DATASHEET

Absolute Resilience for Security

Proactive Patch Management Built for Modern Threats and Multi-Client Environments



Absolute Resilience for Security is a cloud-based patch management solution designed to help organizations proactively detect and remediate operating system and software vulnerabilities across their endpoint fleet. Built on Absolute's award-winning platform and powered by its patented Persistence® technology, the solution provides always-on visibility and control, even on compromised or remote devices. It includes comprehensive support for OS and third-party application patches, advanced scanning, automated patch deployment, and compliance reporting — all accessible through the Absolute Console. For MSPs, it offers the operational scale, automation, and resilience needed to deliver secure, uninterrupted service across multiple client environments.

Why MSPs Choose Absolute Resilience for Security

In a world where endpoint vulnerabilities are weaponized within hours and customers expect immediate response, MSPs must deliver reliable, automated patch management as a foundational security service. Absolute Resilience for Security empowers MSPs to provide seamless, real-time visibility and control over patch health across diverse and distributed customer environments — all from a centralized console.

With Absolute's firmware-embedded Persistence® technology, MSPs can ensure always-on visibility, even if devices are off-network, compromised, or remote. It's a differentiated offering that helps MSPs reduce risk, boost compliance, and deliver superior service.

Key Capabilities Tailored for MSPs

Centralized Patch Management

- Unified console to assess patch health across multi-tenant client environments
- Supports Windows, macOS, Linux, and major third-party applications

Proactive Vulnerability Response

- Detect unpatched vulnerabilities in real-time
- Patch deployment scheduling to minimize end-user disruption
- Automatic patch content updates within 24 hours of release
- Identify and report configuration-based vulnerabilities—such as open ports, disabled firewalls, or outdated settings—with actionable insights to support compliance and remediation.

Compliance-Ready Reporting

- Audit-ready reports aligned with NIST, GDPR, CCPA, HIPAA, and PCI
- Demonstrate value to clients with regular patch compliance reporting

Always-On Connection

- Embedded in the BIOS of 600M+ PCs for resilient endpoint management
- Ensures continued control even when devices are offline or tampered with

Flexible Policy Management

- Schedule patching windows based on client-specific SLAs or operational hours
- Maintain endpoint compliance without impacting end-user productivity

MSP Benefits at a Glance

- **Increase Recurring Revenue:** Offer premium security services with enterprise-grade patch automation and compliance monitoring.
- **Reduce Operational Overhead:** Streamline patching across thousands of endpoints with minimal technician intervention.
- **Enhance Client Trust and Retention:** Proactively protect client environments and demonstrate results with automated, compliance-aligned reporting.
- **Ensure Business Continuity:** Minimize exposure to vulnerabilities by rapidly identifying and remediating risks across all managed devices.
- **Multi-Tenant Management:** Deliver services to multiple customers through a unified console with role-based access controls.
- **Build a Differentiated Security Offering:** Combine proactive patch management with Absolute capabilities offered through other Secure Endpoint product tiers – like Visibility, Control, Resilience and Resilience for Automation – for a layered, zero-trust aligned security strategy.
- **Detect More Than Just Missing Patches:** Go beyond traditional patching with visibility into configuration-related vulnerabilities that may expose client environments to risk.

Get Started with Absolute Resilience for Security

Join 21,000 global organizations leveraging Absolute Security to secure over 14 million endpoints. Future-proof your security stack and grow your MSP business with a solution built for resilience, automation, and scale.

Absolute Visibility

Source of truth for device and application health.

What's Included

- ✓ Device Health
- ✓ Security Posture
- ✓ Device Usage
- ✓ Geolocation
- ✓ Web Application Usage
- ✓ Endpoint Data Discovery

Absolute Control

Lifeline to protect at-risk devices and data.

All Visibility capabilities, plus

- ✓ Geofencing
- ✓ Device Freeze
- ✓ File Delete
- ✓ Device Wipe
- ✓ End User Messaging
- ✓ Remote Firmware Protection

Absolute Resilience

Delivers application self-healing and endpoint recovery from unexpected downtime.

All Control capabilities, plus

- ✓ Application Health
- ✓ Application Resilience
- ✓ Remediation Script Library
- ✓ Investigations and Recovery of Lost/ Stolen Devices
- ✓ Rehydrate

Absolute Resilience for Security

Seamless and proactive patch management.

All Resilience capabilities, plus

- ✓ Patch Management
- ✓ Third-Party Application Patching
- ✓ Patch Compliance Reporting

MOST POWERFUL

Absolute Resilience for Automation

Remediation of security vulnerabilities through automated workflows.

All Resilience for Security capabilities, plus

- ✓ Vulnerability Remediation
- ✓ Continuous Monitoring
- ✓ Intelligent Automation and Workflows

Request a Demo

Or **contact us** to learn how Absolute can become a core part of your managed security stack.



ABSOLUTE®

Absolute Security is partnered with more than 28 of the world's leading endpoint device manufacturers, embedded in the firmware of 600 million devices, trusted by thousands of global enterprise customers, and licensed across 16 million PC users. With the Absolute Security Cyber Resilience Platform integrated into their digital enterprise, customers ensure their mobile and hybrid workforces connect securely and seamlessly from anywhere in the world and that business operations recover quickly following cyber disruptions and attacks. Our award-winning capabilities have earned recognition and leadership status across multiple technology categories, including Zero Trust Network Access (ZTNA), Endpoint Security, Security Services Edge (SSE), Firmware-Embedded Persistence, Automated Security Control Assessment (ASCA), and Zero Trust Platforms.

Learn More

ABSOLUTE SECURITY, ABSOLUTE, the ABSOLUTE LOGO, SYXSENSE, and NETMOTION are registered trademarks of Absolute Software Corporation ©2025, or its subsidiaries. All Rights Reserved. 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. Absolute Security is a Crosspoint Capital portfolio company. ABT-Resilience-for-Security-DS-072125