

New Research From Absolute Software Underscores Security and Compliance Challenges Remain Across Distributed Workforces

Report reveals OS fragmentation, endpoint and network complexity creating false sense of security for enterprises

VANCOUVER, British Columbia & SAN JOSE, Calif.--(BUSINESS WIRE)--April 24, 2023--Absolute Software™ (NASDAQ: ABST) (TSX: ABST), the only provider of self-healing, intelligent security solutions, today announced new research revealing the increasing complexity in enterprise device environments, including operating system (OS) fragmentation and volume of applications, is impacting security and compliance posture.

The findings in Absolute's '2023 Resilience Index' contradict the long-held belief that having more security solutions directly equates to more protection. Leveraging the analysis of anonymized data from millions of customer devices across the globe, this report provides insights and benchmarks for organizations looking to strengthen cyber resilience in today's widely distributed, hybrid workplaces.

The work-from-anywhere model is exacerbating the strain on IT and security teams – compounding existing device health and security challenges with a broad mix of networks, hardware, OS versions, and patches. More than 80 percent of devices analyzed use the Microsoft® Windows® OS, with the large majority on Windows 10 – and within that device population, there are 14 different versions and more than 800 builds and patches to manage. Absolute's telemetry data also shows there are 67 applications installed on the average enterprise device, with 10 percent of those devices having more than 100 applications installed.

While many of these tools enable employees to be productive, they also contribute to increased complexity. This complexity can create conflict among applications; impede the patching and maintenance of devices and applications, especially if those devices are remote; and lead to software failing or going offline over time.

In this report, Absolute looks at common security applications deployed for hybrid workers and assessed the health of leading vendors within the categories of: Endpoint Protection (EPP), Endpoint Detection and Response (EDR), and secure access. The data shows seven of the 10 apps analyzed across these categories were installed and healthy on less than 80 percent of devices, on average – and in some cases, as low as 47 percent. When self-healing capabilities via Absolute Application Resilience™ were enabled, application health and efficacy rates across these same vendors increased significantly, as much as 52 percentage points.

“Security that is not installed or working effectively cannot protect you,” said Christy Wyatt, President and CEO of Absolute Software. “The criticality of these security controls, especially among remote and hybrid workers, cannot be overstated and the ability to keep them healthy is often oversimplified. Even market-leading, world-class software requires repairing for many reasons: changes in the environment around it, or new forms of risk introduced by adversaries or even by the user. By applying intelligence and automation to heal them, we can remediate the risk, restore the user experience, and ensure compliance.”

Other key insights from the ‘2023 Resilience Index’ include:

Distributed, highly mobile users compound complexity: The average number of enterprise device locations across Absolute customers has grown 15 percent year-over-year, with an average of four locations per device observed in February 2023.

Hybrid working means heavy reliance on third-party networks: In hybrid work models, critical applications like Virtual Private Networks (VPNs) and Zero Trust Network Access (ZTNA) need to be deployed, installed, and up to date. However, Absolute data shows this critical tool is either not installed or is not at the required version level on more than 30 percent of devices.

Embedded in the firmware of more than 600 million devices, Absolute enables visibility and control across endpoints, applications, and network connections. Leveraging our unique self-healing capability, customers can protect devices, data, and users and ensure that critical security controls operate at maximum effectiveness, while also delivering an optimal remote and mobile user experience. Leveraging our patented Absolute Persistence® technology and Absolute Application Resilience capabilities, both enterprises and security vendors can optimize application efficacy and strengthen security and compliance posture.

Read the full ‘2023 Resilience Index’ [here](#). To learn more about Absolute Software and the company’s intelligent, self-healing security solutions, visit [here](#).

Report Methodology

This report was developed using anonymized data from 14 million Absolute-enabled devices active during the period of February to April 2023, across customer organizations in North America, Europe, and APAC, as well as data and information from trusted third-party sources.

About Absolute Software

Absolute Software (NASDAQ: ABST) (TSX: ABST) is the only provider of self-healing, intelligent security solutions. Embedded in more than 600 million devices, Absolute is the only platform offering a permanent digital connection that intelligently and dynamically applies visibility, control and self-healing capabilities to endpoints, applications, and network connections - helping customers to strengthen cyber resilience against the escalating threat of ransomware and malicious attacks. Trusted by nearly 20,000 customers, G2 recognized Absolute as a Leader for the thirteenth consecutive quarter in the Spring 2023 Grid® Report for Endpoint Management and as a Leader for the third consecutive quarter in the Grid Report for Zero Trust Networking.

©2023 Absolute Software Corporation. All rights reserved. ABSOLUTE, the ABSOLUTE logo, and NETMOTION are registered trademarks of Absolute Software Corporation or its subsidiaries. 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.

Contacts

For more information:

Media Relations

Becki Levine
press@absolute.com
858-524-9443

Investor Relations

Joo-Hun Kim
IR@absolute.com
212-868-6760