New Absolute Insights Reveal Increases in Enterprise and Education Device Usage, Vulnerability of Sensitive Data as Endpoints Remain Fragile Amid COVID-19 Outbreak

Data shows heavy device usage up 49 and 62 percent across enterprise and education, respectively; average Windows 10 enterprise device 90 days behind on patching, with delay spiking to 180+ days for average education device

VANCOUVER, British Columbia--(BUSINESS WIRE)--April 30, 2020--Absolute (TSX: ABT), the leader in endpoint resilience, today revealed striking insights in the wake of the global COVID-19 outbreak, including a spike in enterprise and education device usage, sustained gaps in endpoint health and security, and an alarming number of Windows 10 devices not being patched. More of these trends can be found in the company's Remote Work and Distance Learning Insights Center, which is being updated weekly.

Directly after the World Health Organization declared COVID-19 a global pandemic, an estimated 16 million US employees were sent home and instructed to work remotely, while governments around the world implemented widespread school closures impacting over 90 percent of the world's student population. This result placed IT and Security teams under immediate pressure to quickly stand up work-from-home or learn-from-home environments to ensure continued productivity, connectivity, and security.

"COVID-19 marks the beginning of a new era where we believe the nature of work will be forever changed," said Christy Wyatt, President and CEO of Absolute. "As this crisis took hold, we saw our customers mobilize quickly to get devices into the hands of students and employees and navigate the challenges of standing up remote work and distance learning programs. What has become resoundingly clear is there has never been a more critical time for having undeletable Endpoint Resilience."

Now, as focus shifts to optimizing remote work and distance learning programs, Absolute's Insights Center enables both enterprise and education organizations to measure and benchmark the health and security of their remote device programs, pre and post-COVID-19. Top insights include: (as of April 24, 2020)

Sensitive data is piling up on enterprise devices. There has been a 46 percent increase in the number of items of sensitive data - such as Personally Identifiable Information (PII) and Protected Health Information (PHI) - identified on enterprise endpoints, compared to pre-COVID-19. Compounded by the pre-existing gaps in endpoint security and health, this means enterprise organizations are at heightened risk.*

Enterprise organizations are at heightened risk of breaches or compliance violations. On average, one in four enterprise endpoint devices have a critical security application (Anti-Malware, Encryption, VPN, or Client Management) that is missing, inactive or out-of-date. With the significant increases in sensitive data being stored on these endpoints, enterprises are putting themselves at risk of legal compliance violations and data breaches as COVID-19 cyber attacks accelerate.

Employee and student device usage continues to rise post-COVID. The data shows a nearly 50 percent increase in the amount of heavy device usage – 8+ hours per day – across enterprise organizations, jumping to an increase of 62 percent in heavy education device usage. The average number of hours education endpoint devices are being used daily is also up 27 percent.

Device health sees slight improvement, but patch management continues to plague both Enterprise and Education IT teams. The average enterprise endpoint device running Windows 10 continues to be nearly 3 months behind in applying the latest patch, with that delay spiking to more than 180 days since a patch has been applied to the average student Windows 10 device – leaving students and employees vulnerable.

Absolute's insights also shine a light on the value of automated, self-healing capabilities in both boosting endpoint security control health and minimizing the strain that remote work environments put on the IT organizations tasked with ensuring controls are present and working on remote devices. The data shows that customers using Absolute's patented Application Persistence™ technology to seamlessly manage and repair critical security apps – notably, VPN, antivirus, and encryption apps – saw compliance rates of 94 percent or above, whereas the average enterprise organization recorded compliance rates below 80 percent across the same app categories.

To enable customers to more effectively secure and manage remote work and distance learning environments, Absolute previously announced it has enabled access to key capabilities typically included in its premium Resilience offering for existing customers at no additional cost through August 30, 2020, including:

- Application Persistence for VPN, enabling IT teams to ensure remote employees and students have a continuous, secure connection to their data and applications
- A comprehensive library of automated, custom workflows, allowing IT to proactively pinpoint vulnerabilities and quickly take remedial action, whether a device is on or off the corporate network

To access Absolute's Remote Work and Distance Learning Insights Center, and see additional detail about the offers available to existing Absolute customers, visit here.

For more about information about Absolute, visit www.absolute.com.

***Absolute's Endpoint Data Discovery does not collect or store this information; it merely indicates if it is present on endpoints.*

Methodology

These insights leverage anonymized data from enterprise and education-specific subsets of nearly 8.5 million active, Absolute-enabled devices.

About Absolute

Absolute serves as the industry benchmark for endpoint resilience, visibility and control. Embedded in over a half-billion devices, the company enables more than 12,000 customers with self-healing endpoint security, always-connected visibility into their devices, data, users, and applications – whether endpoints are on or off the corporate network – and the ultimate level of control and confidence required to support the modern enterprise. For the latest information, visit www.absolute.com and follow us on LinkedIn or Twitter.

Contacts

Media Relations
Shannon Tierney
press@absolute.com
408-313-9974

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