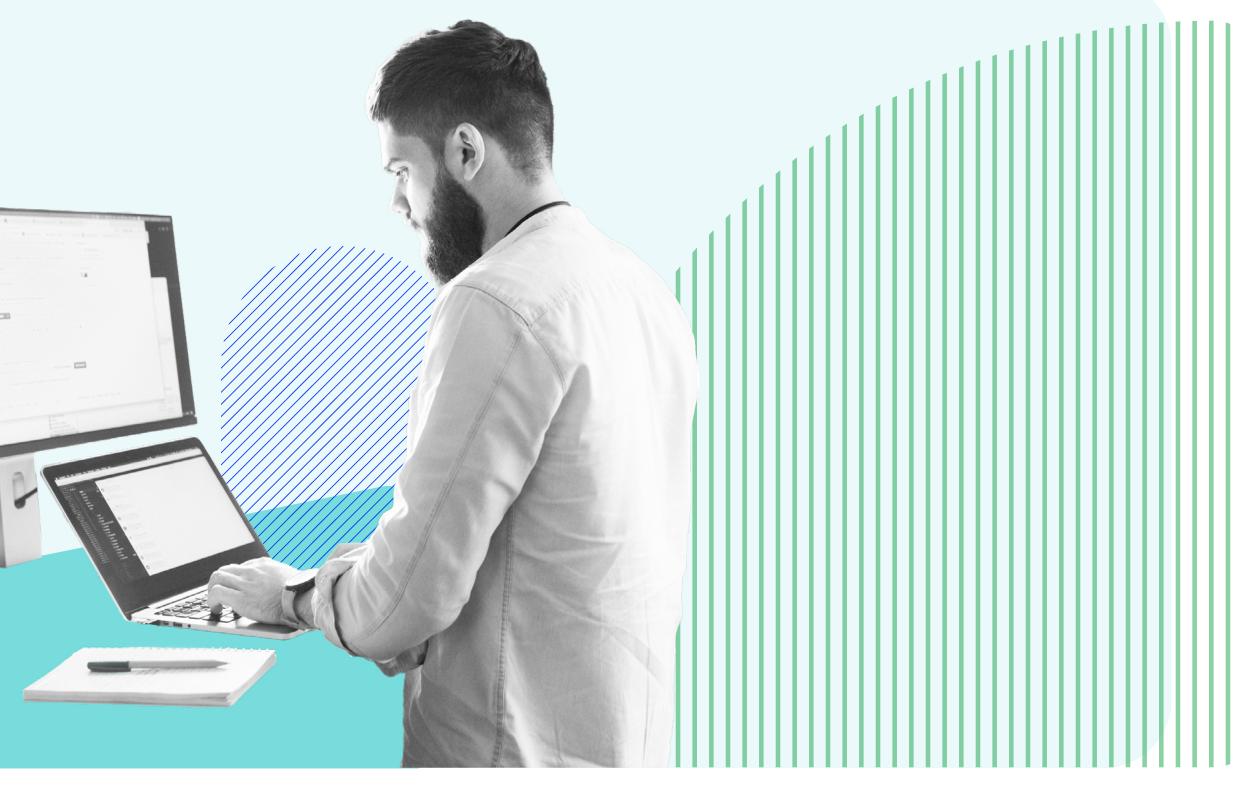
DATASHEET

Absolute Resilience for Security

Proactively Assess Patch Health for Known Operating System and Software Vulnerabilities

E

With the rise in the number and complexity of malware and ransomware attacks as well as IT issues causing widespread BSOD incidents, organizations must enforce cyber resilience across their endpoints through both proactive and remedial measures. One of the fundamental tasks of any IT team is to continuously assess and deploy operating system and software patches to limit exposure to known vulnerabilities that can be exploited by threat actors. This unfortunately can be arduous and time-consuming for capacity-strained IT teams, given the velocity of exposures being disclosed across multiple operating system platforms and software types. Nonetheless, leaving devices unpatched for too long expands the attack surface that threats actors can invariably exploit. Hence, running an efficient and reliable patch management process is essential for organizations of all sizes in today's digital environment.





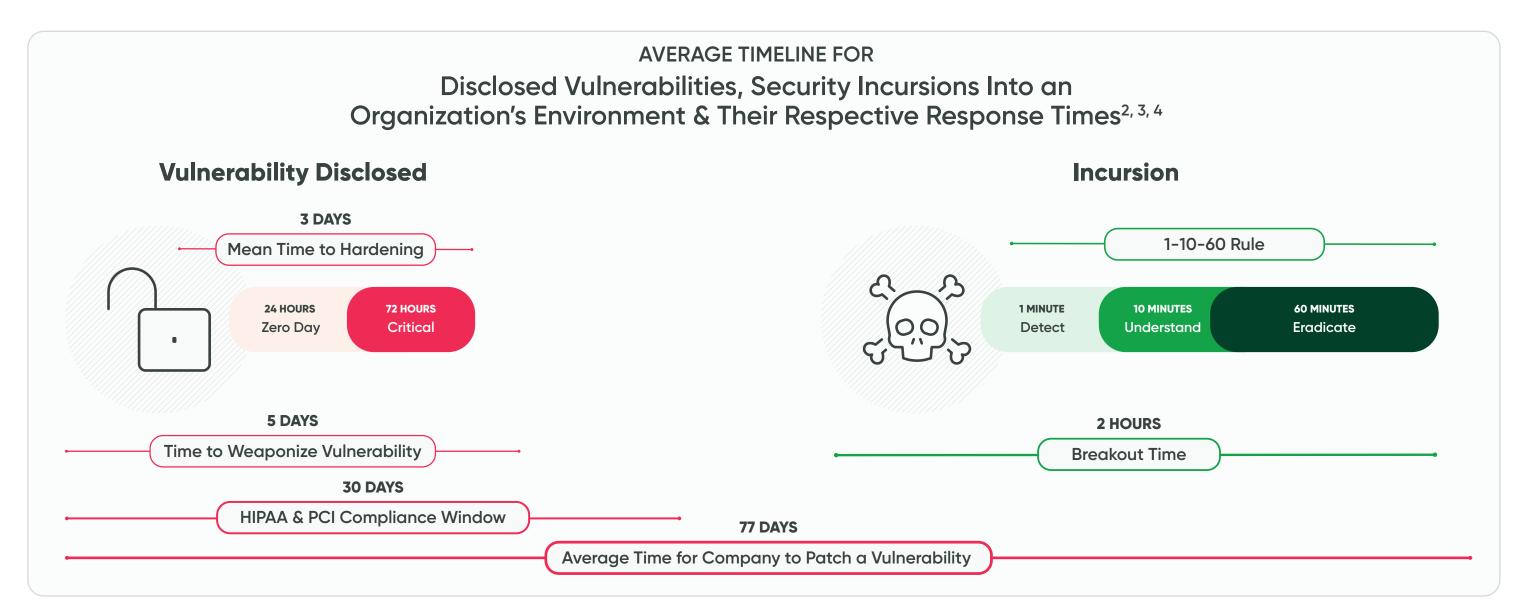
The Need for Seamless Patch Management

Remote and hybrid work policies are here to stay, whether it be across large enterprises or medium sized businesses. As a result, IT and security teams are required to manage and secure endpoint environments that are geographically dispersed. Employees work from a variety of locations today whether it be the company headquarters, the employee's home office or public locations such as a coffee shop or the airport. This ultimately leads to administrators having varying levels of visibility and control across the endpoint fleet. The result? Increased complexity in assessing endpoint compliance factors such as patch health and responding to disclosed vulnerabilities for different operating systems and software deployed across remote devices. Some key challenges that administrators face with respect to patch management include:

Challenges faced by IT and Security teams related to Patch Management:

- Assessing patch health across a remote endpoint population can be time consuming and is highly dependent on the network quality of devices connecting to the corporate network. Devices connecting through unreliable and unsecure public Wi-Fi connections may take time to update.
- Known security flaws in software and operating systems that haven't been addressed by updates. Not updating software regularly leaves systems exposed to known vulnerabilities that hackers can exploit.
- Year Patch management and remediation is a time sensitive exercise needing to be completed swiftly to limit exposure. As shown in figure 1 below, on a patch deployment.¹

Maintaining patch health is essential in complying with cybersecurity frameworks such as the National Institute of Standards and Technology (NIST) and data regulations such as the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR).



average it takes 5 days for threat actors to weaponize disclosed vulnerabilities and typically 77 days for the average corporation to remediate it through

- 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



Harvest the Power of the Absolute Resilience Platform

Absolute Resilience for Security[™] offers seamless patch management for organizations to employ proactive assessment and deployment of operating system and software patches across their endpoints to fortify their security posture. It combines all the capabilities of Absolute Visibility™, Absolute Control™ and Absolute Resilience[™] with the Patch module, enabling IT and security teams to scan their endpoint population to assess patch health in relation to known operating system and software vulnerabilities.

The Patch module can be orchestrated from the cloud-based Absolute Console which is part of the Absolute Platform. The capability leverages the always-on connection provided by Absolute Persistence[®] technology, embedded in more than 600 million devices from leading system manufacturers.

Key Capabilities

- Unified assessment of patch health for automatic detection and deployment.
- Sophisticated patch scanning detection logic to flag devices with operating system or software vulnerabilities.
- Solution Flexible scheduling of patch deployments to ensure end user productivity is protected.
- Automatic availability of patch content appearing in the Absolute Console within 24 hours or less. Content includes:
 - > Operating system and security patches for Windows, Mac and Linux.
 - > Third-party patches include updates to applications like Adobe Acrobat Reader, Google Chrome, Zoom, TeamViewer, Evernote, Java, Firefox, and any other software not directly developed by the OS manufacturer.

/ABSOLUTE	Dashboard > Maintenance Windo	ows - Maintenance Window	<u>rs</u> > Maintenar	nce Window - Config				
///BSOLUTE	Maintenance Windo	w - Config					0	# ×
+ Add Device	<	🖺 Save 🚫 Cancel						
Lul Dashboard	INFORMATION	Details				Blackout Hours		
	Config	Name	Patch Tuesday		R)	Enabled		
Devices	Tasks	Starts at	2 00	hour (24:00) 0 🕒 🕀 m	inutes	Start	End	
	Folicies	Duration	2 00	hours 0 🔿 🗭 m	inutes	08:00	18:00	\$
C Vulnerabilities		TimeZone	(UTC+02:00) Helsin	ki, Kyiv, Riga, Sofia, Tallinn, Vilr	nius 👻	Include weekends		
North			Restart tasks aga	ain until window ends				
Reports			🔲 Use local time (o	only for Cortex policies)				
		Recurrence						
Maintenance Windows		O Weekly	O Monthly	Last day of each Month (Patch Tuesday			
ج Workflows		Occurs		0 🕒 🔂 Day(s) After F	Patch Tuesday			
		 After Patc 	h Tuesday on the	1st 👻				
		🗌 Monday	Tuesday	🗌 Wednesday 🔲 Thurso	day			
		🗌 Friday	Saturday	Sunday				

Configuration to schedule patch deployments across devices.

ABSOLUTE RESILIENCE FOR SECURITY / SECURE ENDPOINT / DATASHEET

/ABSOLUTE [®]	Dashboard > Reports Reports				
+ Add Device	i≣ View Details				
III Dashboard	All Devices	Clear			
	All Patches Patching	Clear			
বি Vulnerabilities	Name	Description	Category	Version	Favorite 🔻
Reports	Patch Deployment History by Patch	history of patch deployments by Patch.	Patching	v5.0.0	
() Maintenance Windows	HIPAA Operating System	Displays the compliance of your environment and details each of the devices and patches which are non- compliant	Patching	v5.0.0	
	and Application Vulperability Scan Patch Deployment History by Device	details each of the devices and patches which are non- compliant History of patch deployments by Device.	Patching Patching	v5.0.0 v5.0.0	
Maintenance Windows	and Application Vulnerability Scan Patch Deployment History by Device SOX Operating System and Application Vulnerability	details each of the devices and patches which are non- compliant History of patch deployments by Device. Displays the compliance of your environment and details each of the devices and patches which are non-	Patching		
	and Application Vulnerability Scan Patch Deployment History by Device SOX Operating System and Application Vulnerability Scan PCI DSS Operating System and Application	details each of the devices and patches which are non- compliant History of patch deployments by Device. Displays the compliance of your environment and details each of the devices and patches which are non- compliant Displays the compliance of your environment and details each of the devices and patches which are non-	Patching Patching	v5.0.0	
	and Application Vulnerability Scan Patch Deployment History by Device SOX Operating System and Application Vulnerability Scan PCI DSS Operating System	details each of the devices and patches which are non- compliant History of patch deployments by Device. Displays the compliance of your environment and details each of the devices and patches which are non- compliant Displays the compliance of your environment and details each of the devices and patches which are non- compliant Risk statistics by Device Type, count of Missing Patches, deployment of Patches, Bitlocker status and a Risk Timeline	Patching Patching Patching Patching	v5.0.0 v5.0.0	
	and Application Vulnerability Scan Patch Deployment History by Device SOX Operating System and Sox Operating System and PCI DSS Operating System and Application Vulnerability Scan Security Patch Risk	details each of the devices and patches which are non- compliant History of patch deployments by Device. Displays the compliance of your environment and details each of the devices and patches which are non- compliant Displays the compliance of your environment and details each of the devices and patches which are non- compliant Risk statistics by Device Type, count of Missing Patches, deployment of Patches, Bitlocker status and a	Patching Patching Patching Patching	v5.0.0 v5.0.0 v5.0.0	

Suite of reports showcasing patch compliance across various security frameworks and data regulations.

Absolute Resilience for Security empowers your IT and security teams to efficiently ensure devices are kept up to date with the latest operating system and software patches, thereby limiting exposure to known vulnerabilities that threat actors look to exploit.

Benefits for Large Enterprises and Medium Sized Businesses

- ✓ Faster patch deployment to respond to known OS and software issues.
- ✓ Improved reporting to prioritize devices based on their risk exposure.
- ✓ Reduced attack surface and strengthened security posture.
- Continuous visibility and compliance of distributed devices against operating system and software issues.



Looking for additional automation and remediation capabilities?

While Absolute Resilience for Security provides seamless patch management to ensure your endpoints are protected from known OS and software exposures, check out Resilience for Automation to protect against thousands of known security vulnerabilities and misconfigurations as well as the ability to create automated remediation workflows.

Absolute Visibility

Source of truth for device and application health.

What's Included

- ✓ Device Health
- ✓ Security Posture
- **Device Usage** \checkmark
- ✓ 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 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



ABSOLUTE SECURITY, ABSOLUTE, the ABSOLUTE LOGO, 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 ^m 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-AbsoluteResilienceSecurity-DS-012025

