Absolute Provides Customers with Automated Workflows to Secure and Manage Remote Devices at No Charge In Expanded Response to Global Coronavirus Outbreak

Includes report and repair capabilities needed to proactively mitigate recent critical vulnerability affecting Windows 10 devices, CVE-2020-0796

VANCOUVER, British Columbia--(BUSINESS WIRE)--March 24, 2020--Absolute® (ABT.TO), the leader in endpoint resilience, today announced it is expanding its response to the global coronavirus outbreak, providing all of its customers with access to a comprehensive library of automated, custom workflows that enable a more seamless way to secure and manage remote devices. As businesses accelerate remote work policies, and cyber criminals look to exploit unsuspecting or distracted employees, Absolute is enabling IT and Security teams with self-healing endpoint security – allowing them to proactively pinpoint vulnerabilities and quickly take remedial action, whether a device is on or off the corporate network. This offer builds on the company's previous announcement that it is extending Application Persistence for VPN at no cost, enabling customers provide uninterrupted remote access to corporate networks, business applications and data.

A prime example of malicious cyber criminal behavior is the remote code execution vulnerability or "wormable", CVE-2020-0796, that emerged last week, carrying the potential to propagate itself from vulnerable computer to vulnerable computer. While Microsoft moved swiftly to warn Windows 10 users and deliver a security update, the difficulties of patching remote devices that may not be connected to the corporate network, as well the probability of failed updates, present a significant risk of exposure to cyber attacks. Absolute's new report and reach script enables IT to mitigate this vulnerability by identifying all potentially affected devices and disabling access to targeted servers until the patch is installed.

Recent data validates the risk exposure presented by unpatched devices and gaps in security policies or applications. Early findings from Absolute's upcoming '2020 State of Endpoint Resilience Report' show that more than half of Windows 10 enterprise devices with versions 1903 and 1909 - those susceptible to CVE-2020-0796 - are more than four weeks behind installing patches. This is hugely concerning in light of another recent study that found 60 percent of breaches are linked to a vulnerability where a patch was available, but not applied.

"There has never been a more critical time to support our customers than right now, as they navigate complex discussions about how to ensure business continuity, keep employees protected and maintain Enterprise Resiliency," said Christy Wyatt, President and CEO of Absolute. "This includes helping them understand where they may be most vulnerable or exposed to risk, which may be much more difficult now that an exponentially larger population of employees are working and connecting remotely. We are committed to ensuring IT and Security teams have effective ways to mitigate that risk with self-healing controls and applications so that they can focus on maintaining business operations and taking care of their own customers."

In addition to the reach script for CVE-2020-0796, Absolute customers have access to more than 130 custom workflows that allow them to easily run queries or reports and then take widespread remedial action such as enforcing patch installations, turning on or repairing VPN applications, and more with just a few clicks. Because of Absolute's unique firmware-embedded position, these actions can be enforced and executed on any device connected to the internet, even if off the corporate network.

In support of IT teams working to ensure business continuity and enable remote employees to reliably and securely connect to corporate systems amid the global outbreak of the novel coronavirus, Absolute is providing free access to its comprehensive library of custom workflows and Reach scripts for Visibility and Control tier customers through August 31, 2020. These tools are already available to Absolute's Resilience tier customers.

To learn more about Absolute custom workflows and Reach capabilities, as well as how to take advantage of this offer, click here. To learn more about Absolute Application Persistence for VPN and the company's previously announced offer, click here.

About Absolute

Absolute empowers more than 12,000 customers worldwide to protect devices, data, applications, and users against theft or attack—both on and off the corporate network. With the industry's only tamper-proof endpoint visibility and control solution, Absolute allows IT organizations to enforce asset management, security hygiene, and data compliance for today's remote digital workforces. Absolute's patented Persistence technology is embedded in the firmware of Dell, HP, Lenovo, and 22 other leading manufacturers' devices for vendor-agnostic coverage, tamper-proof resilience, and ease of deployment. See how it works at www.absolute.com and follow us at @absolutecorp.

Contacts

Media Relations
Shannon Tierney
press@absolute.com
415-544-7226

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