ABSOLUTE®

2024 CYBER RESILIENCE RISK INDEX

Enterprises are Unprepared for AI and the Security Challenges It Brings; Endpoint and Network Security Applications Fail Frequently

Executive Summary

Cyber Resilience is a paradigm larger and more critical than traditional cybersecurity. Organizations with effective Cyber Resilience capabilities have digital operations that can withstand and quickly recover to normal business operations following cyberattacks, technical malfunctions, or deliberate tampering attempts. The purpose of this year's report, "Absolute Security Cyber Resilience Risk Index 2024," is to assess the state of Cyber Resilience for today's global enterprises, as well as identify and uncover several top security risk factors that Cyber Resilience capabilities can mitigate.

Findings are based on anonymized telemetry from millions of mobile and hybrid PCs that run our firmware-embedded solution. To determine what several top risks to enterprise security are today, we analyzed data from 5,070,044 PCs from organizations with 500 or more active devices, running Windows 10 and 11. Among the key findings:

- On Managed PCs, when not supported by automated remediation technologies, PC Endpoint Protection Platforms (EPP) and network access security applications fail to maintain compliance with security policies 24 percent of the time
- To support enterprise AI technologies, 92 percent of enterprise PCs will need to be updated or replaced, leading to massive security challenges
- Most organizations run weeks or months behind in vulnerability patching, opening extensive risk gaps

With this data, Absolute determined three critical risk factors negatively impacting security and compliance:

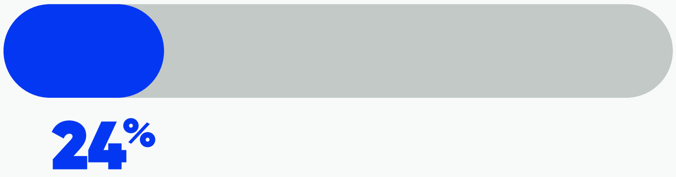
- ✓ Risk Factor 1: **Endpoint and Network Access Security Application failures**
- ✓ Risk Factor 2: **The AI Endpoint Wave**
- ✓ Risk Factor 3: **Organizations Continue to Fall Behind in Critical Patching**

In addition to sharing these key findings an in-depth analysis, the report provides CISOs and other security and risk professionals with guidance on how to:

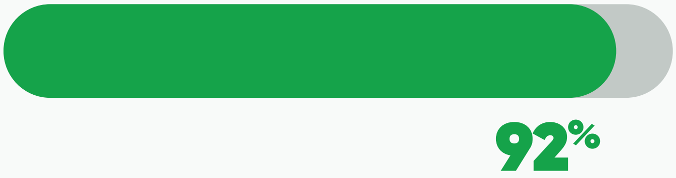
- Determine whether identified risk factors are present in their environments
- Learn what Cyber Resilience is and how it helps reduce these risk factors
- Improve their overall Cyber Resilience posture

Top Enterprise Security Risks

Endpoint Protection Platforms and network access security apps on managed PCs fail to maintain security policy compliance 24% of the time.



92% of enterprise devices aren't ready for AI, lacking basic requirements, such as sufficient RAM.



74

Average patch age (days) on Windows 10 Devices

45

Average patch age (days) on Windows 11 Devices

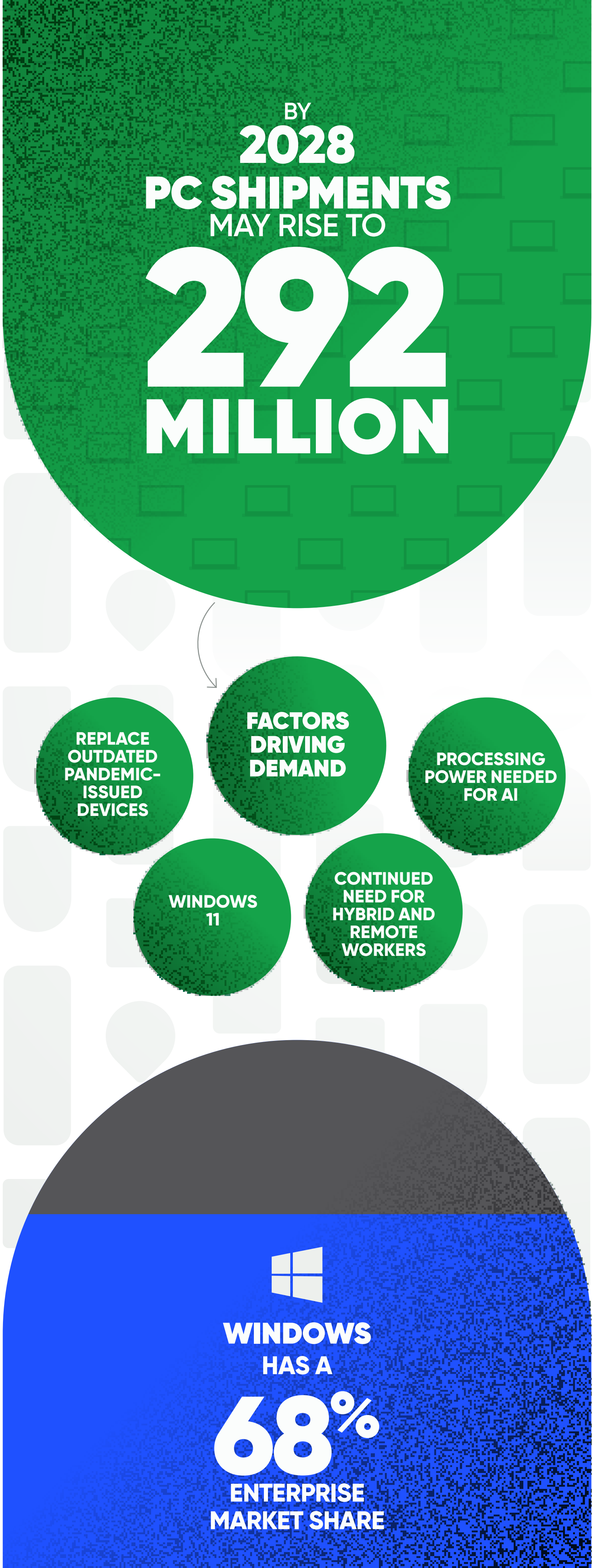
Access to anonymized telemetry from more than five million Windows 10 and 11 mobile and hybrid PCs running Absolute's firmware-embedded solution revealed top risks to enterprise security.

Introduction

PC sales are surging. According to industry analyst firm IDC, PC shipments may rise to 292 million by **2028**. Several factors are driving this demand, including the need to replace outdated devices issued during the pandemic, a frenzy for laptops with increased processing power needed to run enterprise AI-enabled applications, Windows 11, and the full entrenchment of hybrid and remote work.

PC's will continue to be a go-to business tool for decades to come, with Windows holding a **68 percent** market share in the enterprise. For CISOs and other security and risk professionals, PC ubiquity continues to enable attack surfaces for all industries, with each device introducing new vulnerabilities that cybercriminals and threat actors exploit. Regulations will also place further pressure on the PC economy. For example, across the European Union (EU), businesses required to adhere to environmental **regulations** not only have to securely integrate new units, but also find ways of refurbishing and updating millions of devices already in use.

To thrive in today's PC-driven digital business ecosystem and reduce the risk of disruption during these fast-changing business and threat landscape conditions, organizations must move beyond legacy cybersecurity strategies in favor of Cyber Resilience.



BY 2028 PC SHIPMENTS MAY RISE TO 292 MILLION

FACTORS DRIVING DEMAND

REPLACE OUTDATED PANDEMIC-ISSUED DEVICES

PROCESSING POWER NEEDED FOR AI

WINDOWS 11

CONTINUED NEED FOR HYBRID AND REMOTE WORKERS

WINDOWS HAS A 68% ENTERPRISE MARKET SHARE

SECURITY RISK FACTOR 1

Endpoint and Network Access Security Application Failures

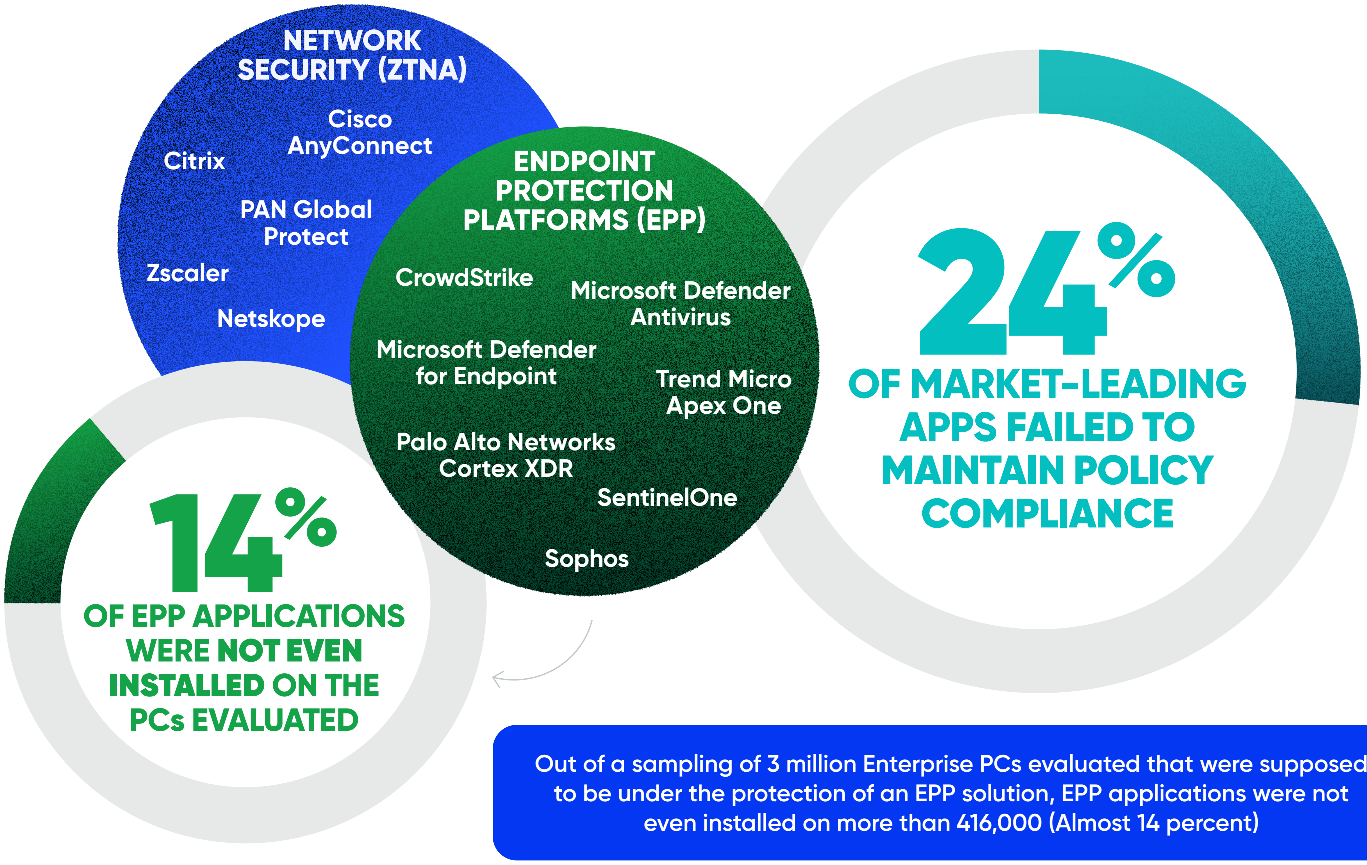
KEY FINDING When not supported by automated remediation technologies, Endpoint Protection Platforms (EPP) and network access security applications fail to maintain compliance with security policies 24 percent of the time, across managed PCs (EPP includes top XDRs, network access security applications include ZTNA).

PCs are the most ubiquitous business computing tool used today, with Windows devices accounting for 68 percent of these. Available telemetry shows that organizations use upwards of a dozen security applications per device, and govern them with four basic security policies:

1. Ensure application is present on the device
2. Ensure application version is correct
3. Verify application is running as expected
4. Verify the application is properly signed and has not been tampered with

To provide insights into how frequently organizations fail to maintain compliance with these policies across endpoint and network access security controls, Absolute Security assessed market-leading solutions deployed across more than 5 million Windows PCs:

ENDPOINT AND NETWORK ACCESS SECURITY APPLICATION FAILURE RATES



Out of a sampling of 3 million Enterprise PCs evaluated that were supposed to be under the protection of an EPP solution, EPP applications were not even installed on more than 416,000 (Almost 14 percent)

Data showed that on average, these applications are **out of compliance with the four security policies 24 percent of the time.** This is especially noteworthy, when considering EPP and Network Security applications, (including Zero Trust Network Access (ZTNA), are the first line of defense on the mobile and hybrid network edge.

Impact to Security

PC Endpoint Protection Platforms (EPP) and network access security applications fail to maintain compliance with security policies 24 percent of the time. This gap in efficacy leaves PCs open to costly disruptions and compromises, ransomware infections, and other threats.

Mitigation: CISOs and other security and risk professionals should deploy solutions that can monitor, report, and help repair endpoint and network access security applications in as near real-time as possible. "Fail Safes" that come standard with applications may not suffice, as malfunctioning or compromised software will not be able to self-mitigate back into an effective state. Underpin your endpoint and network access security controls with technologies that automate the repair and restoration of applications to an effective state following cyberattacks, technical malfunctions, or deliberate tampering attempts.

RISK FACTOR 2

The AI Endpoint Wave

KEY FINDING 92% of Enterprise PCs Not Ready for AI.

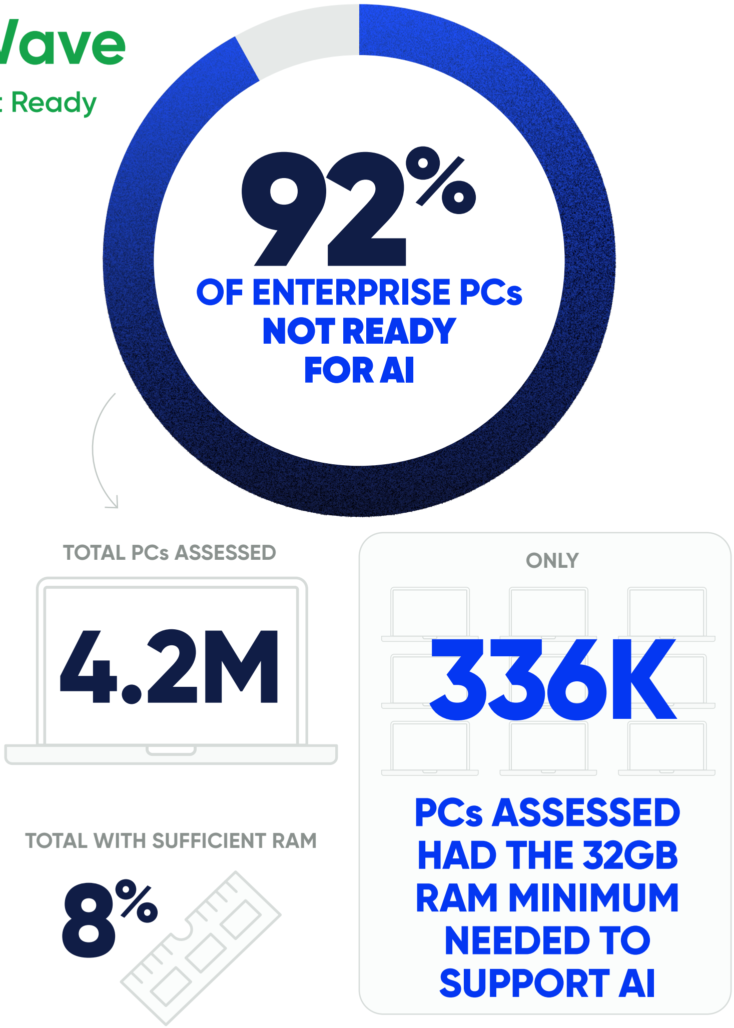
For enterprise PCs to run AI applications and processes effectively, reports show devices should be equipped with a minimum of 32GB of RAM[1] and either a stand-alone GPU or an integrated NPU; with one of the world's top analyst firms advising clients to standardize on this criteria. To assess the AI-based readiness for today's enterprise devices, we analyzed a sample from more than 4 million Windows machines. Our telemetry revealed that most devices lack the basic requirements needed to support AI. It's no wonder why IDC forecasts that demand for PCs supporting new innovations in AI will surge from 50 million units to 167 million by 2027, a 60 percent increase.

Lack of AI Readiness

- 92% (4.2 MILLION sample) of devices have insufficient RAM capacity for AI

Impact to Security

Massive deployments are complex and resource intensive. Huge investments in AI-capable endpoint fleets have the potential to divert budget and human resources away from critical IT and security priorities that can leave gaps in security and risk policies. Devices loaded with new software not only add to complexity but also impact performance and security. Earlier in the report, it was revealed that endpoint security applications fail frequently. Further on, research shows that organizations are running behind in critical endpoint vulnerability patching.



When you consider all these factors, and others, it can easily be understood why the coming massive AI Replacement Wave will require enormous security and risk efforts.

Mitigation: Enterprises investing in huge AI-capable PC roll outs should take steps to ensure maximum efficiency across IT, security, and risk procedures. CISOs and other security and risk professionals should advise their organizations to invest in AI-enabled endpoint fleets equipped with technologies that automate not only roll-out and management processes, but also the repair and restoration of security applications to an effective state, enabling them to provide maximum defense against threats.

The AI Data Security Advantage

AI will undoubtedly enhance cybersecurity capabilities. It will also introduce more risk – as vulnerabilities and AI-enabled threats will arise. When it comes to data security, endpoints that can handle large data sets and language model processing locally may provide an added advantage of storing data on enterprise-owned assets, rather than having to store and process it with third-party cloud hosts. With more localized control over data, organizations can reduce overall risk of data theft and leaks, but only if security and risk controls deployed on the endpoints are functioning properly.

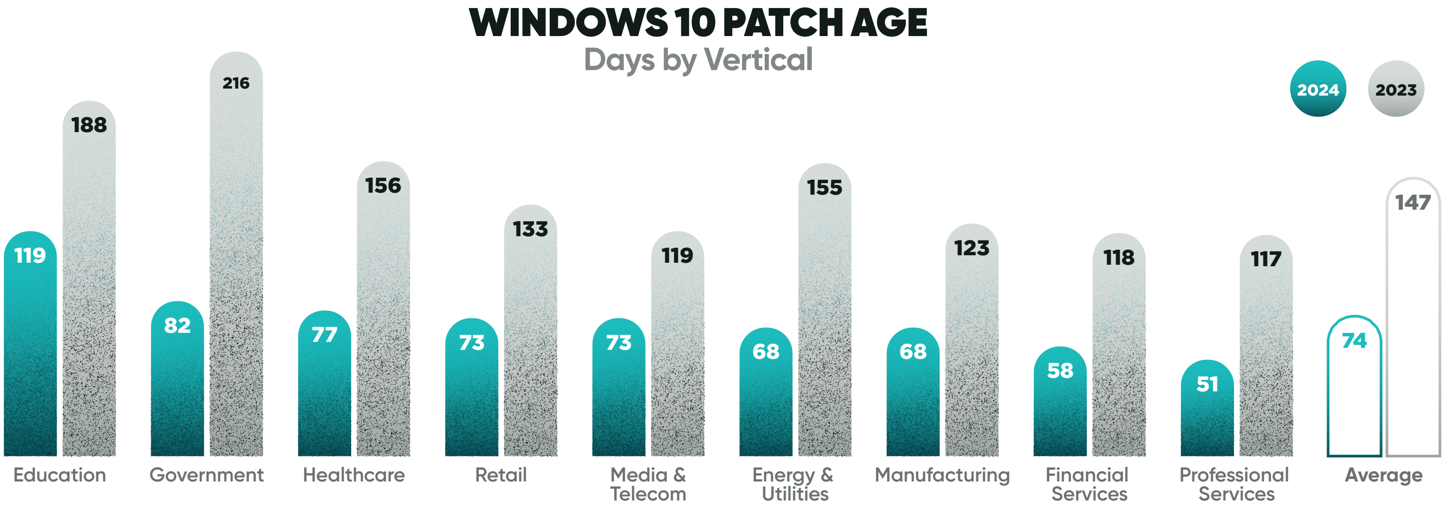
[1] You'll need 32 GB of RAM to run the next Windows on recommended settings, Windows Report, 2024

SECURITY RISK FACTOR 3

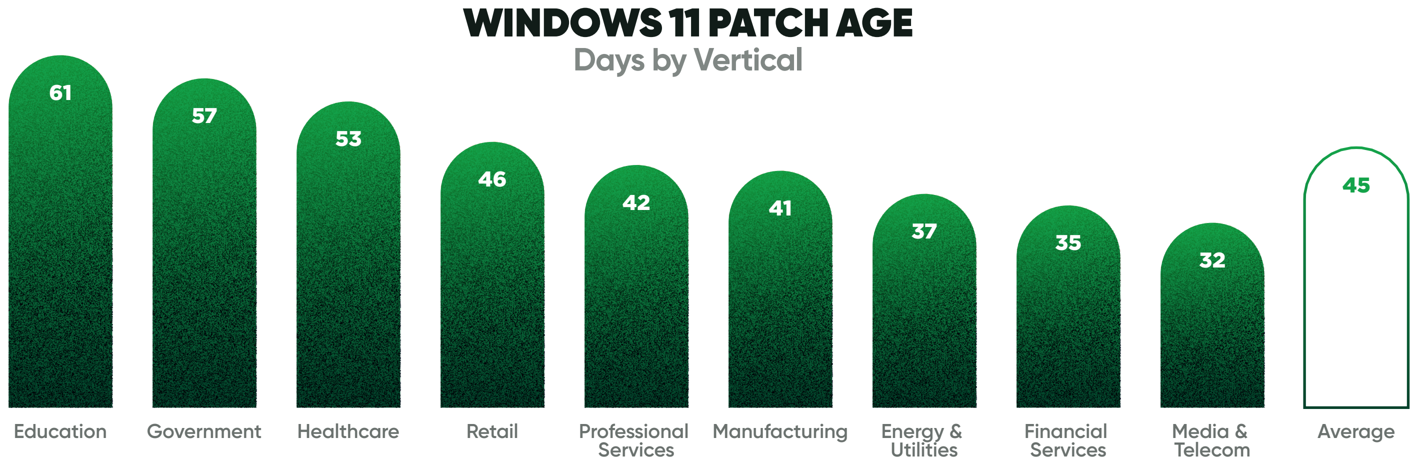
Critical Vulnerability Patching Delayed

KEY FINDING Organizations continue to fall behind in critical patching.

The Google Threat Analysis Group (TAG) reported exploits for 97 Zero Day vulnerabilities in 2023, up from 62 in 2022. CVEdetails.com recorded 29,065 CVEs in 2023 and has already tallied 8,395 in 2024. Despite these increases, organizations continue to lag when it comes to patching, with Windows 10 environments trailing 11, according to telemetry from a sample of Windows PCs running versions 10 and 11.



The state of patching varies across different verticals, with patching schedules and policies set by each organization. According to our research, education organizations take the longest number of days to patch their systems followed by the government sector, although both showed significant improvement YoY. Notably, financial services institutions lead the other organizations in time to patch.



This is the first year Absolute Security evaluated Windows 11 devices for this report. Organizations upgraded to this new OS version showed improvement over counterparts still managing Windows 10, cutting patching time by almost half. Not surprisingly, this is better than what we see for the much larger and longer-lived Windows 10 base. We will continue to track and report this metric in coming months to see if this can be sustained over time.

Impact to Security

In a Service Now commissioned report from the Ponemon Institute, it was revealed that 60 percent of breaches resulted from unpatched vulnerabilities. In a 2023 joint study, dozens of software vulnerabilities enabling ransomware infections were identified. Regardless of which represents a more accurate view of your organization's experience, the consequences of unmitigated CVEs are undeniable – data breaches, ransomware attacks, and unwanted cyber disruptions.

Mitigation: CISOs and other security and risk professionals should deploy solutions that help them identify all impacted assets in their environment, prioritize vulnerabilities affecting their deployed software, and then assign as many patching tasks as possible to automation platforms. Standard vulnerability management platforms may not verify whether assets are in compliance with security policies or performing as expected, even if fully patched. To avoid errors these solutions do not track, add a layer that expands visibility over software and hardware assets to ensure they are operating as needed. Remember, research showed that out of 3 million of the PCs evaluated, EPP applications were not even installed on more than 416,000 (Almost 14 percent) – a critical issue that vulnerability management tools will not identify.

Conclusion

Cyber Resilience is relatively new. Several factors are pushing it into the mainstream. These include White House directives calling for it to be built into software supply chains, recognition that legacy detection and prevention strategies aren't sufficient to defend against advanced threats, and leading industry groups identifying Cyber **Resilience** as an emerging trend.

Although there are myriad factors impacting enterprise security and risk, which can be mitigated with Cyber Resilience capabilities, this report leveraged real-world data to identify a few that are common across organizations. The findings provide providing security and risk leaders with guidance on where they can easily start to implement their own Cyber Resilience strategy.

Absolute Security Cyber Resilience Risk Index Report Methodology

To compile this index, our Absolute Security Cyber Resilience Experts analyzed anonymized telemetry from 5,070,044 PCs running Windows 10 and 11, in use by 21,000 global customers, and 14 million licensed users.

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 21,000 global enterprises, and licensed across 14 million PC users. With the Absolute Security Cyber 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. Our award-winning capabilities have earned recognition and leadership status across multiple technology categories, including Zero Trust Network Access (ZTNA), Endpoint Security, Security Services Edge (SSE), Firmware-Embedded Persistence, Automated Security Control Assessment (ASCA), and Zero Trust Platforms.

Request a Demo