DATASHEET

Absolute Resilience for Automation

Respond Quicker to Security Vulnerabilities through Automated Workflows

The advent of remote and hybrid work along with the increasing number of partners and suppliers has expanded the average organization's digital footprint. This results in heightened risk of potential security vulnerabilities, misconfigurations and blind spots being exploited by threat actors to access critical systems and initiate widespread security events through malware or ransomware. With the complexity and number of such incidents on the rise, organizations must enforce cyber resilience across their endpoints and digital environment to ensure their attack surface is minimized. Furthermore, increased pressure on IT resources due to budgetary constraints means leveraging automation as part of security operations and incident response is vital.

Responding to security vulnerabilities and misconfigurations across multiple systems

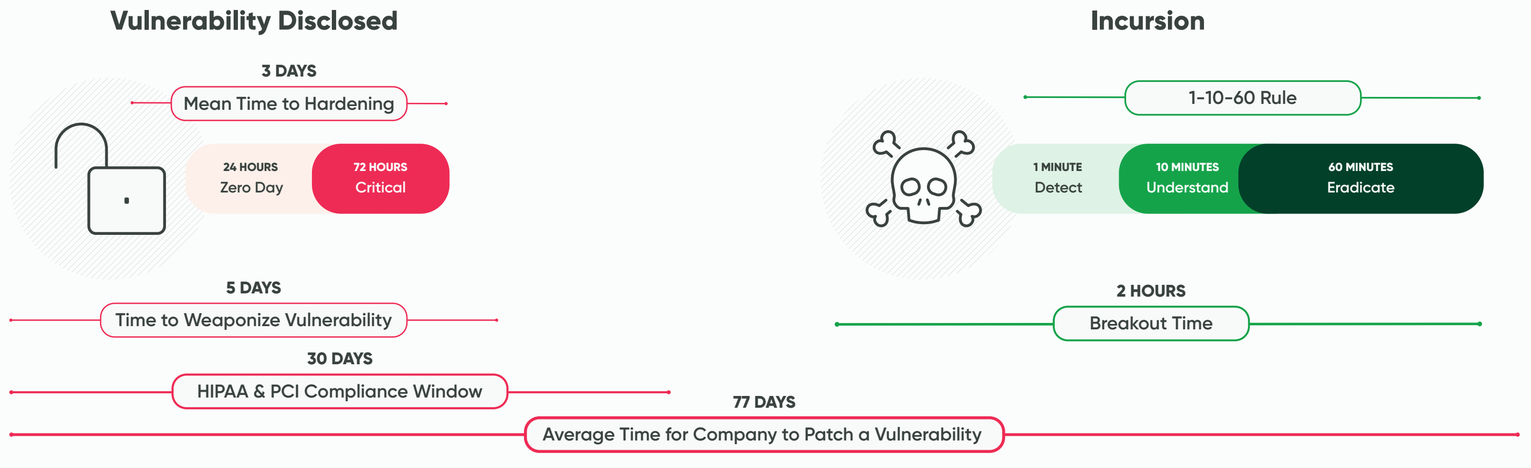
Vulnerabilities can originate from several sources within an organization's perimeter. Examples include security flaws in software and operating systems that haven't been addressed by updates, weak passwords or the reusing of passwords across multiple accounts and improperly configured network settings or firewall rules that create openings for hackers to penetrate a system. On average it takes 5 days for threat actors to weaponize disclosed vulnerabilities and typically 77 days for the average corporation to remediate it through a patch deployment[1]. Hence, there is a clear gap in the ability to identify and respond to security issues in an efficient and timely manner to limit the organization's exposure and attack surface.

Challenges IT and security teams face in responding to misconfigurations and security vulnerabilities:

- ✓ **Unpatched vulnerabilities** Known security flaws in software and operating systems that haven't been addressed by updates.
- ✓ **Outdated software** Not updating software regularly leaves systems exposed to known vulnerabilities that hackers can exploit.
- ✓ **Poor password practices** Using weak passwords or reusing the same password across multiple accounts makes it easier for hackers to gain access.
- ✓ **Misconfigured security settings** Improperly configured network settings or firewall rules can create openings for hackers to penetrate a system.
- ✓ **Remediation urgency** The time sensitive nature of identifying and responding to security vulnerabilities can have a big impact on the amount of damage a threat can have within an environment.

AVERAGE TIMELINE FOR

Disclosed Vulnerabilities, Security Incursions Into an Organization's Environment & Their Respective Response Times[2, 3, 4]



1 2018 State of Endpoint Risk Report by the Ponemon Institute

2 2018 State of Endpoint Risk Report by the Ponemon Institute, Mean Time to Hardening: The Next-Gen Security Metric, The 1/10/60 Minute Challenge: A Framework for Stopping Breaches Faster, U.S. Department of Health and Human Services

3 The State of Patch Management 2025 Report, Adaptiva

4 How quickly do hackers exploit vulnerabilities? The answer may disturb you, cybernews.com

SOURCES WHERE

Security Vulnerabilties Can Originate

Harvest the Power of the Absolute Resilience Platform

Absolute Resilience for Automation™, the highest edition of the Secure Endpoint product, offers automated remediation of operating system, software and security vulnerabilities to eliminate risk and reduce an organization's attack surface. It combines all the capabilities of Absolute Visibility™, Absolute Control™, Absolute Resilience™ and Absolute Resilience for Security™ with two additional critical features, Remediate and Automate.

The Remediate module enables IT and Security teams to scan and monitor for OS and security vulnerabilities, misconfigurations, authorization issues and run remediations workflows from an extensive library to secure devices at the push of a button.

Furthermore, Automate enables practitioners to leverage the workflow builder, a unique and easy-to-use visual framework to create and deploy custom remediation workflows without requiring any advanced coding or scripting expertise. You can build multi-step actions that can be executed directly at the endpoint, reestablishing control and eliminating risk. Once the workflows have been established, utilize policies to detect behavioral and state changes on endpoints in real-time and execute self-healing workflows to harden endpoints and improve compliance.

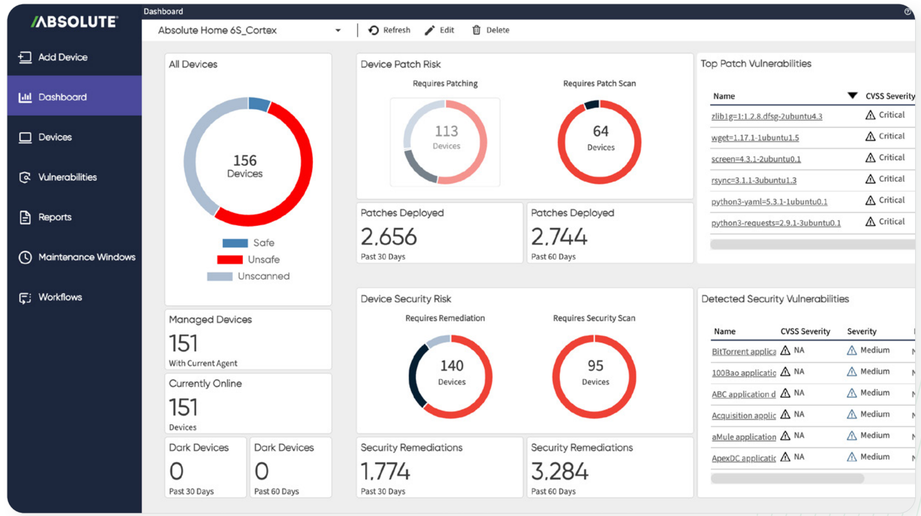
Both modules can be orchestrated from the cloud-based Absolute Console which is part of the Absolute Resilience Platform. The capabilities leverage the always-on connection provided by Absolute Persistence® technology, embedded in more than 600 million devices from leading system manufacturers.

Seamless and Automated Remediation Across Varied Exposures

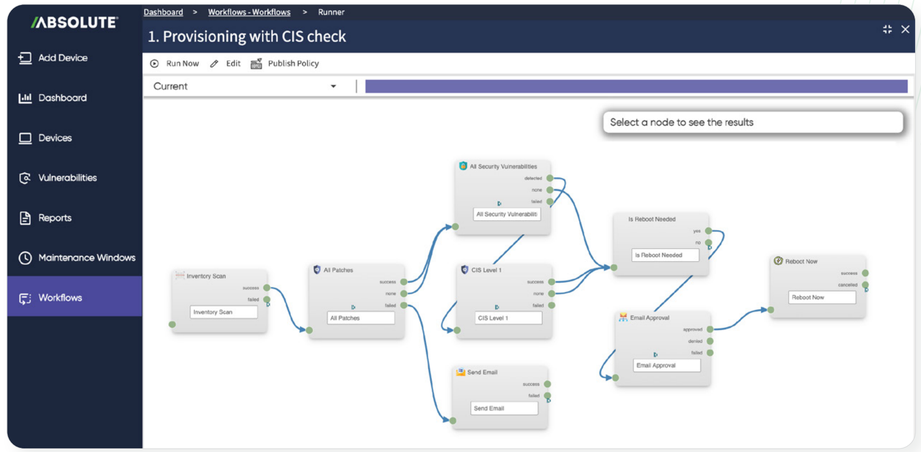
Absolute Resilience for Automation offers automated remediation of operating system, software and security vulnerabilities to eliminate risk and reduce an organization's attack surface.

Key Capabilities

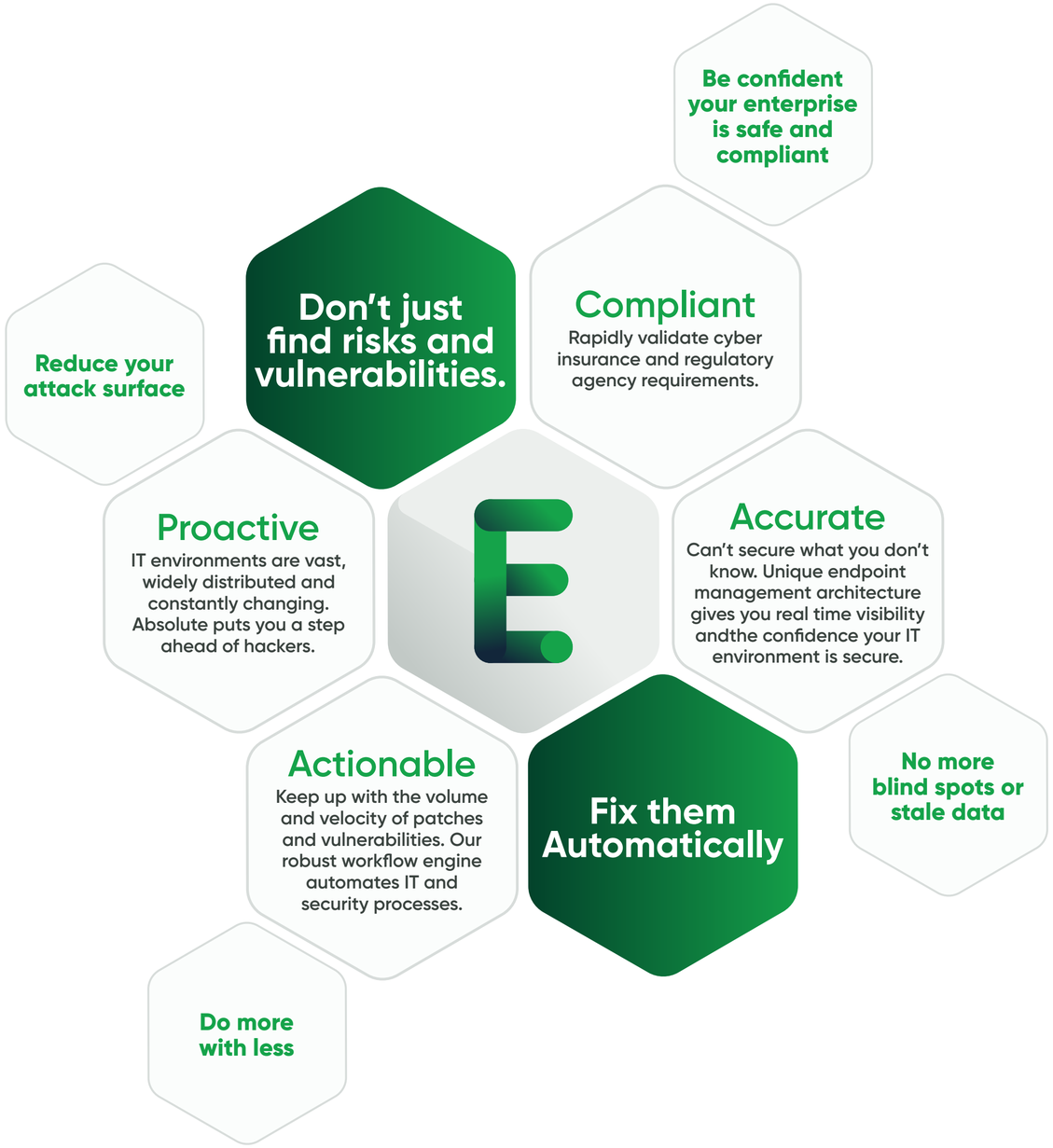
- Scan for operating system and security vulnerabilities, misconfigurations, authorization issues and more and protect against a potential breach before it occurs.
- Deploy remediation scripts: Access an extensive library of prebuilt remediation workflows to secure devices at the push of a button. The workflows can be customized using the automation workflow builder with no coding required to deploy complex remediations that would otherwise require advanced scripting.
- Build multi-step actions using the builder to reestablish control and eliminate risk at the endpoint.
- Access thousands of workflows for existing vulnerabilities as well as new content when it is published in your console as new vulnerabilities are discovered.
- Policy automation: Detect behavioral and state changes on endpoints in real-time and execute self-healing workflows to harden endpoints and improve compliance.



Dashboard showcasing risk associated with patch health and security remediations.



Defining automated remediation workflows using the Cortex builder.



Benefits to Enterprise and Medium Sized Organizations

- ✓ Continuous visibility and compliance against OS and security vulnerabilities for distributed devices.
- ✓ Reduced attack surface without hiring experienced staff.
- ✓ Increased productivity through automation.
- ✓ Combined patch and vulnerability management using live, real-time data to eliminate both OS vulnerabilities and security weaknesses.
- ✓ Security content moves beyond operating system and third-party software vulnerabilities to detect security weaknesses like user account misconfigurations, insecure passwords, out of date antivirus or definitions, disabled firewalls or BitLocker, crypto mining software and open ports.
- ✓ Automation workflows help reduce the mean time to respond to vulnerabilities limiting the attack surface for threat actors to exploit.
- ✓ Reduce load on IT and security teams tasked with identifying and responding to security risks.

Choose According to Your Business Needs

The Absolute Secure Endpoint offers a variety of product editions to choose from, tailored for your organization's IT and security needs.

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

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 21,000 global enterprises, and licensed across 14 million PC users. With the Absolute Security 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.

Request a Demo