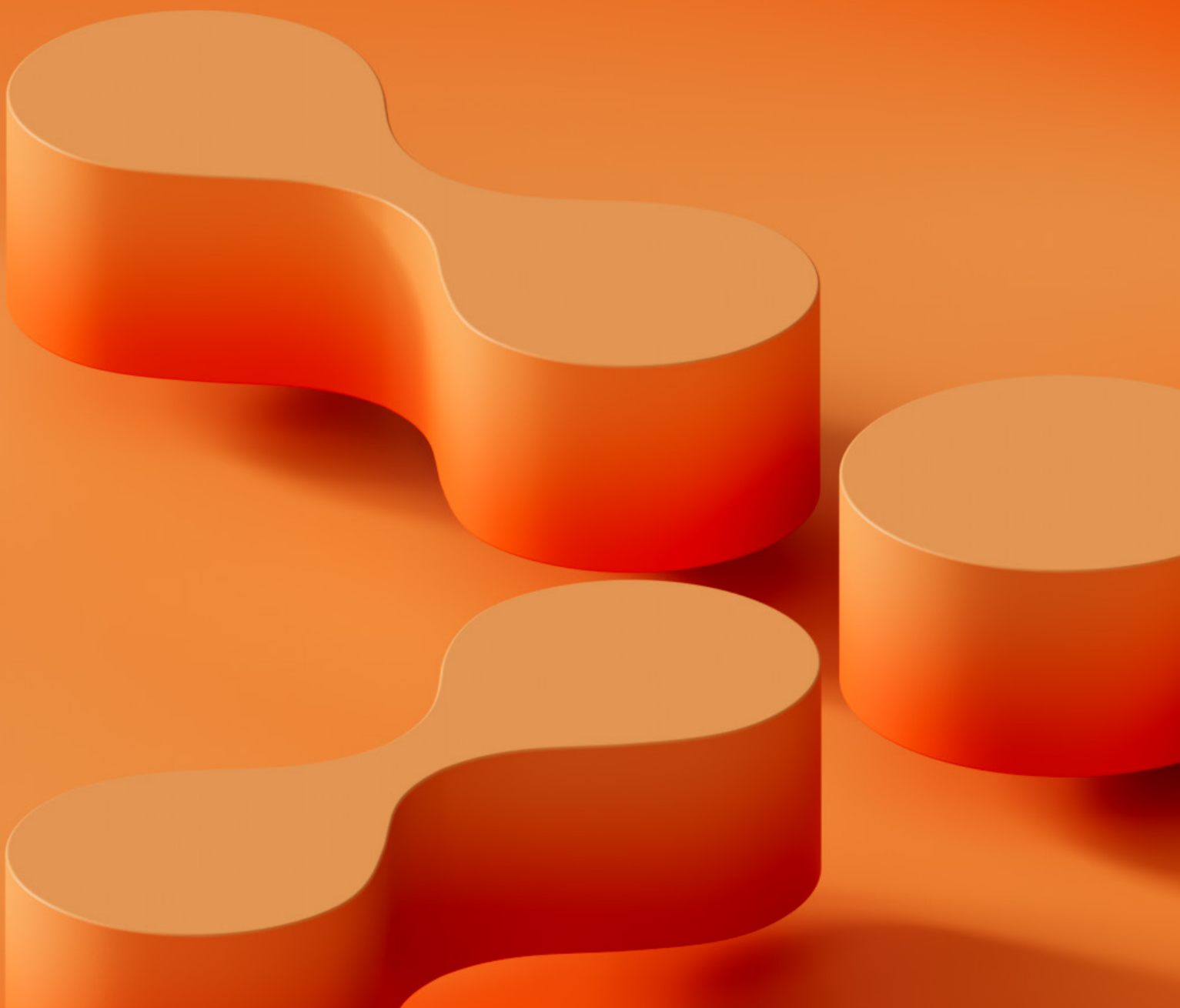


The Trust Factor: How *Trusted Data* Drives Smarter Vulnerability and Exposure Management

Q2—2025



Setting the Stage

In cybersecurity, trust in your data is essential—you can't defend against threats if you don't trust the information you're using. Organizations must have complete confidence in the accuracy of their data to quickly find weaknesses, respond to attacks, and protect their systems. This need for speed is critical as cyber threats are [increasingly sophisticated](#), and there is a [shortage of security professionals](#).

To understand how organizations are managing these challenges, Axonius commissioned a survey of 500 security and IT leaders in the U.S. We wanted to learn how they're dealing with vulnerabilities and exposures to keep their organizations secure in a complex environment.

We found that while security and IT leaders generally feel prepared to act when they discover vulnerabilities, and believe they have enough information to quickly fix them, their actual performance often falls short. Companies are slow to detect and correct vulnerabilities and exposures, and they don't conduct security assessments frequently enough, which gives attackers more opportunities to exploit these weaknesses.

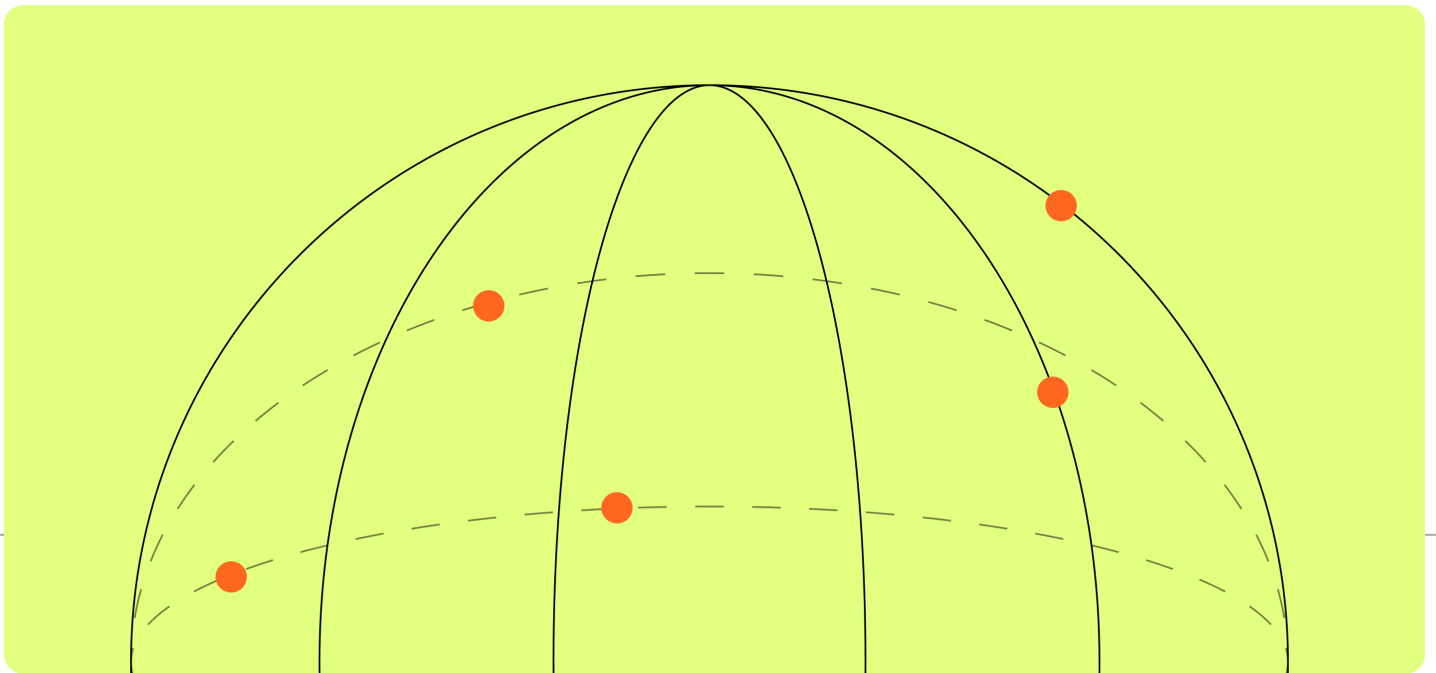
A key underlying issue is a lack of trust in the security data itself. Data is often scattered across isolated systems, which prevents organizations from responding effectively. This combination of issues leaves organizations in a reactive mode, struggling to keep up with threats. Although technologies like AI and automation, and approaches like Continuous Threat Exposure Management (CTEM), have the potential to improve the situation, the core challenge is bridging the gap between feeling ready and being able to execute effectively.

Key Takeaways

- **Confidence in Execution is Hindered by Bad Data:** 90% of leaders say their organization is prepared to take immediate action when a vulnerability or exposure is detected, yet only 25% trust all the data in their security tools.
- **Data Challenges Impede Effective Action:** Leaders cite inconsistent data (36%), incomplete data (34%), and inaccurate data (33%) as reasons for mistrust, and struggle with prioritization / risk assessment (29%) and integrating data across tools (27%).
- **Delayed Remediation and Infrequent Assessments Expose Gaps:** Four in five organizations take more than 24 hours to remediate a critical vulnerability (81%) or exposure (80%), and only about three in ten conduct vulnerability (29%) and exposure (28%) assessments weekly or daily.
- **CTEM Adoption is Growing:** 58% report that they have already adopted a CTEM framework.
- **Data-Driven Remediation is Crucial:** When prioritizing remediation efforts, organizations most often use a risk-based approach (39%), automation (32%), and common vulnerability scoring system (CVSS) (29%).
- **AI and Automation Offer Promise:** The most common applications of AI and automation in vulnerability and exposure management are automated patching and remediation (42%), automated vulnerability scanning and assessment (40%), and AI-driven prioritization of vulnerabilities based on risk (40%).

Confidence vs. Execution:

Ensuring a Strong Data Foundation



Organizations have an unprecedented quantity of data. When used correctly, this data should allow security and IT leaders to generate actionable insights and safeguard against potential vulnerabilities and exposures.

Nearly all (90%) security and IT leaders say their organization is prepared¹ to take immediate action when a vulnerability or exposure is detected. Over four in five (86%) say they have enough actionable insights to base their remediation plan on when a vulnerability or exposure is detected.

However, their confidence is based on unreliable data. These findings beg the question—why are security and IT leaders so confident in their preparedness to handle vulnerabilities and exposures but have so much room to improve their execution?

Protecting their organizations is an intensive process as professionals must continuously monitor systems, apply patches, analyze alerts and stay up to date on the latest tools and security-related insights to protect against vulnerabilities. **Data silos and a lack of trust in data are pervasive issues that are holding organizations back from more effectively detecting and remediating vulnerabilities and exposures.**

¹Very prepared or Prepared

75% of IT and security leaders *don't trust* all their organization's data.

There is mistrust amongst leaders regarding the quality of the data at their disposal. Only 25% of respondents say they trust all the data in their organization's security tools. Leaders who do not trust the accuracy of the data in their organization's security tools highlight concerns of inconsistent data (36%), incomplete data (34%) and inaccurate data (33%), which not only undermines confidence in the data, but also the decisions based upon it.

Top-cited reasons for a lack of trust in the data in their organization's security tools:

- Inconsistent data 36%
- Incomplete data 34%
- Inaccurate data 33%

Translating readiness into swift and effective action remains a complex task. We found that four in five organizations take more than 24 hours to remediate a critical vulnerability (81%) or exposure (80%), indicating room for improvement in how organizations are executing vulnerability and exposure management. The frequency with which security assessments take place is also a concern with only about three in ten conducting vulnerability (29%) and exposure (28%) assessments weekly or daily. This leaves seven in ten organizations not catching potential risks on a weekly basis, increasing the likelihood that threats go undetected and unresolved.

Only three in ten organizations *conduct vulnerability* and *exposure assessments* weekly or daily

Further, security and IT leaders struggle with prioritization / risk assessment (29%) and integrating data across tools (27%). Correspondingly, when asked what would help drive better actionable insights for vulnerability and exposure management, three in ten (29%) say improved threat intelligence feeds, followed closely by real-time data and alerts (27%), and automated prioritization of vulnerabilities (26%).

Data should be connected and reliable, providing organizations the ability to automate the prioritization of vulnerabilities, receive timely alerts, and leverage threat intelligence feeds. Even with access to unprecedented quantities of data and advanced tools, it remains clear that there are gaps in organizations' threat management.

Anticipation to Action: How IT Leaders Balance Proactive and Reactive Approaches to Risk Management



Security and IT leaders outline network security weaknesses (22%), cloud security risks (20%), weak or compromised credentials (18%), and phishing / social engineering attacks (18%) as top risk factors for their organization. Given the diverse nature of these threats, **they recognize the need to balance proactive and reactive strategies for threat management.** Over half (56%) describe their organization's current approach to managing vulnerabilities and exposures as a balance between the two, and 50% believe that such a balance represents the most effective strategy.

Leaders note that limited internal expertise (43%), organizational culture (36%), and lack of budget (31%) prevent their organizations from taking a more proactive approach to managing vulnerabilities and exposures.

50% believe a balance between proactive and reactive strategies to be the *most effective approach*

Organizations are also turning to Continuous Threat Exposure Management (CTEM) to enhance their approach, with 58% reporting that they have already adopted a CTEM framework. An additional 34% plan to implement CTEM in the near future. For many organizations, the top motivations behind adopting or planning to adopt CTEM include a desire to reduce security risk (48%) and to accelerate the speed of remediation (48%).

However, this adoption of CTEM is not without its challenges. The most prominent challenges include integrating CTEM tools across various security platforms (38%), measuring ROI and program effectiveness (35%), dealing with limited budgets and resources (34%), and automating remediation efforts (34%). Failure to address such challenges may leave organizations vulnerable to threats, as gaps in integration, automation, and over-reliance on outdated technology can result in slower detection speed for critical threats.

Top challenges that hinder the adoption of CTEM:

- Tool integration across security platforms 38%
- Measuring ROI and program effectiveness 35%
- Limited budget or resources 34%
- Automating remediation efforts 34%



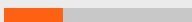
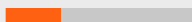






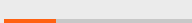
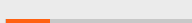


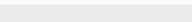
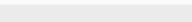
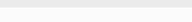
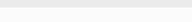
Ultimately, it is the integrity of the data that underpins every decision made in the threat management process. Organizations are increasingly recognizing that better-connected systems and trustworthy data are essential to truly strengthen both proactive detection efforts and reactive response strategies.

Data-Driven Remediation: Risk Prioritization, Integration, and Automated Remediation

When prioritizing remediation efforts for vulnerabilities, organizations most often use a risk-based approach (39%), automation (32%), and common vulnerability scoring system (CVSS) (29%). This multi-pronged approach emphasizes the use of technology to detect and remediate vulnerabilities based on pre-defined rules and helps organizations to tackle vulnerabilities based on risk assessment.

Just over four in five (83%) say their organization remediates a critical vulnerability within two weeks of detection; similarly 85% report the same timeframe for addressing critical exposures. **However, the process is far from streamlined.** Most (98%) organizations use more than one tool for both vulnerability management and exposure detection and remediation. Further, security and IT leaders recognize that a wide array of tools are required to appropriately safeguard their organization from threats. If data points from multiple sources are not accurately aggregated, correlated, and acted upon, this multi-tool approach can create silos amongst groups and complicate the flow of critical information for the organization.

Top tools currently used:

	Vulnerability Detection and Remediation	Exposure Detection and Remediation
Cloud Security Posture Management (CSPM)	35% 	28% 
Endpoint Detection & Response (EDR)	32% 	30% 
Risk Based Vulnerability Management (RBVM)	30% 	27% 
Security Information and Event Management (SIEM)	29% 	30% 
Security Orchestration, Automation, and Response (SOAR) Tools	29% 	24% 
Vulnerability Management Tools	28% 	24% 
Threat Intelligence Platforms (TIPs)	28% 	25% 
Network Security Tools	27% 	27% 
Identity Access Management (IAM)	26% 	31% 

The top priorities for organizations addressing vulnerabilities in their technology stack are protecting customer data (47%) and ensuring the speed of remediation (40%). **Beneath this drive to protect customers lies persistent challenges—prioritization isn't always clear-cut, and existing tools don't always integrate as seamlessly as needed.** The most common challenges they face when remediating vulnerabilities are difficulty in prioritization or risk assessment (29%) and lack of integration with existing security tools (27%). These hurdles can slow down response times and increase the risk of a breach, especially when data is scattered across multiple platforms and lacks consistency.

Top challenges organizations face when remediating vulnerabilities:

- Difficulty in prioritization / risk assessment 29%
- Integration with existing security tools 27%
- High volume of vulnerabilities 26%
- Lack of automation 26%
- Business continuity 26%

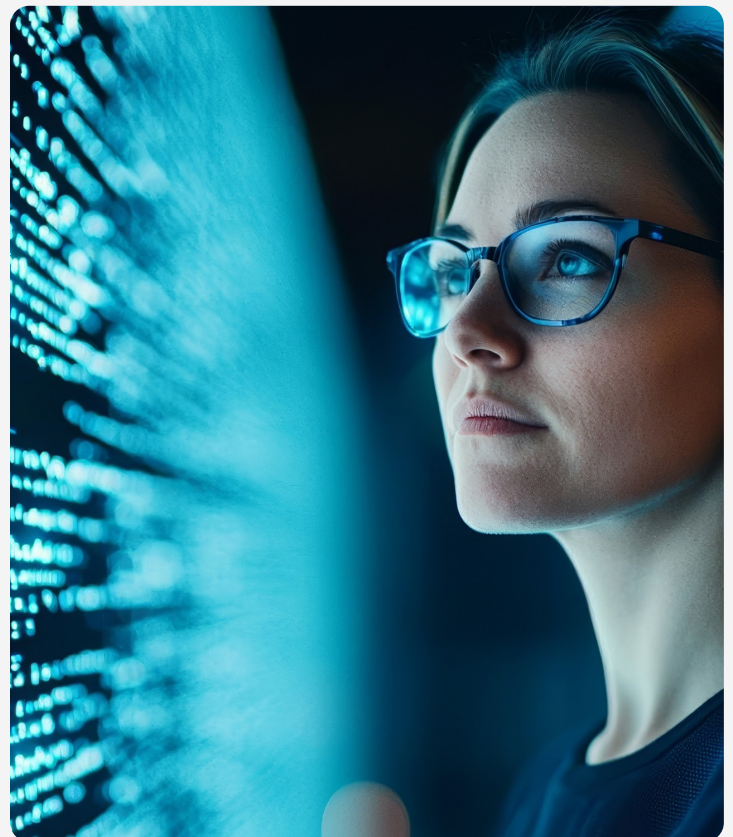
Connected, trustworthy data has the potential to transform how organizations identify and mitigate security risks. When asked what they would most like to improve in their organization's exposure management, leaders say prioritization accuracy (58%) and automated remediation (55%). By incorporating unified data, organizations could streamline their vulnerability management and proactively address vulnerabilities before they escalate into critical threats.

Deep Dive on AI and Automated Remediation

The most common applications of AI and automation in vulnerability and exposure management are automated patching and remediation (42%), automated vulnerability scanning (40%), and AI-driven prioritization of vulnerabilities based on risk (40%). The incorporation of these technologies enables faster identification of potential gaps, helping organizations stay ahead of threats and reduce the risk of exploitation.

Despite these advancements, the **top challenges organizations face in incorporating AI and automation into vulnerability and exposure management are integration issues with existing systems and tools (38%) and data privacy or security concerns (36%).** By ensuring that data is accessible and accurate across security systems, organizations can lay the groundwork for the seamless adoption of AI and automation.

Although there are challenges to address, 31% of IT and security leaders say that AI and automation will become more integrated into all aspects of security management, and 27% say it will enhance decision-making but still require human oversight to ensure effective implementation.



The Path *Forward*

Bridging the gap between readiness to act and effective execution requires a shift to continuous, risk-based security management. This approach allows organizations to move beyond periodic checks and reactive fixes. By continuously discovering assets, prioritizing exposures based on real business risk, and validating remediation efforts, organizations can focus their resources where they matter most.

However, both proactive and reactive strategies depend on having accurate and trustworthy data. Without it, prioritization falters and exposures remain unaddressed. Investing in a strong data foundation and automation is key for enabling real-time visibility and smarter decision-making. Ultimately, investments in these areas will allow organizations to stay ahead of threats and build long-lasting cyber resilience.

About the Study

Axonius commissioned TEAM LEWIS Research to conduct an online survey of 500 security and IT leaders (400 cybersecurity professionals and 100 IT professionals). Respondents were in the United States and held titles of director level or above at organizations with 500+ employees. All respondents had decision-making authority for security and / or IT-related decisions. Data was collected from March 28 to April 2, 2025.

About Axonius

Axonius transforms asset intelligence into intelligent action. With the Axonius Asset Cloud, customers preemptively tackle high-risk and hard-to-spot threat exposures, misconfigurations, and overspending. The integrated platform brings together data from every system in an organization's IT infrastructure to optimize mission-critical risk, performance, and cost measures via actionable intelligence. Covering cyber assets, software, SaaS applications, identities, vulnerabilities, infrastructure, and more, Axonius is the one place to go for Security, IT, and GRC teams to continuously drive actionability across the organization. Cited as one of the fastest-growing cybersecurity startups, with accolades from CNBC, Forbes, and Fortune, Axonius covers the lifecycle of millions of assets for leading customers across industries and around the world.

Bring truth to action with Axonius.
Learn more at www.axonius.com.

Axonius transforms asset intelligence into intelligent action. With the Axonius Asset Cloud, customers preemptively tackle hard-to-spot threat exposures, misconfigurations, and operational inefficiencies across their entire technology footprint – all in one place.

The actionability era of cybersecurity is here. Learn more at www.axonius.com