CUSTOMER SUCCESS WITH ABSOLUTE REACH

"Using Absolute's ability to securely see and control endpoints, we can move from using raw and unverifiable guesswork to verifiable and actionable intelligence when securing user endpoint devices."

Elliot Lewis
President
LEWIS SECURITY CONSULTING, LLC

INFOSHEET

Dark endpoints are a breeding ground for security breaches. When endpoints go rogue or become invisible due to faulty security agents, you need to act fast. The Absolute platform featuring Reach gives you the visibility and control to see, understand and act faster against security threats. See how our customers use Absolute Reach to quickly tackle some of today's top security threats, including malware, unpatched devices and critical firmware vulnerabilities.

THE CHALLENGE: MALWARE

Devices missing security-critical patches leave organizations open to known vulnerabilities that can be exploited by threats such as WannaCry, Shadow Brokers, and other ransomware.

THE SOLUTION: SELF-HEALING ENDPOINT SECURITY

Our customer uses Reach to query all devices in their deployment to determine which devices are missing the required patches. Once the endpoints are identified, the customer disables the SMB service on all affected devices to thwart any ability for the malicious code to be passed between networked devices. With the medium for spreading the malware contained, our customer quickly deployed scripts to identify the exact patch level required, determine their vulnerability level, define performance conditions and then quickly execute approved scripts onto critical devices. This level of deep and persistent awareness reduced vulnerability and contained threats while instantly validating compliance for the organization.

THE CHALLENGE: MISSED PATCHES

Mobile work forces rely on devices that may run off cached and expired credentials or be dropped from the domain after not reconnecting for 60 days or more. This situation can lead to missed critical OS patches or scheduled updates they would otherwise receive when regularly connected to Active Directory.

THE SOLUTION: ALWAYS-CONNECTED IT ASSET MANAGEMENT

Our customer selected Reach so they could create a script that leveraged Absolute's always-connected nature to devices, on and off the network, to safely rejoin the device to the domain and regain compliance with Active Directory policies.

THE CHALLENGE: FIRMWARE VULNERABILITY

Devices were susceptible to an Intel Critical Firmware Vulnerability, which enabled network attackers to remotely gain access to business PCs or devices that use certain Intel technologies.

THE SOLUTION: ALWAYS-CONNECTED IT ASSET MANAGEMENT

Our customer used Reach to deploy and confirm delivery and execution of an Intel created script to scrape attributes and store them in a central database to assess vulnerability and exposure.

THE CHALLENGE: DATA COPIED OFF NETWORK

Data Loss Prevention is a critical part of ensuring that sensitive or critical information is not sent outside the control of IT administrators.

THE SOLUTION: DATA VISIBILITY AND PROTECTION

An accounting firm selected Absolute for its ability to reach devices on or off the network, keeping IT administrators in control. A Reach customer created a custom query to prevent copying files to a USB drive to strengthen their DLP position.

THE CHALLENGE: INSIDER THREATS

Insider threats often arise when users have access to data outside their user level, when users install unapproved software onto devices, or when users engage in suspicious browser activity that could introduce malware. The malicious, negligent or unknowing actions of insiders place data at risk and open up issues around software licensing, support costs and compliance liabilities.

THE SOLUTION: DATA VISIBILITY AND PROTECTION

An Absolute customer created a query to identify and revoke any unauthorized administrator privileges of end users for devices that would allow those users to potentially install unapproved software or copy/transfer sensitive data. An additional script was used to eliminate any previously created guest accounts that were no longer in use. The same customer created another query that identified certain browser activity as "suspicious," allowing for remote capability to clear browsing cache and/or freeze the device.

Enterprises can now customize the power of Absolute with Reach, a powerful new custom query and remediation feature of the Absolute platform.

OUTCOMES with REACH

ELIMINATE BLIND SPOTS
Assess endpoint agent compliance, understand current patch and version profiles, and remediate known vulnerabilities in near real-time.

PROVE COMPLIANCE
Leverage firmware-embedded technology for always-connected visibility over devices, applications and data to evaluate exposure risk and prove compliance.

REMEDIATE ON-DEMAND
Tap into a growing library of verified and actionable scripts or execute custom actions to address new threats.

AUTOMATED AUDITS
Create and execute ITAM queries for inventorying and audits.

For more information about Absolute Reach please visit **absolute.com/reach**