DATENBLATT

Absolute Resilience for Security

Proaktive Bewertung des Patch-Status hinsichtlich bekannter Schwachstellen an Betriebssystemen und Softwareprogrammen

Immer häufiger und komplexer werdende Malware- und Ransomware-Angriffe sowie durch vermehrte IT-Probleme ausgelöste Bluescreen-Fehler zwingen Unternehmen zur Durchsetzung von Cyberresilienz, sowohl durch vorsorgliche Maßnahmen als auch durch Remediation. Eine der Hauptaufgaben jedes IT-Teams ist die fortlaufende Bewertung und das ständige Deployment von Betriebssystem- und Software-Patches. Bekannt gewordene Sicherheitslücken müssen geschlossen werden, damit sie nicht von Bedrohungsakteuren ausgenutzt werden können. Leider raubt diese mühsame Arbeit den eh schon unter Druck stehenden IT-Abteilungen viel Zeit, denn für die unterschiedlichen Betriebssystemplattformen und Softwaretypen wird ständig eine Vielzahl neuer Bedrohungen bekannt. Patchen Sie Ihre Endgeräte jedoch längere Zeit nicht, vergrößern Sie Ihre Angriffsfläche und werden früher oder später Bedrohungsakteure auf den Plan rufen. Ein effizientes und verlässliches Patch-Management ist in unserer digital vernetzen Welt also für Unternehmen aller Größen unentbehrlich.

Warum Sie ein nahtloses Patch-Management brauchen

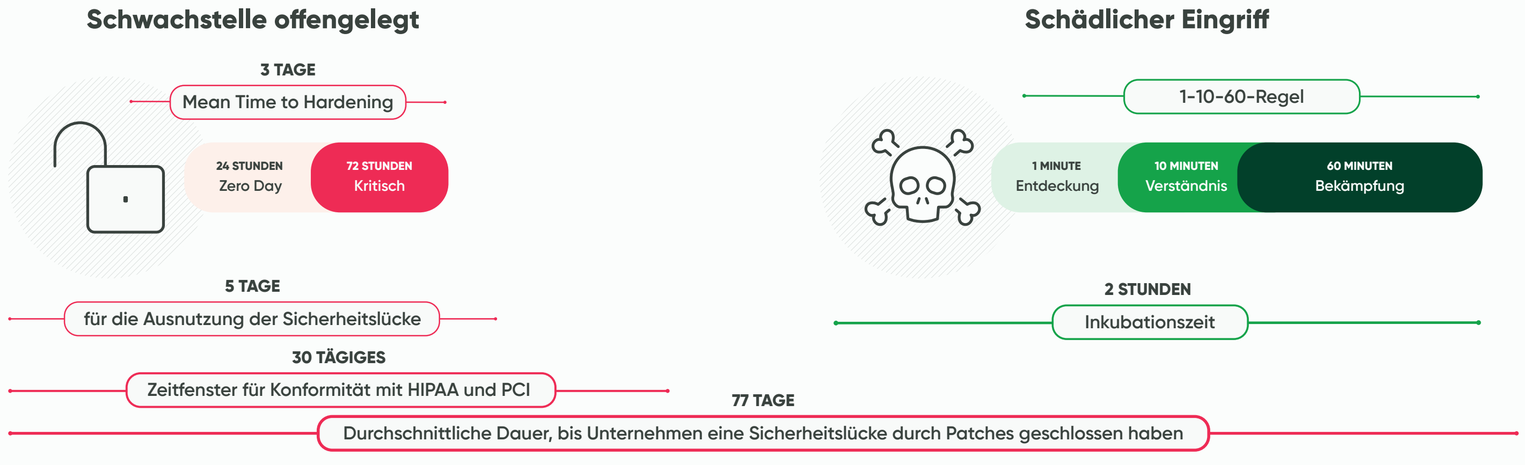
Die Remote- und Hybrid-Arbeit ist mittlerweile weder aus großen Unternehmen noch aus dem Mittelstand wieder wegzudenken. IT- und Sicherheitsabteilungen haben also die Aufgabe, geografisch weit verteilte Endpunkte in ihrer IT-Umgebung zu verwalten und abzusichern. Die heutige Belegschaft arbeitet von den unterschiedlichsten Orten, ob aus dem Hauptsitz des Unternehmens, dem eigenen Homeoffice oder auch von öffentlichen Orten wie Cafés oder Flughäfen. Im Endeffekt führt das dazu, dass Administratoren schwankende Sichtbarkeit und Kontrolle über die Endpunktflotte haben. Das Ergebnis? Es wird immer schwieriger, Compliance-Faktoren zu bewerten. Dazu gehört beispielsweise der Patch-Status und die Reaktion auf bekannt gewordene Schwachstellen diverser Betriebssysteme und Softwareprogramme, die auf den Endgeräten im Einsatz sind. Zu den größten Herausforderungen, mit denen Administratoren beim Patch-Management kämpfen, gehören folgende:

Herausforderungen des Patch-Managements für die IT-Sicherheit:

- ✓ Den Patch-Status einer ganzen Flotte remote verwalteter Endpunkte zu bewerten, kann viel Zeit kosten und hängt hochgradig von der Netzwerkqualität der sich mit dem Unternehmensnetzwerk verbindenden Geräte ab. Endgeräte, die sich über unzuverlässige und unsichere öffentliche WLAN-Netze verbinden, brauchen länger für die Aktualisierung.
- ✓ Bekannte Sicherheitslücken von Softwareprogrammen und Betriebssystemen, die nicht durch entsprechende Updates geschlossen wurden, sind ein großes Risiko. Wenn Sie Ihre Software nicht regelmäßig aktualisieren, können Hacker sich diese öffentlich bekannten Lücken zunutze machen.
- ✓ Patch-Management und Remediation sind zeitsensible Maßnahmen, die zur Schadensbegrenzung so schnell wie möglich abgeschlossen werden müssen. Wie in Abbildung 1 unten zu sehen ist, brauchen Bedrohungsakteure im Schnitt fünf Tage, um bekannt gewordene Sicherheitslücken auszunutzen. Auf Unternehmensseite hingegen dauert es durchschnittlich 77 Tage, um sich via Patch Deployment komplett von einem solchen Angriff zu erholen.[1]

Lückenloses Patch-Management ist wichtig, um die Vorgaben von Frameworks wie dem National Institute of Standards and Technology (NIST) und Datenschutzbestimmungen wie dem California Consumer Privacy Act (CCPA) oder der europäischen Datenschutzgrundverordnung (DSGVO) zu erfüllen.

Durchschnittliche Zeitverzögerung bei bekannt gewordenen Schwachstellen und sicherheitsrelevanten Eingriffen in eine unternehmerische Umgebung und die entsprechenden Reaktionszeiten[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

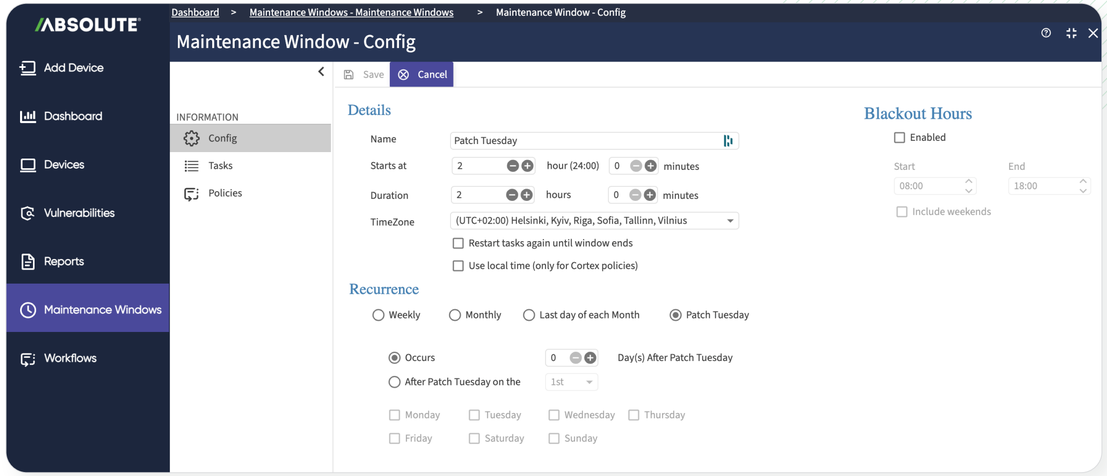
4 How quickly do hackers exploit vulnerabilities? The answer may disturb you, cybernews.com

Machen Sie sich die Power der Absolute Resilience Platform zunutze

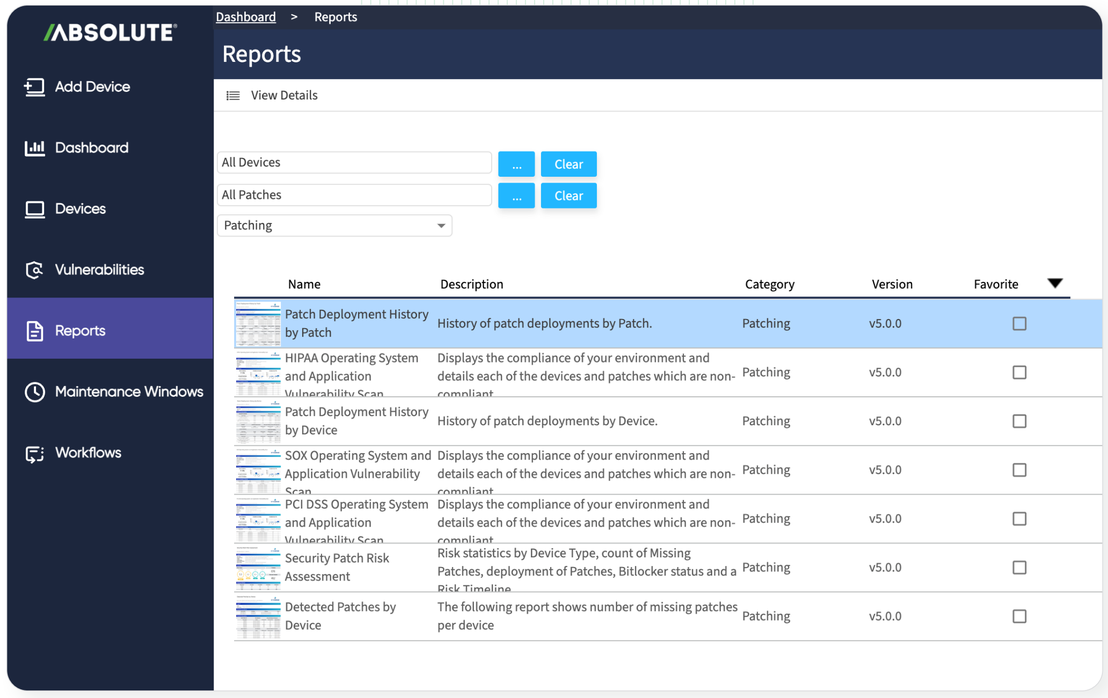
Mit Absolute Resilience for Security™ erhalten Sie nahtloses Patch-Management für Ihr Unternehmen, um Patches für Betriebssysteme und Softwareprogramme proaktiv zu bewerten und deployen. Damit stärken Sie den Sicherheitsstatus aller Ihrer Endpunkte. Das Produkt kombiniert alle Funktionen von Absolute Visibility™, Absolute Control™ und Absolute Resilience™ mit dem Patch-Modul. Damit können Ihre IT- und Sicherheitsexperten die Patches der gesamten Endpunktflotte mit bekannten Schwachstellen in Betriebssystemen und Softwareprogrammen abgleichen und bewerten. Auf das Patch-Modul können Sie direkt in der cloudbasierten Absolute® Console oder der Absolute App zugreifen. Beides ist Teil der Absolute Platform. Diese Funktion nutzt die Always-On-Konnektivität von Absolute Persistence®, die bereits in mehr als 600 Millionen Geräte führender Hersteller integriert ist.

Zentrale Funktionen:

- Einheitliche Bewertung des Patch-Status für automatisches Aufspüren und Deployment.
- Raffinierte Erkennungslogik, die vorhandene Patches scannt und Geräte mit Schwachstellen an Betriebssystemen oder Softwareprogrammen meldet.
- Flexible Terminierung der Patch-Deployments, um die Produktivität der Endbenutzer nicht zu stören.
- Die Patches stehen nach maximal 24 Stunden automatisch in der Absolute Console bereit. Dazu gehören:
  - Betriebssystem- und Sicherheitspatches für Windows, Mac und Linux.
  - Drittanbieter-Patches inklusive Updates für Anwendungen wie Adobe Acrobat Reader, Google Chrome, Zoom, TeamViewer, Evernote, Java, Firefox und andere nicht direkt vom Hersteller des Betriebssystems entwickelte Programme.



Einstellungen für die Terminierung von Patch-Deployments aller Endgeräte.



Auswahl an Berichten über die Patch-Compliance anhand verschiedener Frameworks zur IT-Sicherheit und Datenschutzregulierungen

Mit Absolute Resilience for Security geben Sie Ihren IT-Experten mehr Möglichkeiten an die Hand, die Betriebssystem- und Software-Patches Ihrer Endgeräte effizient auf den aktuellsten Stand zu bringen. Damit begrenzen Sie die Zeitspanne, in der Sie bekannten Schwachstellen ausgesetzt sind, auf die Bedrohungsakteure nur warten.

Vorteile für große Unternehmen und mittelständische Betriebe:

- ✓ Schnelleres Patch-Deployment als Reaktion auf bekannte Probleme mit Betriebssystemen und Softwareprogrammen.
- ✓ Verbessertes Reporting für die Priorisierung von Endgeräten basierend auf ihrem Gefährdungspotenzial.
- ✓ Verkleinerte Angriffsfläche und gestärkter Sicherheitsstatus.
- ✓ Ausgegebene Endgeräte mit kontinuierlicher Sichtbarkeit und Compliance statt mit unsicheren Betriebssystemen und Softwareproblemen.

Sie benötigen zusätzliche Funktionen für die Automatisierung und Remediation?

Absolute Resilience for Security gibt Ihnen nahtloses Patch-Management an die Hand, das Ihre Endpunkte zuverlässig vor Sicherheitslücken in Betriebssystemen und Software schützt. Sie benötigen mehr? Mit Absolute Resilience for Automation schützen Sie sich vor tausenden bekannten Sicherheitsmängeln und Fehlkonfigurationen und können automatisierte Workflows für die Remediation erstellen.

Absolute Visibility

Source of Truth für den Zustand von Geräten und Anwendungen.

Das ist enthalten

- ✓ Gerätezustand
- ✓ Sicherheitsstatus
- ✓ Gerätenutzung
- ✓ Geolokalisierung
- ✓ Nutzung von Webanwendungen
- ✓ Ermittlung von Endpunktdaten

Absolute Control

Ihre Rettungsleine zum Schutz von gefährdeten Geräten und Daten.

Alle Funktionen aus Visibility, plus

- ✓ Geofencing
- ✓ Einfrieren von Geräten
- ✓ Löschen von Dateien
- ✓ Zurücksetzung von Geräten
- ✓ Benachrichtigung von Nutzern
- ✓ Remote Firmwareschutz

Absolute Resilience

Selbstheilung für Anwendungen und Wiederherstellung von Endpunkten bei unerwarteter Downtime.

Alle Funktionen aus Control, plus

- ✓ Anwendungszustand
- ✓ Anwendungsresilienz
- ✓ Sammlung von Wiederherstellungsskripts
- ✓ Nachverfolgung und Wiederbeschaffung von verlorenen/gestohlenen Geräten
- ✓ Rehydrate

Absolute Resilience for Security

Nahtloses und proaktives Patch-Management.

Alle Funktionen aus Resilience, plus

- ✓ Patch-Management
- ✓ Patching für Drittanbieter-Anwendungen
- ✓ Reporting zur Patch-Compliance

TOP-LEISTUNG

Absolute Resilience for Automation

Remediation von Sicherheitsschwachstellen und automatisierte Workflows.

Alle Funktionen aus Resilience for Security, plus

- ✓ Remediation von Schwachstellen
- ✓ Kontinuierliche Überwachung
- ✓ Intelligente Automatisierung und Workflows

ABSOLUTE SECURITY, ABSOLUTE, das ABSOLUTE-LOGO und NETMOTION sind eingetragene Handelsmarken der Absolute Software Corporation ©2025 oder ihren Tochtergesellschaften. Alle Rechte vorbehalten. Andere hier erwähnte Namen oder Firmenlogos können Marken von Absolute oder ihren entsprechenden Eigentümern sein. Das Fehlen der Symbole ™ und ® als Ergänzung zu den jeweiligen Handelsmarken oder insgesamt hierin stellen keinen Verzicht auf Eigentümerschaft an den betreffenden Handelsmarken dar. Absolute Security ist ein Portfoliounternehmen von Crosspoint Capital. ABT-AbsoluteResilienceAutomation-DS-012025

Absolute Security ist Partner von mehr als 28 der global führenden Endgerätehersteller und in die Firmware von 600 Millionen Endgeräte eingebettet. Über 21.000 internationale Unternehmenskunden vertrauen auf Absolute und mehr als 14 Millionen User sind weltweit lizenziert. Digitale Unternehmen, welche die Plattform von Absolute Security Resilience nutzen, ermöglichen ihren mobilen und hybriden Mitarbeitern, sich sicher und nahtlos von überall aus mit dem Unternehmensnetzwerk verbinden zu können. Außerdem stellen sie damit sicher, dass ihre betrieblichen Prozesse sich schnell von Cyberangriffen und Störungen erholen. Mit unseren preisgekrönten Leistungen haben wir uns ein hohes Ansehen und den Status als Branchenführer in verschiedenen Tech-Kategorien erarbeitet, darunter Zero Trust Network Access (ZTNA), Endpunktsicherheit, Security Services Edge (SSE), Firmware-Embedded Persistence, Automated Security Control Assessment (ASCA) und Zero-Trust-Plattformen.

Demonstration anfragen

ABSOLUTE SECURITY, ABSOLUTE, das ABSOLUTE-LOGO und NETMOTION sind eingetragene Handelsmarken der Absolute Software Corporation ©2025 oder ihren Tochtergesellschaften. Alle Rechte vorbehalten. Andere hier erwähnte Namen oder Firmenlogos können Marken von Absolute oder ihren entsprechenden Eigentümern sein. Das Fehlen der Symbole ™ und ® als Ergänzung zu den jeweiligen Handelsmarken oder insgesamt hierin stellen keinen Verzicht auf Eigentümerschaft an den betreffenden Handelsmarken dar. Absolute Security ist ein Portfoliounternehmen von Crosspoint Capital. ABT-AbsoluteResilienceSecurity-DS-012025