Absolute Remediate

Endpoint Threat Remediation At Scale

BENEFITS

- Eliminate blind spots
- Respond effectively to device threats and vulnerabilities
- Enforce security controls
- Mitigate non-compliance risk
- Prevent shadow IT
- Increase IT efficiency
- Reduce helpdesk tickets
- Improve end user experience
- Avoid coding complexity

Absolute Reach is an amazing, mind-blowing technology that takes the product to the next level of possibilities. We have the potential to address a risk or compliance issue — that can save the day. We also enjoy the fact that we can ensure all of our devices are up-to-date.

Mike Fallat
Manager, IT Procurement
Ogletree Deakins

Ogletree Deakins

The Challenge: Endpoint Management Beyond Traditional Tools

With remote and hybrid workforces being the new normal and devices routinely operating off the corporate network, you need to extend your reach beyond the constraints and network dependencies of traditional tools. Endpoint management ingrained with automated resilience is critical to enforce standard configurations and protect devices, keep end users productive, and your IT team efficient. Maintaining compliance and ensuring business continuity across a distributed workforce requires visibility and automated action.

The Solution: An Undeletable Tether And Unlimited Versatility

Absolute Reach is a powerful remote query and remediation tool, a core component of the Absolute Remediate solution, powered by its unique firmware-embedded, self-healing Absolute Persistence® technology. It gives you the unbreakable visibility you need to be able to touch any device, on or off your corporate network, and the flexibility to remotely gather any precise insights or take urgent remedial action at scale.

Common scenarios:

- Set up devices remotely and at scale, even when traditional device management tools are not functional
- Detect and fix deviations from standard configurations
- Detect critical OS vulnerabilities across your entire device population
- Implement urgent workarounds and enforce operating system updates
- Speed up audits and automate regular compliance checks
- Uninstall unauthorized software
- Install or troubleshoot applications
- Adjust settings and automate maintenance to optimize end user experience
- Anticipate and prevent common device issues to avoid downtime

How it Works

- Cloud-based, no network infrastructure required
- Query or remediate one or multiple Windows or Mac devices, at scale
- Always available to target any endpoint, on or off your corporate network
- Library of 130+ pre-built, ready-to-use scripts
- Unlimited flexibility to create custom scripts using PowerShell or BASH
- Confirm successful execution of your actions

The Reach Library: Ready-To-Use Solutions to Common IT And Security Challenges

Absolute Remediate comes with a comprehensive library of pre-built scripts, ready to be used without any need for coding, to solve a myriad of common IT and security challenges without the limitations of traditional tools. To execute an action or query information using a script, simply select devices within your environment, search for the appropriate script for your specific situation, enter the required parameters, and execute it. You can also explore the entire library within the Settings area of your Absolute Console.

Common scenarios:

- Set up devices remotely and at scale, even when traditional device management tools are not functional
- Detect and fix deviations from standard configurations
- Detect critical OS vulnerabilities across your entire device population
- Implement urgent workarounds and enforce operating system updates
- Speed up audits and automate regular policy checks
- Uninstall unauthorized software
- Install or troubleshoot applications
- Adjust settings and automate maintenance to optimize end user experience
- Anticipate and prevent common device issues to avoid downtime

Optimize End User Experience

Streamline User Management

Users and Groups

- Add local group
- Add local user
- Add/remove domain user/group to/from local group
- Backup local user and group
- Remove local user or local group
- Delete aged user profiles
- Enable or disable user account on computer
- Set local administrator password

Audit User Accounts

- Audit the local administrators
- Gather enabled and disabled local accounts
- Gather user profile information

Control Permissions and Sharing

File/Folder Permissions

- Add file/folder permissions
- Copy file or folder permissions
- Remove permissions (file or folder)

File/Folder Sharing

- Share a Windows folder
- Change Windows file share permissions
- Remove Windows file share
- Enable/disable administrative shares

Ensure Consistent End User Experience

Software Installation

- Simple MSI installer
- Simple EXE installer
- Force SCCM Windows Software Installation Cycle

Desktop Shortcuts

- Create a shortcut on the desktop
- Update shortcut target and working directory paths

User Notifications

- Enable or disable Security Center displaying messages
- Enable or disable Message Center
- Enable or disable toast notifications
- Show a device return notification

System Personalization

- Add font
- Change the time zone to a specific time zone name
- Change Windows wallpaper
- Enable or disable Windows optional feature
- Gather Windows features

User Interaction

- Enable or disable AutoPlay
- Enable or disable Cortana
- Enable or disable Quick Access
- Pin or unpin the OneDrive icon

Streamline Device Maintenance

Optimize Device Performance

Optimize Start-up Behavior

- Change what power buttons do
- Enable or disable start-up delay
- Enable or disable Windows Hello biometrics
- Enable or disable background image on login screen
- Enable or disable the legal notice message on the login screen
- Audit the startup programs

Adjust Standby/Screensaver Settings

- Change display standby settings
- Enable or disable the 3D-text screensaver
- Copy new screensaver and set as default screensaver
- Disable screensaver
- Change screensaver settings

Optimize Hibernation/Shutdown Behavior

- Change what closing the lid does
- Enable or disable hibernation
- Enable or disable fast shutdown

Manage Page File Configuration

- Set page file size based on RAM percentage
- Change page file size
- Enable automatic management of page files on a device
- Enable or disable clear page file on shutdown

Configure Restore Points

- Create a system restore point on a device
- Change system restore frequency

Ensure Linux Compatibility

- Detect Windows Subsystem for Linux 2 (WSL2)

Scale Trouble-shooting and Maintenance

Detect Events and Errors

- Set event viewer log sizes
- Collect frequent errors and warnings of event logs
- Export events log
- Search event ID
- Search event string

Control Applications

- Start a Windows application
- Control Services
- Add Windows service
- Enable or disable a Windows service
- Start/stop/restart Windows service
- Remove Windows service

Control Processes

- Start processes with optional arguments
- Kill Windows process
- Stop Windows process
- Cancel all local printer jobs

Automate Regular Maintenance

- Create hourly, daily, weekly, monthly or quarterly scheduled tasks
- Collect all scheduled tasks
- Delete scheduled task

Audit System Details

Gather Hardware Details

- Collect hardware information
- Get printers report
- Collect local disks information

Confirm Storage Status

- Export disk space information
- Get folder size report on local drives
- Collect information recursively about files in a specified folder

STRENGTHEN SECURITY POSTURE

Maintain operating system Health

Assess Vulnerabilities

- Detect ZombieLoad or MDS vulnerability
- Meltdown and Spectre vulnerability assessment
- Search for an installed hotfix
- Report latest required Windows updates
- Report failed Windows updates

Enforce Windows Updates

- Windows Update configuration
- Force SCCM Windows Update Evaluation Cycle
- Disable Windows Update sharing/Windows delivery optimization
- Enable or disable the auto-restart notification window

Manage Windows Licensing

- Change OS licensing from MAK to KMS

Adjust Network and Firewall Configuration

Adjust Network Settings

- Add/modify hosts file entry
- Remove or comment out a hosts file entry
- Restore the previous hosts file version
- Back up and clear hosts file
- Config static DNS
- Enable DHCP for DNS
- Flush DNS resolver cache
- Release/renew IP address
- Flush ARP tables
- Enable or disable the IPv6 of a system
- Enable or disable SMBv3 compression

Adjust Firewall Rules

- Add firewall application rule
- Add firewall port rule
- Remove firewall application / port rules
- Reset advanced firewall settings

Enforce standard device configurations

Force Group Policy Updates

- Force GPupdate (machine)
- Force GPupdate (user)
- Ensure Endpoint Protection
- Force heartbeat check-in of Symantec Endpoint Protection client
- Force System Center Endpoint Protection / Windows Defender Check-in

Audit and Remove Software

- Collect .exe files
- Uninstall Chrome browser
- Uninstall Firefox browser
- Uninstall HP Assistant software
- Remove Microsoft Intune

Optimize SCCM Performance

- Force SCCM Check-in
- Clear SCCM Cache
- Force the Absolute Report & Repair to report the proper SCCM version

Adjust Configurations

- Merge a .reg file into the registry
- Replace a string value in a text file
- Create or change the value of a Windows registry key

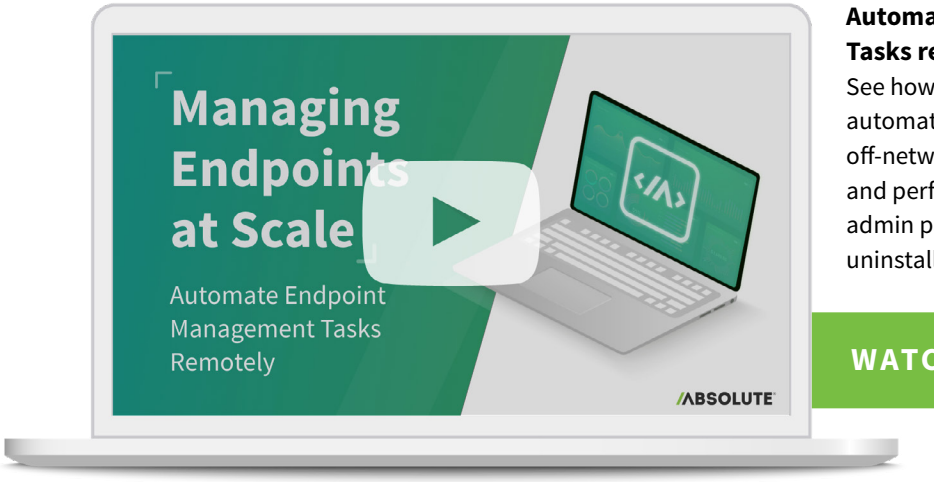
Respond to Risk with Flexibility

Prevent Data Leaks

- Enable or disable USB removable media
- Disable writing to USB storage
- Empty recycle bin

Pinpoint Missing Devices

- Unmute and set volume level
- Play beep on a device
- Mute computer
- Get GPS location



Automate Endpoint Management Tasks remotely and at Scale

See how Absolute Reach lets you automate and extend your IT capabilities off-network. Remotely gather information and perform critical actions like setting admin passwords and installing or uninstalling applications.

WATCH VIDEO

ABOUT ABSOLUTE

The Absolute Platform for Endpoint Resilience® enables devices and security controls to maintain a secure operational state automatically, without user intervention. Embedded in the firmware of over half a billion devices, Absolute is uniquely able to provide continuous visibility, control, and intelligence of the entire endpoint environment — data, devices, and applications. Our self-healing connection and granular endpoint telemetry allow IT and security teams to streamline device management, maintain compliance, remediate threats, and ensure that endpoint security controls are always installed, effective, and delivering their intended ROI. See how it works at **absolute.com** and follow us at **@absolutecorp**.

EMAIL:
sales@absolute.com

PHONE:
North America: 1-877-660-2289
EMEA: +44-118-902-2000

SALES:
absolute.com/request-a-demo

WEBSITE:
absolute.com

SUPPORTED PLATFORMS: