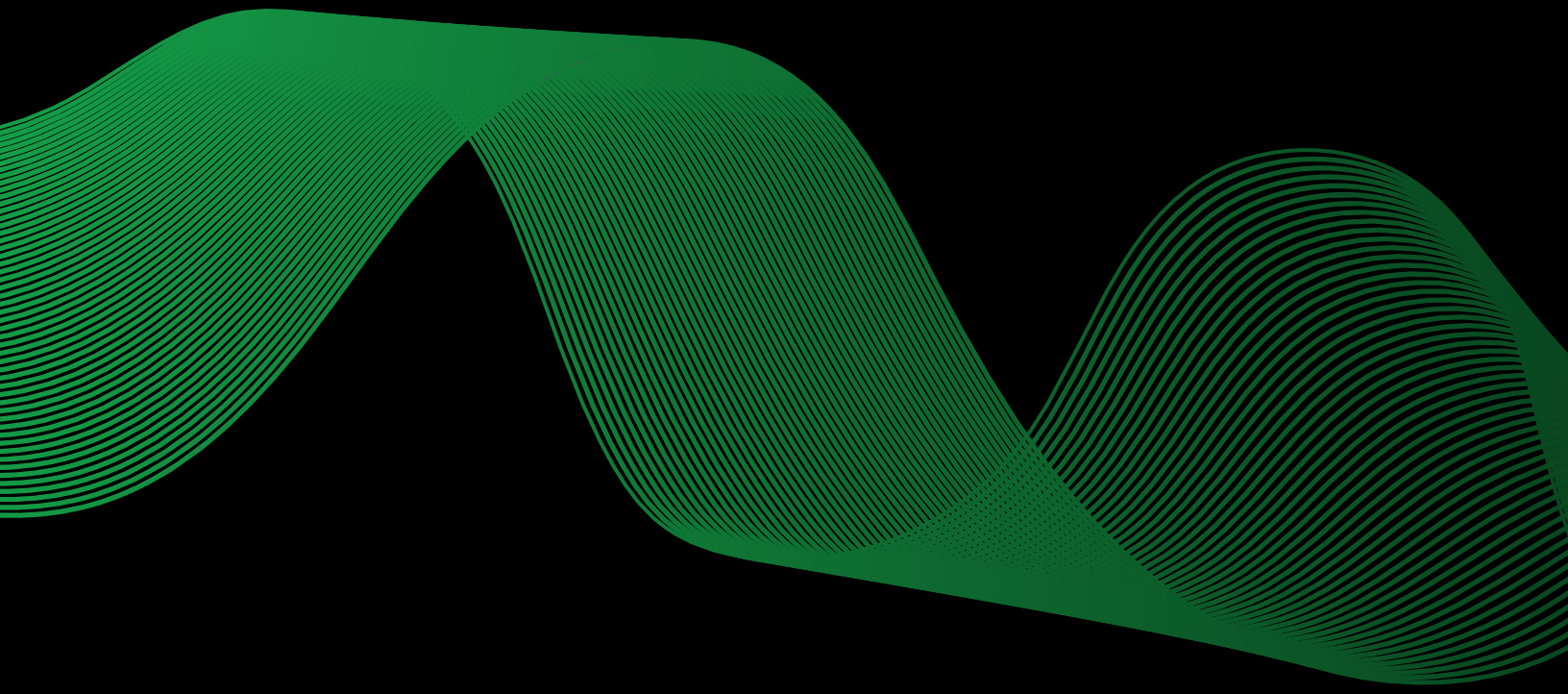
2025

Resilience Risk Index

You Can't Handle the Breach

New Report Reveals Most Enterprises Are Unprepared to Prevent or Recover from Cyberattacks



ABSOLUTE®

Contents

Executive Summary 3

Endpoint Compliance and Resilience 7

Software Vulnerability Resilience 13

Endpoint and Data Protection Resilience 15

AI Readiness and Resilience 17

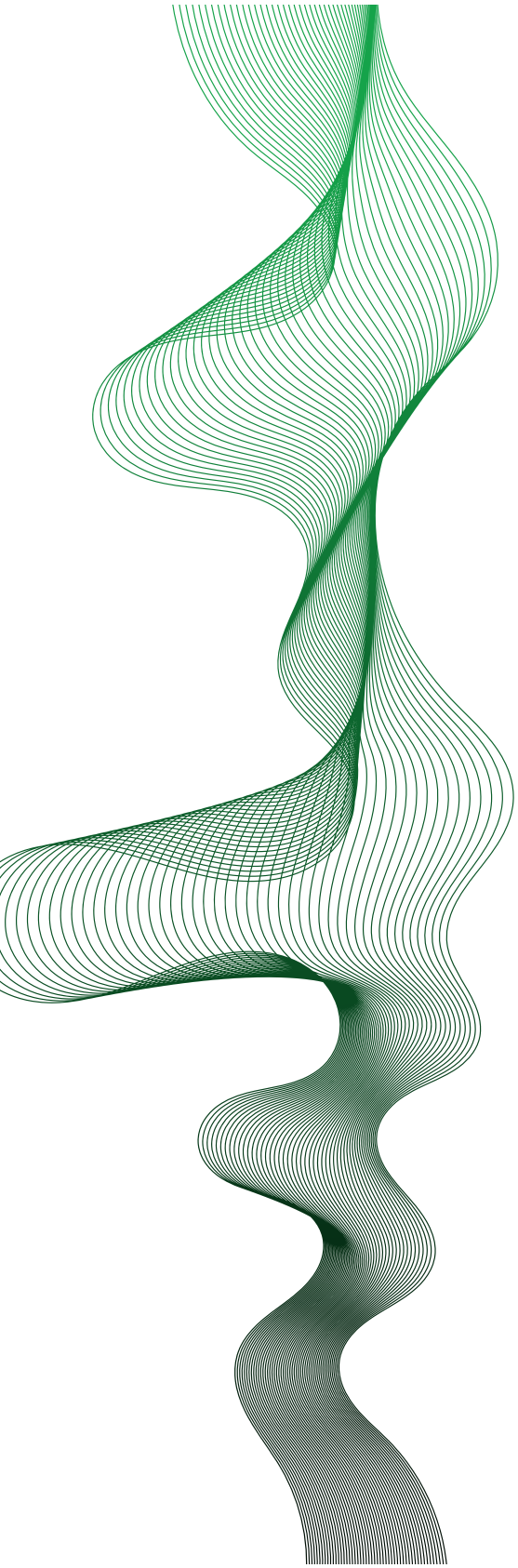
AI Visibility and Control Resilience 19

Conclusion 21

How Absolute Helps 22

About Absolute Security 24

Executive Summary



By 2028, IT spending will exceed $5 trillion,[1] with cybersecurity accounting for close to $300 billion.[2] Most of these investments are necessary to reduce risk, but none are fool proof when it comes to stopping cybercriminals. Nor do they address the risk created by rapidly increasing complexity that software and hardware sprawl are driving.

Despite these investments, security-related losses are on the rise. Some estimates show that by 2028, cybercrime is expected to cost the global economy trillions of dollars in losses annually, far outpacing the growth of enterprise security investments. In 2025, ransomware alone is expected to cause as much as $57 billion in damages,[3] with Chief Information Security Officers (CISOs) now reporting the average cost of a ransomware attack on their organization has reached $4.5 million per incident.[4]

The consequences of a significantly disruptive event go far beyond just the devices and systems that are impacted. When contemplating the total negative effect that an incident can have in the face of a disruption, companies need to consider the broader picture. Organizations need to be clear about what the consequences to their core business would be if employees are unable to connect or complete transactions. They should also assess the potential for regulatory and legal penalties. It's equally important to consider the reputational damage and loss of customer trust that could follow. Ultimately, organizations must prepare for the possibility of complete business failure if recovery efforts fall short. The attacks on Travelex, Stoli Vodka, and Johnson Controls show how one significant ransomware event and the failure to quickly recover can contribute to the long-term impairment of a business.

When thinking about the supply chain risk of the security ecosystem it is important to understand that cybercrime is not the only costly disruption that CISOs and other IT leaders must consider. The accelerated investment in prevention and detection solutions has added to the inherent complexity of managing these devices, making it even more difficult to maintain the security posture they are deployed to support. Whether it is a failure to update software, security supply chain compromise, or a bad actor taking advantage of a key control vulnerability, the result may be the same: your organization coming to a total standstill.

The July 2024 CrowdStrike BSOD incident, while not a malicious cyberattack, was a very real example of what the impact of a security supply chain attack could be. This incident alone is estimated to have shut down more than eight million Windows endpoints[5] and caused businesses caught in the fallout to have lost as much as $5 billion.[6] This is only a single example of how quickly and easily things can go wrong, regardless of the root cause. While CrowdStrike is known as a leader in its category, the disruption shows how organizations using vendors with even a low probability of failure need to be prepared for the inevitable.

Today, we are faced with a combination of technical failures, vulnerabilities, ineffective compensating controls, and growing attacks. This means that organizations will eventually see their environments hit with a threat, breach, or incident that could negatively impact their operations and bottom lines. This report highlights how a lack of resilience is causing organizations to struggle to keep top-ranked security solutions fully operational.

CISOs and IT leaders who have accepted this reality are driving the emergence of a new strategic imperative – Resilience.[7] By taking proactive steps to embed Resilience into their infrastructures, they are positioning themselves to get ahead of problems and to swiftly recover when incidents and attacks inevitably occur.

However, as the scale and severity of today's threats and disruptions expands, from mass ransomware attacks to software failures, the conventional notion of Resilience may already be obsolete. We are now at a point where organizations need something more – **Extreme Resilience.**

Absolute Security defines Extreme Resilience as having full visibility into the inherent risks in every layer of your security architecture — combined with a plan for resilient operations, automated remediation, and rapid recovery. This approach ensures your business stays operational, protected against threats, and able to quickly restore continuity after IT incidents, technical disruptions, ransomware attacks, and other threats.

We recognize that defining Extreme Resilience is only half the battle and that endpoint security is one critical component of an enterprise-wide resilience plan.

The Absolute Security Resilience Risk Index 2025 is designed to help CISOs and IT leaders understand what Extreme Resilience is, what the top barriers to achieving it are, and how to overcome the related challenges.

With insights into anonymized telemetry from more than 15 million enterprise PCs, this year's analysis identified five key areas where maintaining Resilience merits industry attention. It reveals the risks these failures represent and proposes strategies and tools that can be used to enforce Resilience across your IT and security stacks.

Five top findings that significantly impact resilience in 2025:

1. **Endpoint Compliance and Resilience**
   Across all PCs deployed, 22% of the time, critical endpoint security controls fail to maintain compliance with the organizations' applied security and performance policies. This increases the risk of breaches, ransomware incidents, and IT disruptions.

2. **Software Vulnerability Resilience**
   Windows 10 & 11 vulnerability patching is delayed an average of 56 days. This opens an extended window for attackers to execute exploits and for software to continually crash, malfunction, and freeze systems.

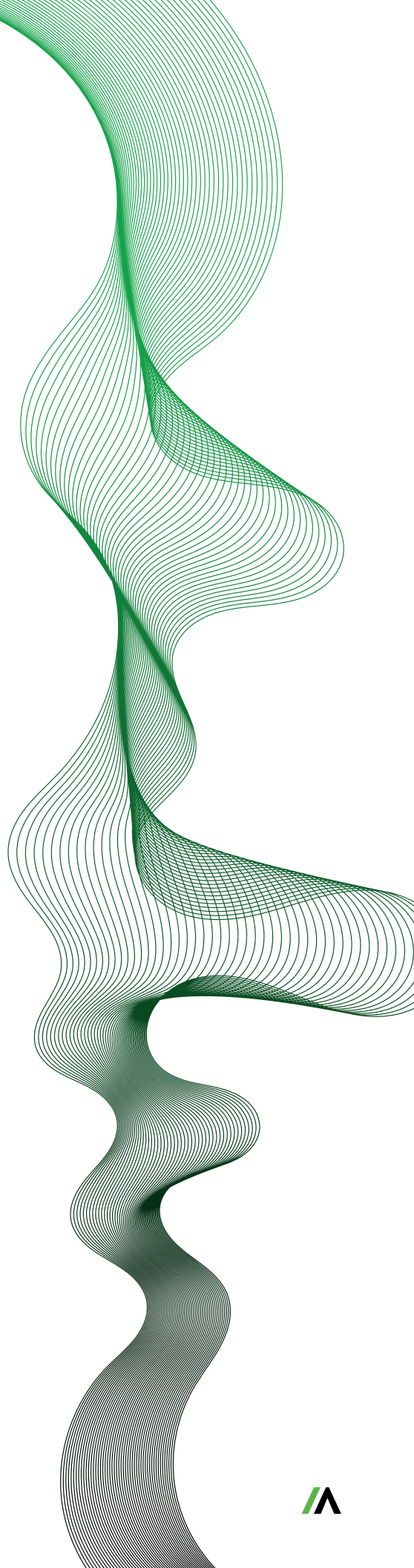
3. **Endpoint and Data Protection Resilience**
   Despite policies in place, 35% of PCs are not encrypted, 18% store sensitive data, and 26% are unaccounted for. This leaves them vulnerable to unauthorized access, susceptible to data breaches, and subject to compliance violations.

4. **AI Readiness and Resilience**
   AI capabilities can dramatically help the cyber community protect endpoints, though an aging PC population may hinder the ability to adopt these new tools. While the impending device refresh cycle could cause complexity, until the requirements for AI and the deployment of AI ready PCs converge, businesses must be selective about where they are able to apply these new capabilities.

5. **AI Visibility and Control Resilience**
   Shadow AI is growing, with PCs logging millions of visits to generative AI sites, including DeepSeek. This is causing CISOs to lose oversight of where and how data is being shared and how frequently employees are visiting non-authorized websites and using non-sanctioned AI applications.

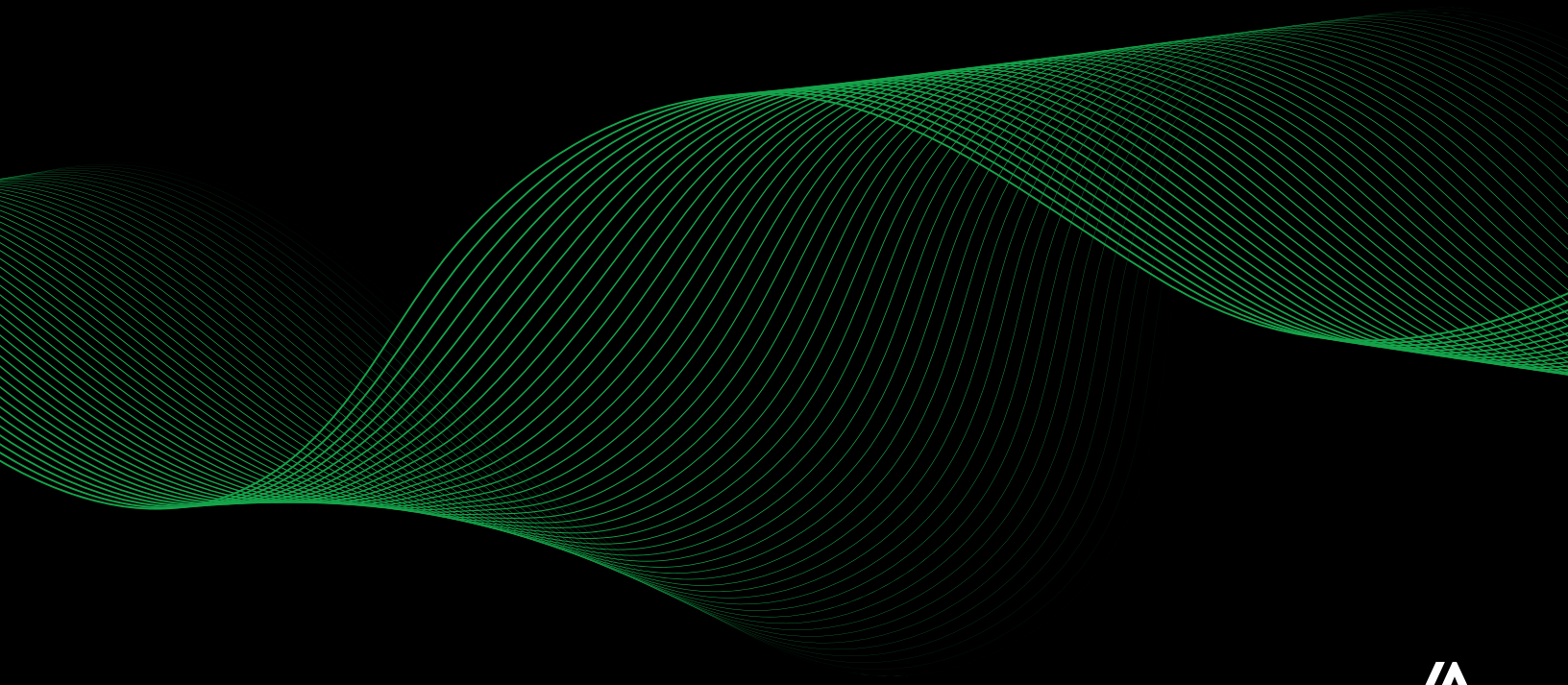
These findings reveal that enterprises are not prepared to defend against or recover from the impact of a breach or IT incident. There is now an urgent need for CISOs to move beyond legacy reactive security and IT practices. Enterprises must embed Extreme Resilience into their infrastructures to proactively mitigate risk, sustain operations, manage growing complexity, and adapt to an intensifying threat landscape.

To build a winning strategy, CISOs must look beyond just stopping attacks. They must also confront the hidden risks posed by fragile software, expanding IT sprawl, and the operational challenges that arise from managing increasingly complex environments. This report outlines where significant gaps exist today and provides details on how embedded Resilience closes them.



Extreme Resilience

Having full visibility into the inherent risks in every layer of your security architecture — combined with a plan for resilient operations, automated remediation, and rapid recovery. This approach ensures your business stays operational, protected against threats, and able to quickly restore continuity after IT incidents, technical disruptions, ransomware attacks, and other threats.



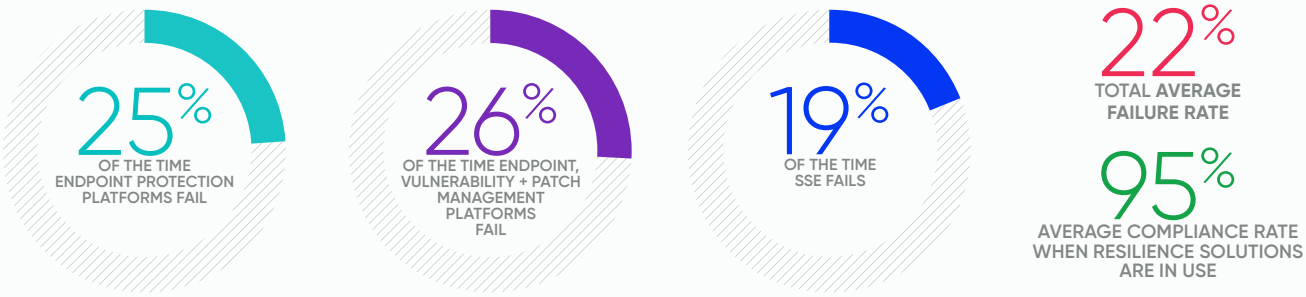
FINDING 1

Endpoint Compliance and Resilience

Across all PCs deployed, 22% of the time, organizations fail to keep critical endpoint security controls compliant with their security and performance policies.* This increases the risk of breaches, ransomware incidents, and IT disruptions. In contrast, when underpinned by resilience solutions that force these controls to remain operational, they maintain a benchmark performance rate of 95%.

FIGURE 1

Overall and Category Compliance failure rates



*** Internal Security & Performance Compliance Criteria Measured are:**

- Ensure application is present on the device
- Ensure application version is correct, as specified by customer policy
- Verify application is running as expected
- Verify the application is properly signed and has not been tampered with

Endpoint Security Controls assessed include Endpoint Protection Platforms (EPP, EDR, XDR), Security Service Edge (SSE), and Endpoint, Vulnerability and Patch Management Platforms. Although there are many such solutions in use, we focused on several identified as leaders in top industry analyst reports.

Vendors Evaluated Include: Cisco, CrowdStrike, Fortinet, Ivanti, ManageEngine, Microsoft, Netskope, Palo Alto Networks, Qualys, Rapid7, SentinelOne, Sophos, Tanium, Tenable, Trend Micro, and Zscaler. Vendors are listed in alphabetical order and do not correspond with the numbers in the images.

Figures 2, 3, & 4:

Orange shows the percentage of time that each endpoint security control maintains compliance with security and performance policies. Red shows the percentage of time these controls fail to maintain compliance.

FIGURE 2

Endpoint Protection Platform (EPP/XDR/EDR) Assessment

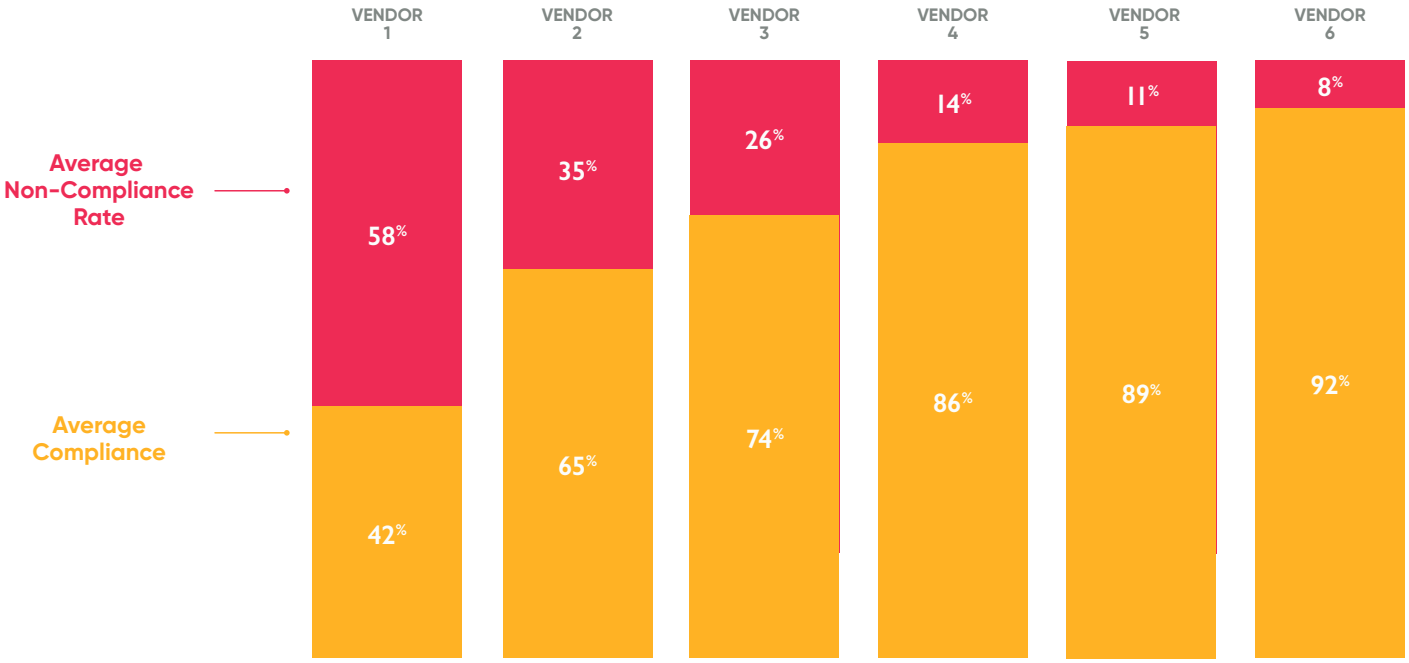


FIGURE 3

Security Service Edge (SSE) Vendor Assessment

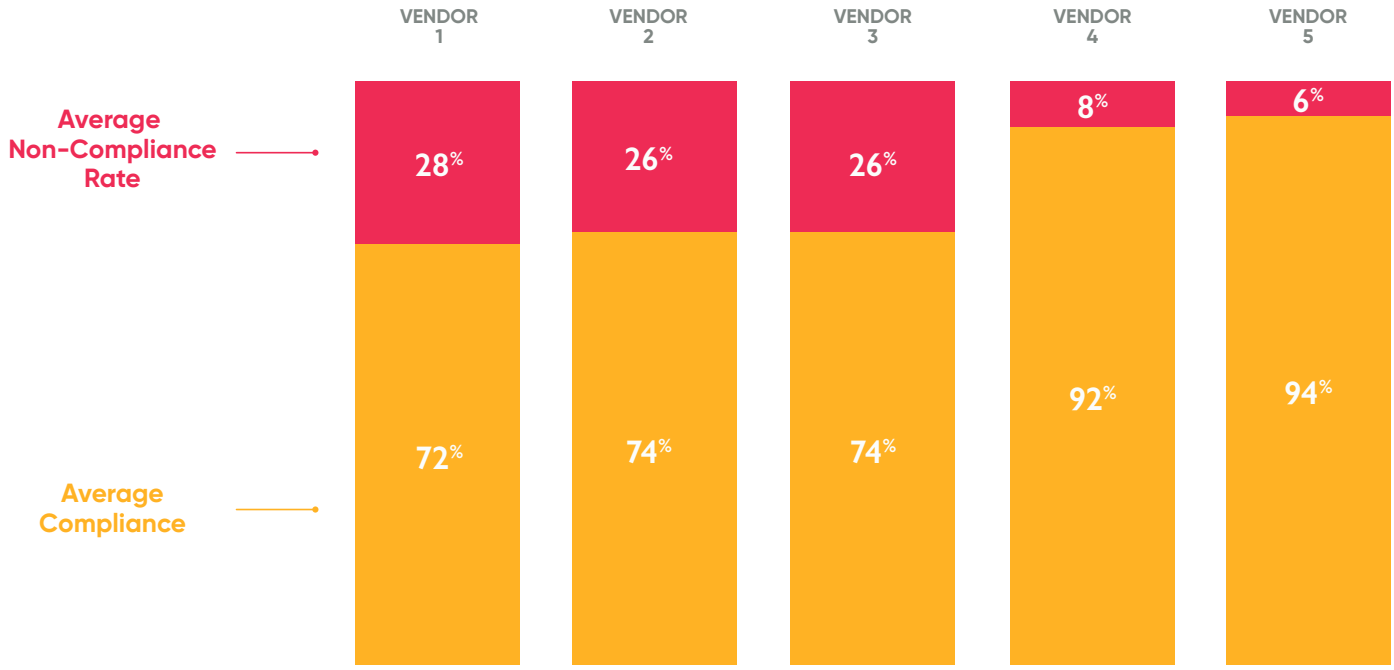
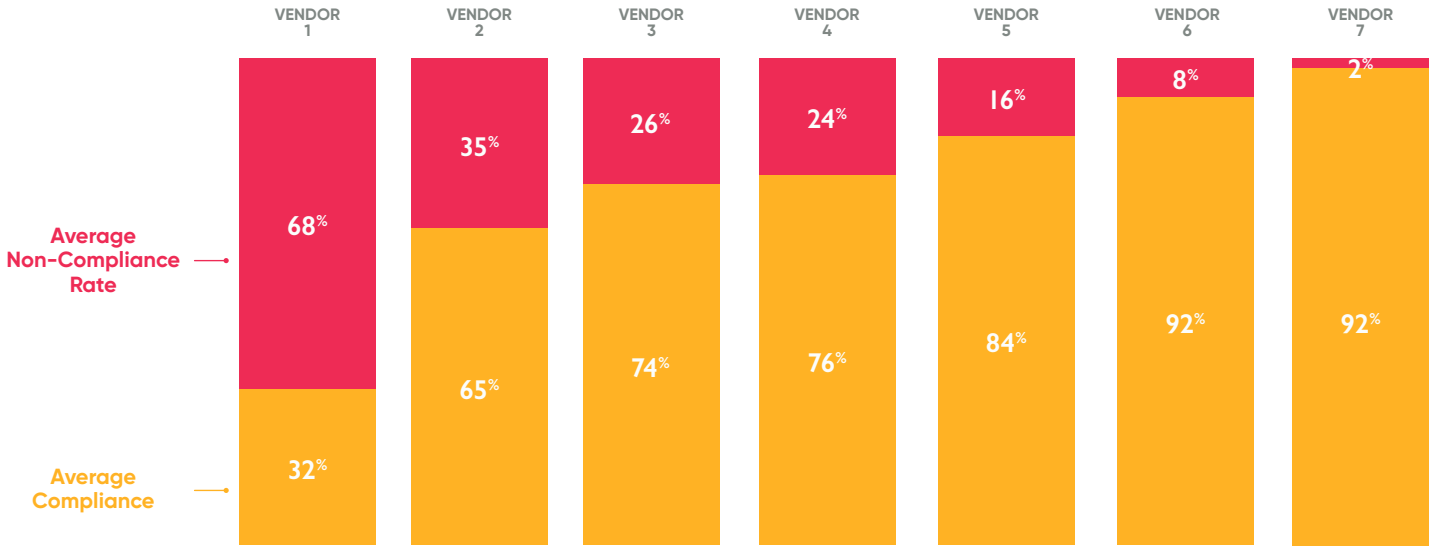


FIGURE 4

Endpoint, Vulnerability and Patch Management Platforms





The Risk

These security and risk controls are the first line of defense and maintenance at the edge of your network. If they are unable to maintain compliance with your set security policies, for any reason – whether it be a user issue, bad actor, or missed update – it makes catching vulnerabilities and blocking threats such as ransomware even more difficult.



Mitigation

Underpin your endpoint security, management, and access controls with an embedded solution that can enforce resilience across all your deployed hardware and software. An effective solution will provide control, visibility, health status monitoring, and automated and immediate restoration at scale for all your endpoints, operating systems (OS), security controls, and productivity applications.

SECURITY SPOTLIGHT:

The MITRE ATT&CK framework provides real-world examples of why non-compliant endpoint security controls present a major risk. Since 2020, MITRE has listed "Defense Evasion"[8] and "Impair Defenses"[9] as known tactics threat actors use to compromise networks. According to MITRE, adversaries may use both to disable defenses and avoid detection to launch their attacks, deploy their tools, spread ransomware, and to execute other nefarious activities. Having a solution in place that can detect and alert you when your endpoint security controls are acting in a suspicious or unhealthy manner, or missing from a device, could mean the difference between detecting or missing an intrusion.

Concentration of Risk:
The More Prevalent a Solution, The Broader Potential Impact

Concentration of Risk is an additional factor Absolute Security has identified that organizations must now consider, as it has the potential to exacerbate an incident. To demonstrate this concept, we considered how risk changes across enterprises within an assessed security category. Orange shows the percentage of time that end users were able to keep their endpoint security tools compliant with their policies. Red shows the percentage of time they fell out of compliance. The width of the columns shows the level of compliance enforced across the PCs assessed, by percentage.

FIGURE 5
Concentration of Risk

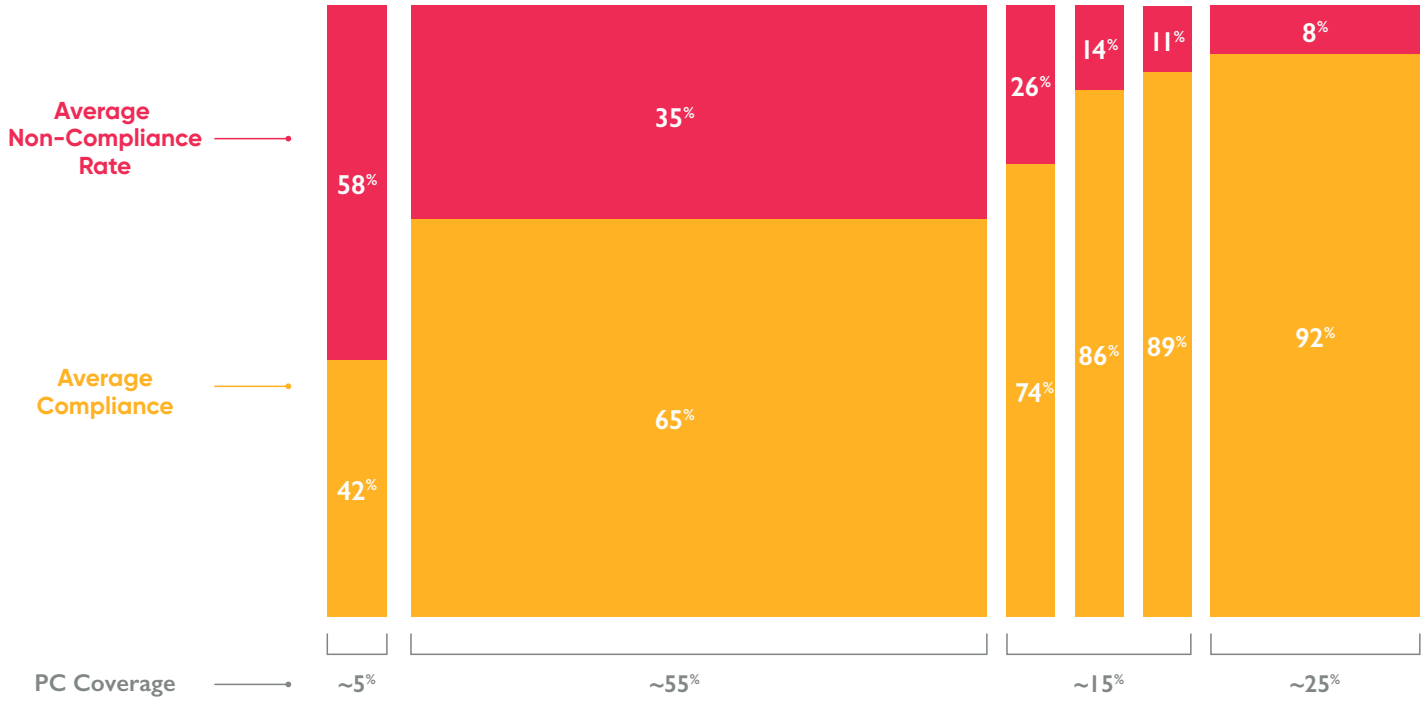


Figure 5 shows that 5 percent of PCs are protected with tools that organizations fail to keep compliant nearly 60 percent of the time, while organizations are able to maintain the highest level of compliance observed for only 25 percent of PCs. However, if a technical incident or compromise were to strike one of the solutions in the 25 percent band, five times as many PCs would be impacted compared to an incident affecting PCs in the lower-performing band. This Concentration of Risk shows that no organization can afford to be without technologies that enforce resilience and enable rapid recovery. Some solutions may maintain compliance better than others, but all remain subject to multiple risk factors.

What Goes Down, Must Come Up

Whether an abrupt shutdown is caused by a cyberattack or control failure, an organization must fully recover and restore operations as quickly as possible. In the case of the CrowdStrike event, customers struggled to locate impacted devices, remediation was manual, and many customers reported that it took days if not weeks or longer to complete full restoration. This would be representative of recovery challenges for other large cyber events. When such a crisis occurs, having the ability to quickly connect with and restore impacted devices will be essential to every organization's ability to restore business continuity.

Remediation

When systems go down, regardless of the cause, be prepared with a remote capability that can restore every PC to a healthy state, at scale, under any failure condition, without having to wait for the vendor to issue a mitigation. Most importantly, when it comes to Windows PC deployments, use a solution that works even when the OS and applications are corrupt, tampered with, or crashing.

RECOVERY IN PERSPECTIVE:

Based on available industry data, spanning multiple organizations that track shipments, it can be estimated that there are as many as a billion endpoint devices in use by enterprises today. Imagine if an EPP vendor with a low rate of non-compliance and a high Concentration of Risk holding just 20 percent of the market share were to experience a BSOD incident or other paralyzing cyberattack. If this vendor was deployed across 20 percent of all PCs in use, then as many as 200 million endpoints could go down as a result of the incident. Having a low rate of non-compliance in this case would not be what matters, having an effective recovery capacity would be paramount.

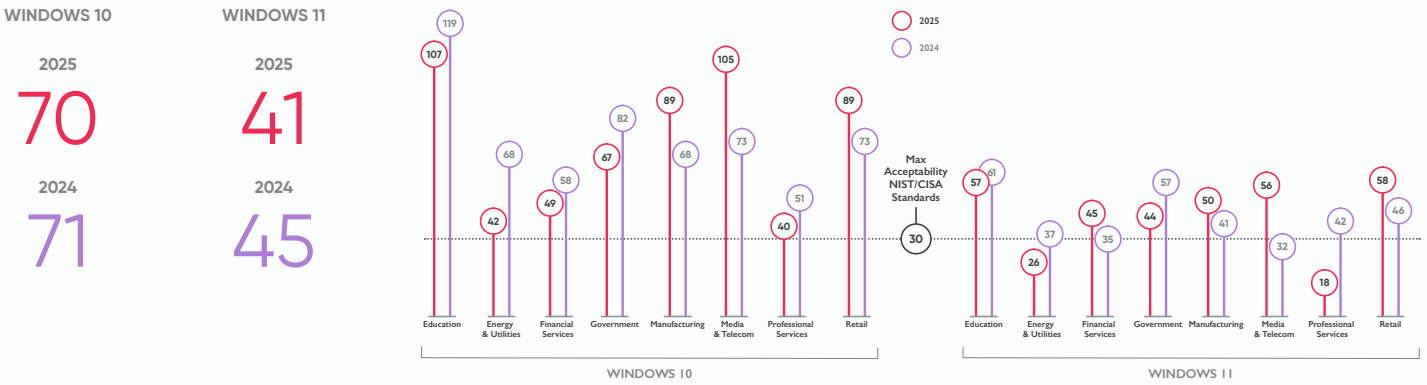
FINDING 2

Software Vulnerability Resilience

Windows 10 & 11 vulnerability patching is delayed an average of 56 days, opening an extended window for attackers to execute exploits and for software to continually crash, malfunction, and freeze systems.

FIGURE 6

Organizations are Falling Behind in Patching



Organizations set their own patching schedules, with factors such as available resources, risk tolerance, and regulatory compliance influencing policies and decisions. Industry guidance on vulnerability scanning, remediation, and patch management is available from numerous sources, with the Cybersecurity and Infrastructure Security Agency (CISA) recommending that patching should not exceed 30 days.[10] Since our 2024 assessment, most industries have improved their average patch time, with Retail, Manufacturing, and Media & Telecom worsening.

The Risk

Most successful cyberattacks find a foothold via unpatched software[11] including 32% of all ransomware attacks.[12] Currently, there are more than 52,000 Common Vulnerabilities and Exposures (CVEs).[13] In 2024, 768 CVEs were publicly reported as being exploited in the wild, a 20% increase over 2023.[14] At the time of publication, there were more than 3,000 Windows 10 vulnerabilities[15] and 580 known for Windows 11.[16]

Research shows that attackers exploit CVEs quickly, sometimes within 24 hours[17] of being made public. Gartner reports that since 2021, it takes only seven days for a vulnerability to be exploited. Despite what CISA says is an acceptable amount of time to apply a patch to a vulnerability, a top analyst recently informed Absolute Security during a discussion, "We frequently cover this in inquiry. The reality is that no time gap is acceptable."

Regardless of which industry finding represents a more accurate view of your experience, the consequences of unmitigated CVEs are undeniable – data breaches, ransomware attacks, and unwanted disruptions and incidents.

COMPLEXITY:

Microsoft continues to dominate the enterprise endpoint market, holding more than 72% of the market share. Windows 10 accounts for 54% with 11 accounting for 43%, with the remaining attributed to older versions.[18] When last reported, Microsoft had issued more than 10,000 patches since Patch Tuesday began. Absolute Security telemetry revealed in a previous Index that enterprise devices are weighed-down with as many as 67 apps, with some containing more than 100. When considering these factors along with the number of CVEs, patches, updates, and zero day vulnerabilities and exploits still unknown, it becomes clear that complexity alone will inevitably cause an issue in every organization.

Mitigation

CISOs and IT leaders should deploy solutions that can identify all impacted assets in their environment, prioritize vulnerabilities affecting deployed software, create and apply temporary mitigations ahead of official patches being made available, and automate as many of these tasks as possible.

Vulnerability and patch management solutions may not verify whether software assets are compliant with security policies or performing as expected, even when fully patched and correctly configured. These same tools may also fail to operate within compliance parameters, as revealed in figure 1. To avoid failures, underpin these software assets with solutions that enforce resilience to ensure they are always on, up to date, protected against vulnerabilities and threats, and fully operational.

FINDING 3

Endpoint and Data Protection Resilience

35% of PCs are not encrypted, 18% store sensitive data, and 26% are unaccounted for, leaving them vulnerable to unauthorized access, susceptible to data breaches, and subject to compliance violations.

Because Absolute Security is embedded in the hardware of more than 600 million endpoint devices, we can gain an unprecedented level of visibility across the millions of PCs we are activated in. In this year's report, we've added a view into how frequently devices lack encryption, hold sensitive data, or are simply unaccounted for.

FIGURE 7

Unprotected Devices

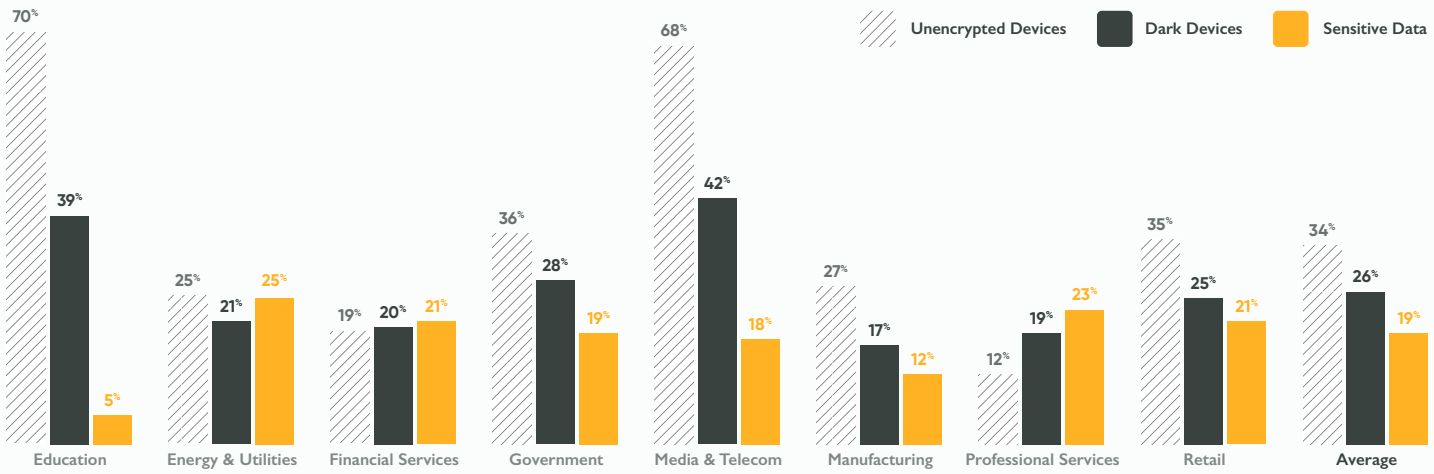


Figure 7 shows how frequently PCs are unencrypted, unaccounted for, and holding sensitive data.



The Risk

PCs that lack encryption are vulnerable to unauthorized access, potentially exposing sensitive data to breaches. Endpoints holding sensitive information amplify this risk. These machines represent prime targets for attackers seeking valuable data such as personally identifiable information (PII) or intellectual property (IP). Unaccounted for devices indicate a lack of visibility and control across organizational networks – a gap that could allow compromised or stolen devices to go unnoticed, providing attackers with prolonged access to data and systems. Collectively, these findings indicate that a substantial number of endpoints are at risk, undermining data integrity and organizational security. Without intervention, the likelihood of costly breaches, regulatory penalties, and reputational damage increases sharply.

Solutions deployed to mitigate these risks may fail to operate within acceptable compliance requirements, as revealed in figure 1. To avoid failures, underpin software and hardware assets with solutions that enforce resilience to ensure they are always on, up to date, protected against vulnerabilities and threats, and fully operational.



Mitigation

Organizations should enforce mandatory encryption across all PCs to ensure data remains secure, even on lost or stolen devices. They should conduct regular audits and deploy endpoint management tools that can address unaccounted for PCs to improve asset tracking and visibility. To limit exposure, PCs containing sensitive information need to be protected with data classification and access controls that enforce multi-factor authentication and least-privilege policies. An incident response plan should be in place to ensure swift action during breaches.

FINDING 4

AI Readiness and Resilience

In a recent Google report, 63 percent of security professionals believed that AI will enhance security measures. In a recent survey conducted by Absolute Security, CISOs shared that same enthusiasm for the impact of AI. However, the ability to use these capabilities on an aging PC population may slow down adoption. In our 2024 edition, we revealed that 92 percent of enterprise PCs were not ready for the growing AI wave, based on a review of several million PCs. This presumed that a minimum RAM capacity of 32GB[19] was needed to take advantage of AI benefits.

This year, an analysis of millions of devices still revealed a PC population unable to absorb these new capabilities broadly. With some newer reports showing that a minimum of 16GB may be acceptable,[20] we looked at the percentage of devices equipped with 16GB and 32GB.

FIGURE 8

AI Readiness is Lagging

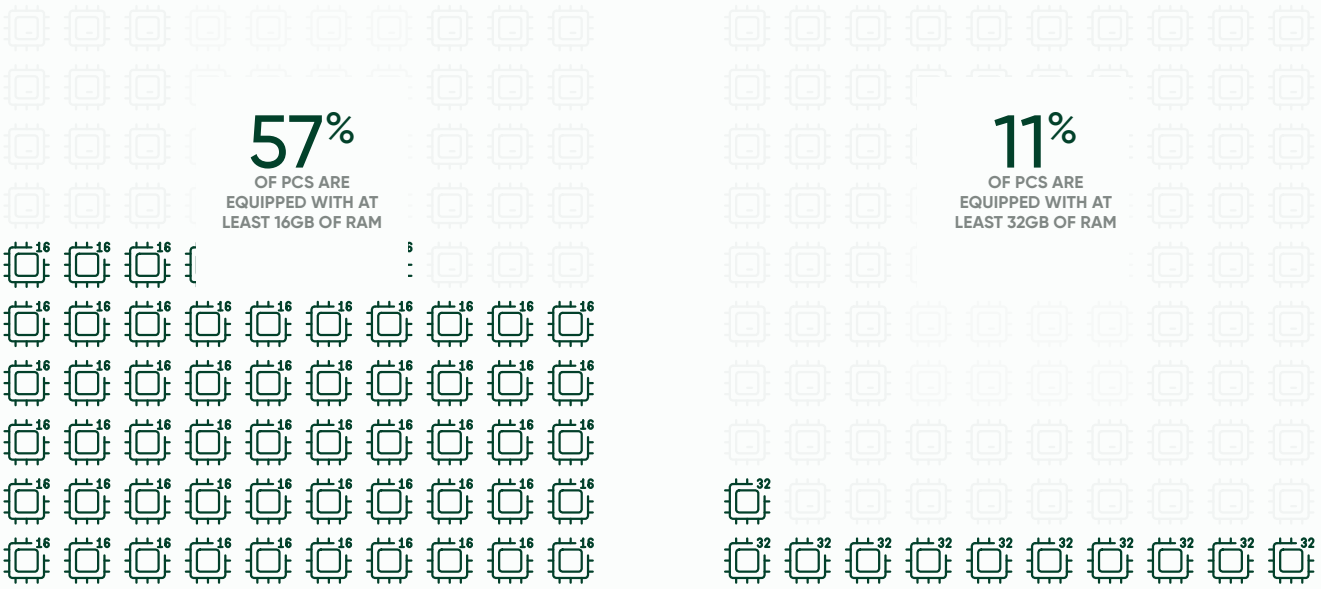


Figure 8 shows the percentage of PCs that are AI ready.



The Risk

IDC forecasts that demand for PCs supporting new innovations in AI will surge from 50 million units to 167 million by 2027, a 234% percent increase. Massive AI deployments are complex and resource-intensive. Devices loaded with new AI software not only add to complexity but also impact performance and security. Earlier in the report, it was revealed that endpoint security and risk applications fail frequently and that organizations are falling behind in critical endpoint vulnerability patching. Considering all these factors, it becomes clear why the coming AI replacement wave will add to the complexity and require enormous security and risk management efforts. In the meantime, enterprises may need to be selective in their deployment of these capabilities, as the underlying requirements to run them become more accessible or until the PC install base is refreshed.



Mitigation

Enterprises investing in large-scale AI-capable PC deployments should take steps to maximize efficiency across IT, security, and risk procedures. CISOs and IT leaders should guide their organizations to invest in AI-enabled endpoint fleets that automate not only deployment and management but also the repair and restoration of security controls and productivity applications.

FINDING 5

AI Visibility and Control

Shadow AI is growing, with PCs logging millions of visits to generative AI sites. Among those being accessed are DeepSeek, which has faced global backlash. The U.S., Italy, Taiwan, Australia and other countries are placing restrictions on it over data security concerns, with a total ban imposed in some cases. CISOs have struggled to maintain oversight of where and how data is being shared and how frequently employees are visiting non-authorized websites and using non-sanctioned AI applications.

Most CISO and IT leaders would agree that generative AI use is expanding, with Shadow AI adding unknown risk. One leading analyst organization predicts that a majority percentage of workers will ignore their organizations' security policies and use an AI platform of their choice to perform tasks.[21]

To better understand how generative AI is being used, over a 90-day period we assessed a cohort of more than 13 million PCs to determine how often users were visiting several popular sites, including the now notorious DeepSeek.

FIGURE 9

PCs Visited Generative AI Sites More than 3 Million Times

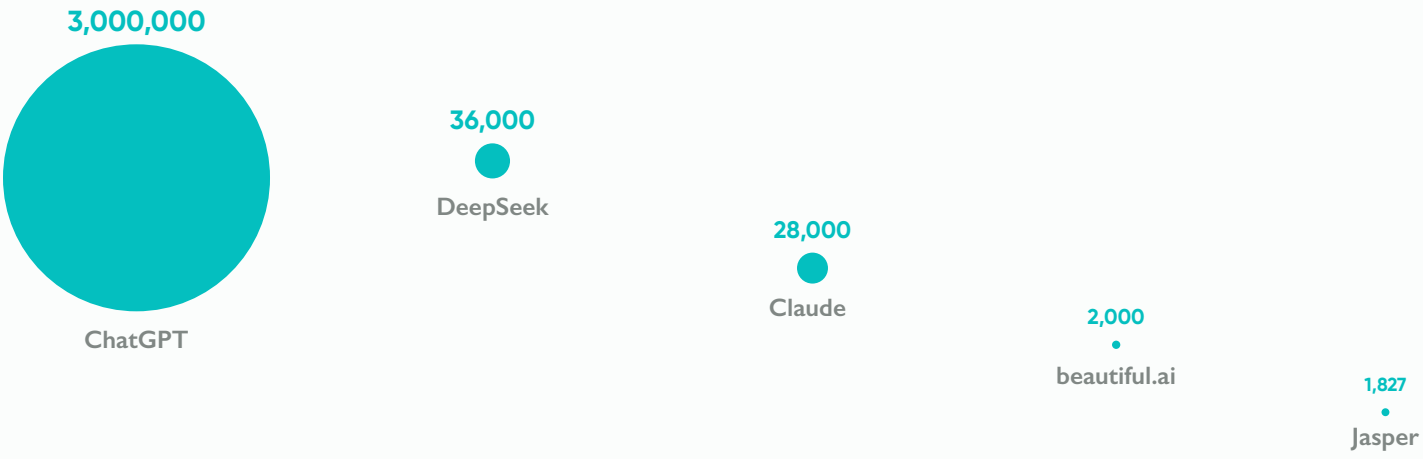


Figure 9 shows how frequently PCs are visiting several select and popular AI sites, including DeepSeek.



The Risk

While we do offer customers the ability to scan for and deter AI access, our telemetry doesn't indicate whether the sites visited are sanctioned or prohibited by the organizations managing the assessed devices. It is noteworthy that our data shows DeepSeek being accessed regularly, despite security-related bans and concerns.



Mitigation

The rapid adoption of advanced generative AI in the workplace is making it increasingly difficult for CISOs and IT leaders to keep up. As these tools demonstrate cost-saving and efficiency benefits, experts predict unauthorized use will continue to grow. To mitigate AI-related risks, organizations should deploy solutions that enable visibility, control, and enforcement of AI usage policies across endpoints. This includes having the ability to detect both local and cloud-based AI model and services usage, along with the ability to remove unauthorized local models and to block access to unauthorized cloud-based AI models and services. Advanced SSE solutions and endpoint security platforms can provide these protections along with Data Loss Prevention (DLP) and Remote Browser Isolation (RBI). Additionally, integrating resilience-enforcement solutions are essential to ensure these technologies continue functioning effectively. despite attacks and increasing complexity.

Conclusion

Extreme Resilience remains an industry problem that cybersecurity professionals and provider companies must work together to address. Remaining resilient and secure in the face of today's escalating threats and disruptions requires acknowledging the expanding range of risks and taking deliberate steps to strengthen infrastructures. Organizations must remain vigilant, understand where their greatest vulnerabilities lie, and focus on the key risks and mitigation strategies identified in this report to build Extreme Resilience. The findings from this year's Absolute Security Resilience Risk Index highlight several critical areas where enterprises must act decisively to embed resilience and secure their futures:

- Enterprises today are exposed not only to increasingly sophisticated cyberattacks, but also to operational risks stemming from technical failures, unpatched vulnerabilities, unprotected data, AI-driven complexity, and shadow IT.
- Endpoint security, vulnerability management, data protection, and AI governance gaps are leaving organizations vulnerable to breaches, ransomware, compliance failures, and major business disruptions.
- Traditional reactive security models are no longer enough. CISOs and IT leaders must confront the full spectrum of risks — including those caused by fragility within their own environments.
- To survive and lead, enterprises must proactively embed Extreme Resilience into their infrastructures: ensuring endpoints, security controls, software, and critical business systems are always on, fully operational, and able to recover swiftly.
- Organizations that enforce resilience across their IT and security stacks will be best positioned to mitigate emerging risks, sustain continuity, manage rising complexity, and adapt to an accelerating threat landscape.

A Call to Action:

In an era where we see much global uncertainty and acceleration of risk through new technical capabilities, we need to remain vigilant. This requires broad collaboration across our industry to build resilience:

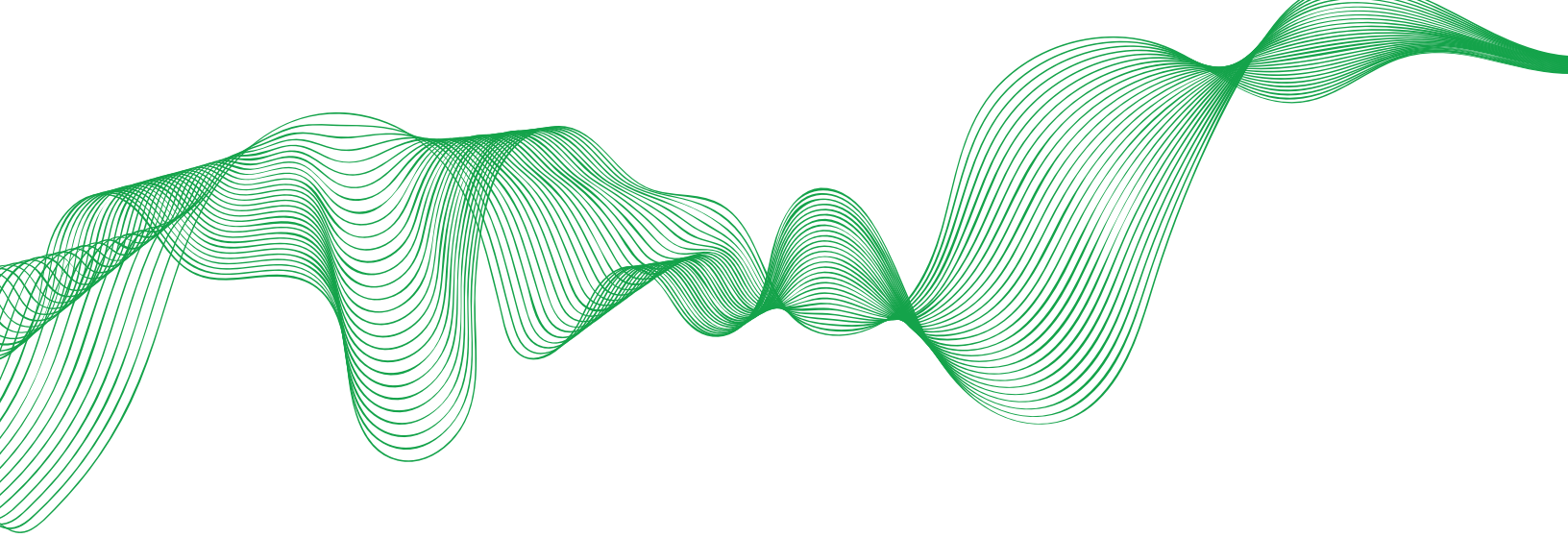
- Solution vendors should be transparent in their adoption of secure development processes and technical capabilities that can enhance their overall resilience and protect their customers.
- Business leaders need to require their supply chains to provide this transparency and accountability as well as prioritize investment in their own resilience strategies. Careful planning that ensures the ability to respond and restore to critical events as they occur will reduce impact when an incident strikes.
- Boards and cyber leadership teams need to incorporate resilience and business recovery strategies that include the full restoration of service after an event.

As an industry we will not make significant progress in achieving Resilience without transparency and collaboration.

How Absolute Helps

Endpoint Resilience can be a useful part of a broader Cyber Resilience Strategy and plan. The Absolute Security Resilience Platform provides an integrated and modular approach to enterprise security and resilience that ensures your enterprise is always on, fully operational, protected against threats, and able to quickly recover following an attack or disruption. Embedded in the firmware of more than 600 million endpoints, it provides comprehensive capabilities needed to embed resilience across enterprise organizations. With Absolute Security, customers can:

- Help ensure security and risk controls are always on, fully operational, and able to automatically self-heal in the face of misconfigurations, complexity, tampering attempts, and cyberattacks.
- With a single click and at scale, remotely rehydrate mobile, remote, and hybrid PC fleets to full operational capacity following a ransomware attack or IT incident, even when the device OS and other security and management tools are crashing, compromised, or corrupted.
- Manage risk across their PC fleets with automated vulnerability scanning and patch management to keep operating systems (OS), security controls and productivity applications fully updated and protected against risk.
- Ensure Zero Trust access to systems and data for remote and hybrid workers with robust Comply-to-Connect access controls that are custom-built to provide an optimized user experience.



SOURCES

1 Gartner, Forecast: Enterprise IT Spending by Vertical Industry Market, Worldwide, 2022-2028, 4Q24 Update

2 Gartner, Forecast: Information Security, Worldwide, 2022-2028, 4Q24 Update

3 Cybersecurity Ventures: Global Ransomware Damage Costs Predicted To Exceed $275 Billion By 2031

4 Absolute Security Censuswide CISO Survey 2025

5 Reuters: Microsoft says about 8.5 million of its devices affected by CrowdStrike-related outage

6 InformationWeek: CrowdStrike Outage Drained $5.4 Billion From Fortune 500: Report

7 Gartner, Leadership Vision for 2025: Security and Risk Management, Jan. 13, 2025

8 MITRE ATT&CK: Defense Evasion (TA0030)

9 MITRE ATT&CK: Impair Defenses (T1562)

10 CISA INSIGHTS: Remediate Vulnerabilities for Internet-Accessible Systems CYBER

11 Mandiant: M-Trends 2024 Special Report

12 Sophos: Unpatched Vulnerabilities: The Most Brutal Ransomware Attack Vector

13 CVE.org: Published CVE Records

14 InfoSecurity Magazine: 768 CVEs Exploited in the Wild in 2024

15 Security Scorecard CVE Details

16 Security Scorecard CVE Details

17 SC Media: 1 in 4 high-risk CVEs are exploited within 24 hours of going public

18 Statcounter Global Stats

19 You'll need 32 GB of RAM to run the next Windows on recommended settings

20 The Year Of The AI PC Is 2025

21 Forrester Report: Predictions 2024: Artificial Intelligence

About Absolute Security

Absolute Security is partnered with more than 28 of the world's leading endpoint device manufacturers, embedded in the firmware of 600 million devices, trusted by thousands of global enterprise customers, and licensed across 16 million PC users. With the Absolute Resilience Platform integrated into their digital enterprise, customers ensure their mobile and hybrid workforces connect securely and seamlessly from anywhere in the world and that business operations recover quickly following cyber disruptions and attacks.

To learn more, visit www.absolute.com and follow us on LinkedIn, X, Facebook, and YouTube.

ABSOLUTE SECURITY, ABSOLUTE, the ABSOLUTE LOGO, AND NETMOTION are registered trademarks of Absolute Software Corporation ©2025, or its subsidiaries. All Rights Reserved. Other names or logos mentioned herein may be the trademarks of Absolute or their respective owners. The absence of the symbols ™ and ® in proximity to each trademark, or at all, herein is not a disclaimer of ownership of the related trademark. Absolute Security is a Crosspoint Capital portfolio company.

