SPONSORED CONTENT | WHITE PAPER

Market Pulse

Bridging the resilience gap across public and private sectors

CSO

SPONSORED BY

splunk> a CISCO company

Market Pulse

Digital resilience has evolved from a best practice to a necessity for organizations navigating today's complex threat landscape. Despite advancements in cybersecurity, recent Foundry research reveals significant gaps in preparedness and response capabilities. Alarmingly, even among the most cyber savvy organizations, only 33% are confident they could recover from a cyber incident within 12 hours, underscoring the need for urgent action to close these gaps.

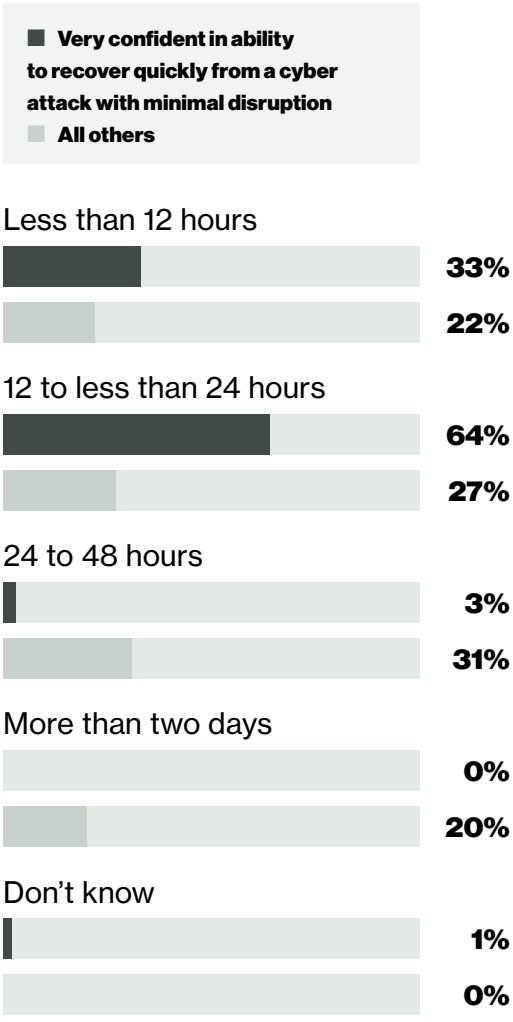
This white paper explores key findings and provides actionable strategies to enhance digital resilience. From foundational practices such as "cyber veggies" to leveraging cutting-edge technologies such as artificial intelligence (AI), organizations can build robust systems that ensure rapid recovery, minimize downtime, and maintain operational continuity.

The confidence gap

On behalf of Splunk, in October 2024, Foundry surveyed 207 senior IT and data security decision-makers at organizations averaging more than 5,000 employees. Among the key findings is a disparity between recovery expectations and preparedness.

Even among the respondents who rated themselves "very confident" in their ability to recover from a cyber attack, only 33% believe they can be back in operation within 12 hours and more than 50% believe it would take longer than 24 hours to recover, pointing to a significant gap in incident response capabilities (see Figure 1). Although the importance of rapid recovery is widely recognized, many organizations lack

Figure 1 | How quickly can your organization be back in operation after a cybersecurity outage?



SOURCE: FOUNDRY

Market Pulse

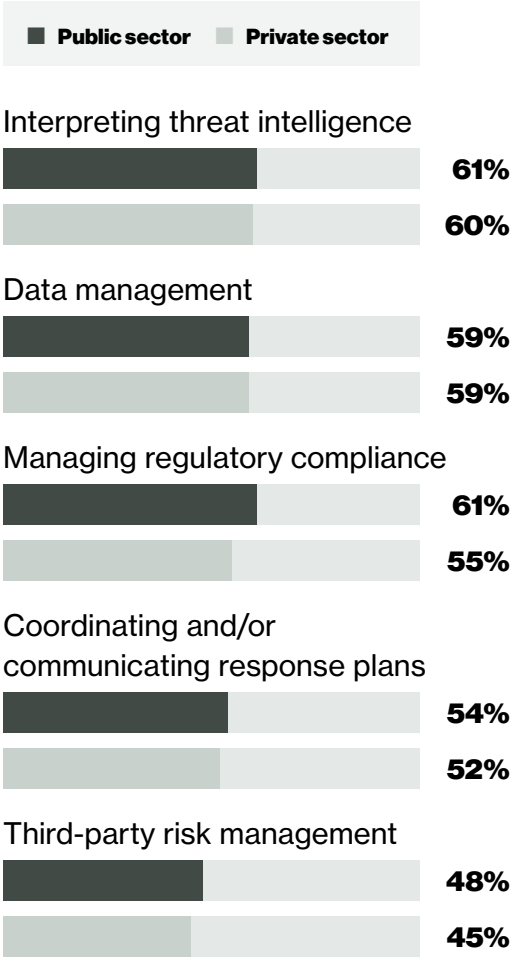
the tools and processes necessary to achieve it.

As cyber attacks grow in sophistication, the need for robust resilience planning becomes more critical. Building resilience requires investments in scalable technologies, enhanced incident response protocols, and systems designed to minimize operational disruptions and support swift recovery when incidents occur.

The survey highlights sectoral disparities, with private sector organizations reporting slightly higher confidence and preparedness (53% vs. 43%) than their public sector counterparts (47% vs. 44%). However, both sectors face significant resource constraints. Among public sector organizations, 47% indicated their cybersecurity budgets are insufficient to meet priorities, while 35% of their private sector counterparts feel the same, further compounding the challenges in achieving rapid recovery.

Public and private sector respondents largely agreed on the top challenges they face in building digital resilience, with interpreting threat intelligence and data management leading the pack (see Figure 2).

Figure 2 | Top challenges in building digital resilience



SOURCE: FOUNDRY

Cyber veggies: The foundation of resilience

The survey confirmed that a strong foundation in core cybersecurity practices is essential for operational stability. Practices such as patch management, incident response planning, and continuous threat monitoring – collectively referred to as "cyber

Market Pulse

veggies" – are critical in mitigating risks and enabling resilience.

The research shows a strong correlation between consistent implementation of these practices and preparedness, with 88% of organizations that follow strong cyber hygiene rating their ability to be resilient as 9 or 10 on a 10-point scale, compared to just 33% of those with inconsistent practices.

The survey also uncovered discrepancies between sectors in terms of preparedness:

- **Asset inventory.** Consistently addressed by 48% of private sector organizations, compared to 41% in the public sector
- **Multifactor authentication (MFA).** Adopted by 54% of private sector respondents, versus 40% in the public sector
- **Vulnerability and patch management.** Practiced by 49% of private sector organizations, compared to 39% in the public sector

Prioritizing cyber hygiene practices builds a foundation for advanced resilience strategies, enabling organizations to adapt to increasingly complex threats.

Sample cyber veggies

- **Patch management** to reduce vulnerabilities
- **Data backup and recovery protocols** to ensure availability during disruptions
- **Incident response planning** that is tested regularly
- **Continuous monitoring and threat intelligence** for real-time threat detection

Market Pulse

The role of technology in digital resilience

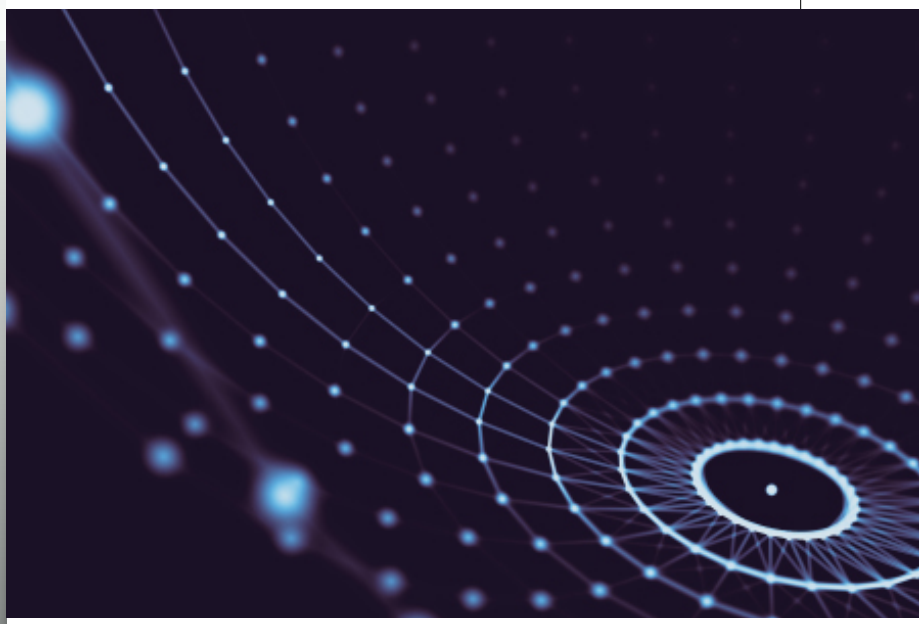
Secure data management and zero trust

Secure data management remains a cornerstone of digital resilience, with 31% of surveyed organizations ranking it as a top priority. In an era of increasing data breaches, the implementation of zero-trust architecture has emerged as a key strategy. This model requires strict identity verification for system access, ensuring that sensitive information remains protected, even in compromised environments.

Key best practices for secure data management include:

- **Data encryption.** Encrypting data both at rest and in transit significantly mitigates exposure during breaches. This step is foundational for safeguarding sensitive assets in today's interconnected environments.
- **Automating data classification.** Automating the classification of data helps enforce tailored security policies and ensures that sensitive information is protected at the appropriate level.
- **Regular access control audits.** Conducting routine audits ensures compliance, identifies security gaps, and supports adherence to evolving regulations.

Organizations that adopt these practices report enhanced agility and resilience, enabling them to adapt swiftly to new cybersecurity challenges. Investments in related areas further underscore their importance: 50% of respondents plan to prioritize advanced threat intelligence solutions, and 46% aim to enhance their cybersecurity monitoring capabilities.



Leveraging AI and automation

AI and automation are at the forefront of reshaping

Market Pulse

digital resilience strategies, enabling organizations to address resource gaps and enhance operational efficiency. According to the research, 99% of all organizations plan to integrate AI into their cybersecurity efforts in the coming year, with 64% intending to rely on it significantly. These technologies provide organizations with the ability to process vast amounts of data in real time, enabling faster and more accurate threat detection while optimizing incident response capabilities.

Key applications of AI and automation include:

- **Predictive analytics.** Used by 41% of organizations, predictive analytics helps companies anticipate system failures and prioritize recovery efforts while providing actionable insights for preemptive threat mitigation.

- **Automated patch management.** Automation streamlines vulnerability management, reducing exposure by ensuring regular updates. This practice is particularly critical in the public sector, where 29% of organizations prioritize it, compared to 16% in the private sector.

- **Simulated disaster recovery.** Organizations are leveraging AI-driven disaster recovery simulations to refine workflows, identify bottlenecks, and optimize response strategies, significantly enhancing their preparedness for real-world incidents.

AI and automation applications act as force multipliers, reducing human resource strain and enabling faster decision-making in the face of evolving cyber threats. By integrating AI-driven solutions into their operations, organizations can not only respond to threats more efficiently but also shift from reactive to proactive resilience strategies.

Expanding the impact

By combining AI, automation, and robust data management practices, organizations can address challenges that previously hindered digital resilience. These technologies not only strengthen defenses but also create scalable, adaptable frameworks that prepare organizations for the ever-changing threat landscape. As the adoption of AI and automation increases, the potential for these tools to transform resilience strategies will continue to grow, positioning organizations to stay ahead of both known and emerging threats.

Market Pulse

Overcoming challenges in resilience

Bridging the confidence/ preparedness gap

Confidence and preparedness are closely linked, with 69% of respondents expressing confidence in their understanding of digital resilience. However, only 44% of decision-makers rated their actual preparedness as high, highlighting a significant gap between understanding and readiness.

Simulation exercises such as table-top drills are vital for refining incident response protocols, improving team coordination, and building the muscle memory needed to handle real-world threats. Organizations must also prioritize continuous learning to adapt to evolving risks.

Cost-effective and scalable solutions

But budget constraints remain a significant challenge, with 41% of respondents citing insufficient funding. Public sector organizations are disproportionately affected (47%), compared to private sector counterparts (35%).

Scalable solutions, such as cloud-based tools and open source technologies, can address these financial limitations.

Planned investments in resilience-focused technologies include:

- Threat intelligence solutions (50%)
- Cybersecurity monitoring (46%)
- Generative AI tools (43%)

Automation further supports efficiency by streamlining repetitive tasks such as patch management, enabling resource-constrained teams to achieve greater resilience.

Looking ahead and recommendations

AI and the future of resilience

AI continues to redefine how organizations approach digital resilience by automating complex processes, analyzing vast amounts of data in real time, and providing predictive insights. However, the research shows many organizations are still in the early stages of implementation. For AI to achieve its full potential, businesses must focus on well-defined use cases that align with their broader resilience objectives.

Market Pulse

Key opportunities for AI adoption include:

- **Enhancing threat detection.** AI can identify patterns and anomalies that human teams might overlook, enabling faster identification of emerging threats.
- **Automating incident response.** Streamlined workflows driven by AI can reduce response times and ensure consistency in addressing incidents.
- **Predictive analytics.** By leveraging AI's ability to analyze patterns and historical data, organizations can identify potential impending system failures or vulnerabilities. AI models can process vast amounts of data, detect subtle anomalies, and forecast future risks, enabling companies to take proactive measures to address issues before they escalate.

For AI adoption to succeed, organizations should prioritize training for teams on integrating AI into existing workflows and invest in scalable solutions that can grow alongside their evolving needs. By fostering a culture of innovation and adaptability, businesses can ensure that AI becomes a transformative tool in their resilience strategies.

Achieving the 12-hour recovery threshold

Reaching the 12-hour recovery threshold requires a holistic approach that blends technology, operational discipline, and regular system evaluations. Although only 33% of organizations currently believe they could recover within this timeframe, improving this metric is achievable through strategic investments and process enhancements.

Steps to decrease recovery times include:

- **Technology integration.** Invest in advanced threat detection and incident response tools that can streamline the recovery process. Automation plays a critical role in expediting tasks such as data restoration and system configuration.
- **Scenario-based training.** Regular disaster recovery simulations, including red- and blue-team exercises, help teams refine their protocols and identify potential bottlenecks before they arise during a real-world incident.

Market Pulse

- **Continuous improvement.** Organizations should conduct regular audits of their recovery plans and iterate on findings to address weaknesses. Feedback loops are critical to adapting plans to align with the latest threat intelligence.

- **Cross-functional collaboration.** Building alignment across IT, security, and operations teams ensures that recovery efforts are cohesive and efficient. Shared accountability fosters faster decision-making and execution.

Building resilience for the future

The insights from this research emphasize the need for comprehensive digital resilience strategies. By prioritizing foundational practices, adopting AI-driven solutions, and fostering a culture of continuous improvement, organizations can bridge recovery gaps, protect critical assets, and achieve greater operational stability.

To learn more about Splunk's solutions for building resilience, contact us for a consultation or visit: www.splunk.com/en_us/solutions/digital-resilience.html.