



# Absolute Secure Endpoint

Absolute Secure Endpoint setzt auf Always-On-Konnektivität durch Absolute Persistence® und ermöglicht damit IT- und Sicherheitspersonal, Hardware-Probleme anzugehen und Laptops und unternehmenskritischen Anwendungen, sich selbst zu heilen. Damit erleichtern Sie Ihr IT -Management, stärken Ihren Sicherheitsstatus und verbessern Ihre Compliance.

	Absolute Visibility	Absolute Control	Absolute Resilience	Absolute Resilience for Security	Absolute Resilience for Automation	Verfügbarkeit des Features
	Source of Truth für den Zustand von Geräten und Anwendungen.	Rettungsleine zum Schutz von gefährdeten Geräten und Daten.	Selbstheilung für Anwendungen und zuverlässige Reaktion auf Risiken.	Nahtloses und proaktives Patch-Management.	Remediation von Sicherheitschwachstellen mit automatisierten Workflows.	Nach Betriebssystem
<b>Hardware tracken<sup>14</sup></b>						
Reporting und Warnungen zu hunderten von Hardware-Attributen	✓	✓	✓	✓	✓	Windows, Apple, Linux
Berichte zum Geräte-Leasing überwachen	✓	✓	✓	✓	✓	Windows, Apple, Linux
Neu aktivierte Geräte und Verbindungshistorie tracken	✓	✓	✓	✓	✓	Windows, Apple, Linux
Entweder vorgefertigte oder benutzerdefinierte Reports nutzen	✓	✓	✓	✓	✓	Windows, Apple, Linux
Fehlende Geräte markieren und bei Verbindung mit dem Internet benachrichtigen lassen	✓	✓	✓	✓	✓	Windows, Apple, Linux
<b>Installierte Software tracken</b>						
Reporting zu installierter Software nach Gerät oder nach Population	✓	✓	✓	✓	✓	Windows, Apple
<b>Geräte-Einblicke festhalten</b>						
Definierte Datenpunkte aus der Absolute DataExplorer Library sammeln <sup>1</sup>	✓	✓	✓	✓	✓	Windows
Mit dem DataExplorer Builder die Erfassung benutzerdefinierter, auf bestimmte Bedürfnisse zugeschnittener Datenpunkte konfigurieren	●	●	✓	✓	✓	Windows

✓ ENHALTEN
● NICHT ENHALTEN
⊕ ADD-ON-FEATURE
📄 NUR REPORTING

	Absolute Visibility	Absolute Control	Absolute Resilience	Absolute Resilience for Security	Absolute Resilience for Automation	Verfügbarkeit des Features
<b>Sicherheitsstatus von Geräten bewerten<sup>14</sup></b>						
Statusbericht Verschlüsselung	✓	✓	✓	✓	✓	Windows Apple <sup>2</sup>
Statusbericht Anti-Malware	✓	✓	✓	✓	✓	Windows Apple
<b>Gerätenutzung erfassen</b>						
Gerätenutzung durch Analyse der Anmeldungen/Entsperrungen und Geräte-Interaktionen auswerten	✓	✓	✓	✓	✓	Windows Apple
Reporting zur durchschnittlichen täglichen Nutzung je Gerät	✓	✓	✓	✓	✓	Windows Apple
Reporting zu besuchten Websites und ROI der Web-Apps in Ihrer Umgebung nachvollziehen <sup>3</sup>	✓	✓	✓	✓	✓	Windows
<b>Sensible Dateien auf Geräten identifizieren</b>						
Dateien wie PII-, PHI-, DSGVO-Daten, finanzielle Informationen, sozialversicherungsrelevante Daten oder geistiges Eigentum in und außerhalb des Netzwerks entdecken	✓	✓	✓	✓	✓	Windows Apple
Risikobewertung für Daten inkl. geschätzter Wiederbeschaffungskosten durchführen	✓	✓	✓	✓	✓	Windows Apple
Geräte mit sensiblen Daten identifizieren, die sich mit einem Cloud-Speicher synchronisieren (Dropbox, iCloud, Box, OneDrive)	✓	✓	✓	✓	✓	Windows Apple
<b>Geräte-Standort überwachen<sup>14</sup></b>						
Standort der Geräte tracken inkl. 365 Tage Historie	✓	✓	✓	✓	✓	Windows Apple
Geofences definieren und nicht autorisierte Gerätebewegungen registrieren	●	✓	✓	✓	✓	Windows Apple
<b>Endgeräte aus der Ferne einfrieren</b>						
Geräte mit benutzerdefinierter Nachricht einfrieren – terminiert oder nach Bedarf <sup>14</sup>	●	✓	✓	✓	✓	Windows Apple
Offline-Timer stellen und Geräte automatisch einfrieren	●	✓	✓	✓	✓	Windows Apple
Für Extraschutz Geräte via Firmware einfrieren <sup>13</sup>	●	✓	✓	✓	✓	Windows <sup>4</sup>

✓ ENHALTEN

● NICHT ENHALTEN

⊕ ADD-ON-FEATURE

📄 NUR REPORTING



	Absolute Visibility	Absolute Control	Absolute Resilience	Absolute Resilience for Security	Absolute Resilience for Automation	Verfügbarkeit des Features
<b>Aus der Ferne Daten von Geräten löschen</b>						
Dateien selektiv löschen	●	✓	✓	✓	✓	■ Apple
End-of-Life-Datenbereinigung mit Compliance-Zertifikat	●	✓	✓	✓	✓	■ Apple
<b>Remote Firmwareschutz ermöglichen<sup>13</sup></b>						
Skalierbares Supervisor-Passwort verwalten <sup>5</sup>	●	✓	✓	✓	✓	■
<b>Sichere Endbenutzerkommunikation auf dem Gerät</b>						
Benutzer Ihrer Endgeräte durch wichtige Benachrichtigungen direkt auf ihren Bildschirmen informieren oder um Feedback bitten	●	✓	✓	✓	✓	■ Apple
<b>Sofortige und skalierbare Geräteabfrage und Korrekturen</b>						
Mehr als 130 vordefinierte Workflows aus der Reach Library ausführen	●	●	✓	✓	✓	■ Apple
Benutzerdefinierte PowerShell- oder BASH-Skripte auf Geräten ausführen	●	●	✓	✓	✓	■ Apple <sup>6</sup>
<b>Reporting zum Anwendungszustand</b>						
Grundlegende Parameter bezüglich des Anwendungszustands von über 2.000 Business-, Produktivitäts-, und Sicherheitsanwendungen auf Windows und Mac überwachen, um Ausfälle zu erfassen und Selbstheilung zu ermöglichen.	●	●	✓ <sup>7</sup>	✓	✓	■ Apple
Erweitertes Monitoring des Anwendungszustands einer ausgewählten Gruppe geschäftskritischer Sicherheitsanwendungen mit automatisierter Schadensminderung. <sup>8, 14</sup>	📄	📄	✓	✓	✓	■
<b>Selbstheilung kritischer Sicherheitsanwendungen<sup>8, 14</sup></b>						
In unserem <b>Absolute Application Resilience catalog</b> <a href="#">7</a> können Sie nachlesen, welche geschäftskritischen Anwendungen unterstützt werden.	📄	📄	✓	✓	✓	■
Andere Anwendungen <sup>9</sup>	●	●	●	●	●	■

✓ ENHALTEN

● NICHT ENHALTEN

⊕ ADD-ON-FEATURE

📄 NUR REPORTING



	Absolute Visibility	Absolute Control	Absolute Resilience	Absolute Resilience for Security	Absolute Resilience for Automation	Verfügbarkeit des Features
<b>Nachverfolgung und Wiederbeschaffung von gestohlenen Geräten<sup>13</sup></b>						
Gestohlene Geräten zurückholen	●	●	✓	✓	✓	■ Apple
Servicegarantie für nicht zurückerhaltene Geräte <sup>10</sup> (Nur für Education)	●	●	✓	✓	✓	■ Apple
<b>Rehydrate</b>						
Stellen Sie betroffene Endgeräte nach unerwarteten Störungen oder IT-Sicherheitsvorfällen aus der Ferne wieder her	●	●	✓	✓	✓	■
Nutzen Sie von Absolute voreingestellte Wiederherstellungspläne auf Firmwareebene, um Ihre Endgeräte wieder vollständig vertrauenswürdig und konform zu machen	●	●	✓	✓	✓	■
<b>Patch-Management</b>						
Geräteübergreifende und einheitliche Bewertung des Patch-Status Ihres Betriebssystems sowie automatisiertes Deployment	●	●	●	✓	✓	■ Apple
Patching für eine Vielzahl von Drittanbieter-Anwendungen	●	●	●	✓	✓	■ Apple
Reportings über die Patch-Compliance anhand verschiedener Frameworks zur IT-Sicherheit und Datenschutzregulierungen	●	●	●	✓	✓	■ Apple
<b>Bewertung von Sicherheitsschwachstellen &amp; Remediation</b>						
Suchen und finden Sie Sicherheitslücken und Fehlkonfigurationen und identifizieren Sie potenzielle Gefahren, bevor sie Schaden anrichten können	●	●	●	●	✓	■ Apple
Ihnen steht ein umfangreiches Verzeichnis aus vorgefertigten Workflows für die Remediation zur Verfügung, um Ihre Geräte auf Knopfdruck abzusichern	●	●	●	●	✓	■ Apple
<b>Automatisierte Workflows</b>						
Erstellen und deployen Sie maßgeschneiderte Workflows mit dem visuellen und intuitiven Workflow-Baukasten für Automatisierungen, ohne Code schreiben zu müssen	●	●	●	●	✓	■ Apple
Erstellen Sie mehrstufige Maßnahmen, um die Kontrolle zurückzugewinnen und das Risiko am Endpunkt zu eliminieren	●	●	●	●	✓	■ Apple
Automatisieren Sie Richtlinien, um Verhaltens- und Statusveränderungen an Endpunkten in Echtzeit zu ermitteln und führen Sie selbstheilende Workflows für Endpunkthärtung und höhere Compliance aus	●	●	●	●	✓	■ Apple

✓ ENHALTEN

● NICHT ENHALTEN

⊕ ADD-ON-FEATURE

📄 NUR REPORTING



Absolute-Plattform-Komponenten	Absolute Visibility	Absolute Control	Absolute Resilience	Absolute Resilience for Security	Absolute Resilience for Automation	Verfügbarkeit des Features
Absolute Persistence <sup>13</sup>	✓	✓	✓	✓	✓	■
Engine für Regeln & Richtlinien	✓	✓	✓	✓	✓	■ Apple
Warnungen – Vordefiniert und benutzerdefiniert	✓	✓	✓	✓	✓	■ Apple
Dashboards	✓	✓	✓	✓	✓	■ Apple
API-Bibliothek <sup>11</sup>	✓	✓	✓	✓	✓	■ Apple
Cloudbasierte Steuerungskonsole	✓	✓	✓	✓	✓	■ Apple
Rollenbasierte Zugriffskontrolle	✓	✓	✓	✓	✓	■ Apple
Single Sign-On	✓	✓	✓	✓	✓	■ Apple
Zwei-Faktor-Authentifizierung	✓	✓	✓	✓	✓	■ Apple
Absolute Connector für ServiceNow®	✓	✓	✓	✓	✓	■ Apple
Automatisierte Maßnahmen	●	✓	✓	✓	✓	■ Apple
Absolute Connector für Forescout eyeSight	●	✓	✓	✓	✓	■ Apple
Universeller SIEM Connector	●	✓	✓	✓	✓	■ Apple
Accelerated Device Actions <sup>12</sup>	●	●	✓	✓	✓	■ Apple

1 Kontaktieren Sie den [Absolute Sales](#) und fragen Sie nach der Definition neuer, benutzerdefinierter Geräte-Datenpunkte über die DataExplorer Library. DataExplorer wird nicht von Windows 11 SE unterstützt.

2 Mac-Geräte unter Apple M1 benötigen den Absolute Agent in der Version 7.15 oder höher, um Statusdetails zu aktualisierter Verschlüsselung zu erfassen.

3 Nur für den Chrome-Browser auf Windows- und Chromebook-Geräten verfügbar.

4 Firmware Freeze ist nur für zulässige [Windows-Geräte verfügbar](#).

5 Nur für zulässige [Lenovo-Geräte verfügbar](#).

6 Alle Skripte in der Absolute-Reach-Bibliothek werden von Windows unterstützt (mit Ausnahme von Windows 11 SE) und einige von MacOS. Absolute Application Health is available with eligible Absolute Resilience licenses. These do not include Absolute Resilience for Education, Absolute Resilience for Student Devices and Absolute Resilience for Chromebook.

7 Self-healing of critical applications is available through Absolute Resilience. It is not supported on Windows 11 SE. Contact [Absolute Sales](#) for more information.

8 Die Selbstheilung geschäftskritischer Anwendungen ist via Absolute Resilience verfügbar. Windows 11 SE unterstützt dies nicht. Kontaktieren Sie den Absolute-Vertrieb für weitere Informationen.

9 Absolute fügt seinem Katalog unterstützter Anwendungen durch Application Resilience ständig weitere Anwendungen hinzu. Falls Sie eine bestimmte Anwendung gern resilienter gegen externe Faktoren machen würden, können Sie dies beim Absolute-Vertrieb anfordern.

10 Nur für Education-Kunden aus Nordamerika, Großbritannien und Australien. Es gelten die Allgemeinen Geschäftsbedingungen. Mehr Details finden Sie in den FAQs.

11 API-Support für ein bestimmtes Produkt-Feature oder eine bestimmte Funktion hängt von der Verfügbarkeit des Features für das jeweilige Basis- oder Add-On-Produkt ab. Geräte ohne Lizenz für das jeweilige Feature haben keinen Zugriff auf APIs für dieses.

12 Accelerated Device Actions ist via Absolute Resilience verfügbar. Unterstützte Maßnahmen umfassen das besonders schnelle Einfrieren von Geräten, die Zurücksetzung von Geräten, das Löschen von Dateien, die Benachrichtigung von Nutzern, Absolute-Reach-Skripte und die Ermittlung von Endpunktdaten. Diese Maßnahmen sind auch mit Absolute Visibility und Absolute Control verfügbar, jedoch nicht auf beschleunigte Art und Weise.

13 Folgende Funktionen werden im Absolute-Umfeld nach FedRAMP nicht unterstützt. Grund dafür sind die festgelegten Richtlinien, die einschränken, welche Daten die Systemgrenze überqueren dürfen:

- › Selbstheilung durch BIOS Persistence für Endgeräte mit älterer Firmware Persistence 1.x – Diese Geräte können registriert, getrackt und verwaltet werden, BIOS Persistence wird jedoch nicht unterstützt. Die meisten ab 2019 gebauten Endgeräte verfügen über Firmware Persistence 2.x. Sollten Sie Zweifel haben, sprechen Sie den Absolute-Vertrieb an.
- › Nachforschungen und Diebstahl-Reporting.
- › Registrierung und Verwaltung von Chromebook-Geräten.
- › Das Lenovo Remote Supervisor Password und die Funktion Lenovo Firmware Lock.
- › Die Deregistrierung von Geräten innerhalb von FedRAMP kann nur über die Absolute Console durchgeführt werden und nicht über externe IT-Sanierungsunternehmen.
- › Aktivierung von Absolute in der Fabrik via Dell Custom Factory Integration Order Ready.
- › Maßgeschneiderte Integrationen oder Berichte, die von Absolute Professional Services (PS) erstellt wurden. Andere solcher Dienste wie Absolute Assist sind jedoch verfügbar.
- › Der Absolute IdP-Service – Die Plattform unterstützt SAML 2.0 für die Authentifizierung. Es obliegt jedoch dem Kunden, einen IdP-Service einzubinden, der AAL2- oder AAL3-Standards erfüllt.

14 Diese Funktionen sind im Compliance-Modul der Absolute Secure Access Enterprise Edition enthalten. Dieses Modul bietet die Überwachung des Anwendungszustands und Selbstheilung nur für Secure Access.



# ABSOLUTE®

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-SecureEndpoint-Product-Features-MX-012325