

FACTSHEET



Absolute Secure Endpoint & Access

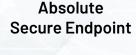
Behalten Sie immer die Kontrolle über Ihre Endpunkte – auch wenn diese sich nicht in Ihrem geschützten Unternehmensnetzwerk befinden.

Mit der Verlagerung von Arbeitsplätzen ins Homeoffice werden Sicherheitsrichtlinien zunehmend vernachlässigt und Kontrollen deaktiviert. Dadurch werden Endpunkte für Sicherheitsadministratoren oft unsichtbar und Daten gehen unbemerkt verloren. Im Laufe der Zeit sammeln sich an den Endpunkten Sicherheitslücken an, die sie anfällig für Kompromittierungen machen. Das unvermeidliche Ergebnis: Complianceverstöße, Datenverletzungen, unangemessene Ressourcenaufwände für die Endgeräteverwaltung und unsichere Audits.

Mit Absolute können Sie tief in Ihre Geräte eindringen, um sensible Daten, die gefährdet sind, zu entdecken und fehlende Geräte oder verdächtiges Verhalten zu identifizieren. In jeder Phase eines Vorfalls – Vorzeichen, Schwachstelle, Verstoß oder Wiederherstellung – bietet Absolute Ihnen eine Reihe persistenter Werkzeuge, um zuverlässig zu reagieren und sich zu erholen.

Sie erhalten **sofortige Benachrichtigungen über Schwachstellen**, Auffälligkeiten oder neue Aktivitäten auf fehlenden Geräten. Sie können diese sperren und die enthaltenen Daten löschen, um potenzielle Risiken zu minimieren. Sie können gegenüber Regulierungsbehörden beweisen, dass die Daten während eines Vorfalls stets geschützt waren, indem Sie transparente Protokolle verwenden.





/ABSOLUTE®



Visibility









(G)= "





Factsheet: Absolute Secure Endpoint & Access

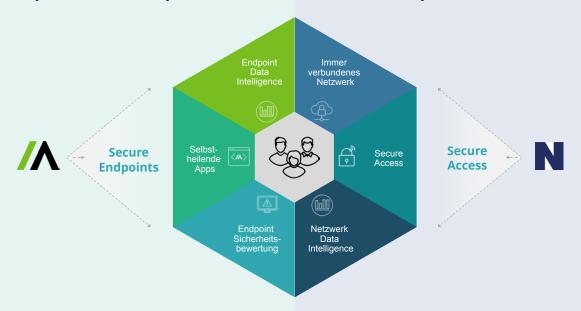
Absolute bietet folgende Lösungen, um den Schutz und die Integrität von Endpunkten vollständig zu gewährleisten:

Absolute Secure Endpoint

Absolute Secure Endpoint ist die einzige Technologie, die auch dann unverändert bleibt, wenn das Gerät neu installiert, der Speicher ausgetauscht oder die Firmware aktualisiert wird. Die Selbstheilungsverbindung stellt sicher, dass kritische Anwendungen wie SCCM, VPN, Antivirensoftware und Verschlüsselung stets in einem optimalen Zustand und auf dem neuesten Stand sind. Darüber hinaus bleiben sensible Daten geschützt, auch beim Zugriff von außerhalb des eigenen Netzwerks.

Absolute Secure Access

Absolute Secure Access gewährleistet auf sämtlichen Endgeräten eine unterbrechungsfreie Anwendungsverbindung und ermöglicht es jedem Endbenutzer, nahtlos von einem Repeater zu einem drahtlosen Zugang in einem sicheren Netzwerk zu wechseln. Wenn Ihre Belegschaft viel unterwegs ist oder in einem Bereich arbeitet, in dem die Konnektivität unbeständig ist, erübrigt sich mit Secure Access das Problem, sich erneut bei geschäftskritischen Anwendungen anmelden zu müssen.



In das BIOS von über 800 Millionen Endgeräten weltweit vorinstalliert

Zur Grundlage von Absolute Endpoint Security gehört die patentierte Persistence-Technologie von Absolute, die eine unzerbrechliche Verbindung zwischen dem Endpoint und der Absolute-Plattform herstellt. Diese Verbindung ist in der Hardware selbst verankert, da Absolute Software in das BIOS oder UEFI von über 800 Millionen Geräten weltweit vorinstalliert ist. Dies gewährleistet eine hohe Sichtbarkeit und Kontrolle über die Endgeräte, unabhängig davon, ob diese sich innerhalb oder außerhalb des Unternehmensnetzwerks befinden.

Alle großen PC-Hersteller – darunter Dell, HP, Microsoft und Lenovo – integrieren die Absolute Persistence®-Technologie in die Firmware, bevor die Geräte das Werk verlassen. Absolute Persistence stellt automatisch den Absolute Agent bei jedem Startvorgang wieder her, selbst wenn das Gerät neu aufgesetzt, die Festplatte ersetzt oder die Firmware aktualisiert wird.



→ ABSOLUTE SECURE ENDPOINT

	ABSOLUTE VISIBILITY	ABSOLUTE CONTROL	ABSOLUTE RESILIENCE
	Good	Better	Best
HARDWARE VERFOLGEN			
Berichten und Benachrichtigen über Hunderte von Hardware-Attributen	•	•	•
Überwachen von Geräteleasing-Berichten	•	•	•
Verfolgen von neuen Geräteaktivierungen und Verbindungshistorie	•	•	•
Nutzung vorgefertigter und benutzerdefinierter Berichte	•	•	•
Markieren fehlender Geräte & Benachrichtigung, wenn sie eine Verbindung zum Internet herstellen	•	•	•
SOFTWARE ÜBERWACHEN			
Bewertung installierter Software nach Gerät oder Population	•	•	•
Berichten und Benachrichtigen über Änderungen der Softwarekonfiguration oder Richtlinien-Nichtkonformität	•	•	•
$Nutzung\ vorgefertigter\ oder\ Erstellung\ benutzerde finierter\ Kataloge\ zur\ Identifizierung\ von\ Software\ \&\ Suiten$	•	•	•
SICHERHEITSHALTUNG BEWERTEN			
Berichterstattung über den Verschlüsselungsstatus	•	•	•
Berichterstattung über den Anti-Malware-Status	•	•	•
GERÄTEVERWENDUNG VERSTEHEN			
Bewertung der Gerätenutzung durch Analyse von Anmelde-/Entsperr- und Geräteinteraktionsereignissen	•	•	•
Berichterstattung über die durchschnittliche tägliche Nutzung pro Gerät	•	•	•
Berichterstattung über besuchte Websites und aktive Zeit auf jeder einzelnen			•
GERÄTESTANDORT ÜBERWACHEN			
Verfolgen des Gerätestandorts mit 365 Tagen Historie	•	•	•
Definieren von Geofences zur Erkennung unbefugter Gerätestandortbewegungen		•	•
GERÄTE AUS DER FERNE EINFRIEREN			
Ein Gerät mit benutzerdefinierter Nachricht einfrieren – geplant oder auf Abruf		•	•
Einen Offline-Timer einstellen, um Geräte automatisch einzufrieren		•	•
DATEN VON GERÄTEN LÖSCHEN			
Selektives Löschen von Dateien		•	•
Durchführen eines End-of-Life-Geräte-Löschvorgangs mit Konformitätszertifikat		•	•
FIRMWARE-SCHUTZ AKTIVIEREN			
Supervisor-Passwort in großem Maßstab verwalten		•	•
GERÄTE SOFORT ABFRAGEN UND BEHEBEN			
Über 130 vorgefertigte Workflows aus der Reach-Bibliothek ausführen			•
Benutzerdefinierte Powershell- oder BASH-Skripte auf Geräten ausführen			•
SENSITIVE DATEIEN AUF GERÄTEN IDENTIFIZIEREN			
Entdecken von PII, PHI, PFI, SSN, GDPR-Daten und geistigem Eigentum im oder außerhalb des Netzwerks			•
Durchführen einer Datenrisikobewertung mit geschätzter Kostenauswirkung			•
ldentifizieren von Geräten mit sensiblen Dateien, die mit Cloud-Speicher (Dropbox, iCloud, Box, OneDrive) synchronisieren			•





ABSOLUTE SECURE ENDPOINT

Absolute Secure Endpoint: Maximale Sicherheit für Ihre Endgeräte



Absolute Visibility

Eine Lösung, die umfassende Einblicke in die Endpunktumgebung bietet, einschließlich Hardware- und Softwareinventar, Gerätenutzung und Sicherheitsstatus.

- ✓ Hardware- und Software-Audits zur Bestandsverwaltung
- Identifikation von verlorenen oder fehlenden Hardwarekomponenten
- Analyse der Nutzung von Webanwendungen zur Optimierung des ROI
- Identifikation sensibler Daten auf Geräten, inklusive Off-Netzwerk- Dateien
- Überwachung des Sicherheitsstatus von Geräten, einschließlich Verschlüsselung und Malware-Schutz



Absolute Control

Die Lösung zur Fernverwaltung von Endgeräten, das Administratoren ermöglicht, Geräte aus der Ferne zu sperren, Daten zu löschen oder Sicherheitsrichtlinien durchzusetzen. Es kann auch erkennen, wo das Gerät zuletzt geographisch erkannt wurde, wenn es eingeschaltet ist und eine Verbindung zum Internet herstellen kann.

Sämtliche Funktionen von Visibility, plus:

- Geofencing zur Kontrolle der Gerätebewegung
- Ferngesteuerte
 Gerätesperre mit
 benutzerdefinierter
 Nachricht
- Selektive Dateilöschung auf Geräten
- Durchführung von Datenlöschungen am Ende des Lebenszyklus eines Geräts



Absolute Resilience

Eine Funktion, die die Ausfallsicherheit von Endpunkten verbessert, indem sie sicherstellt, dass bestimmte Anwendungen immer installiert und funktionsfähig sind.

Sämtliche Funktionen von Control, plus:

- Automatische Reparatur oder Neuinstallation von mission-kritischen Anwendungen
- Bibliothek von Skripten zur schnellen Behebung von Problemen
- Unterstützung bei der Wiederbeschaffung gestohlener Geräte mithilfe des Absolute Investigations Team und Behörden

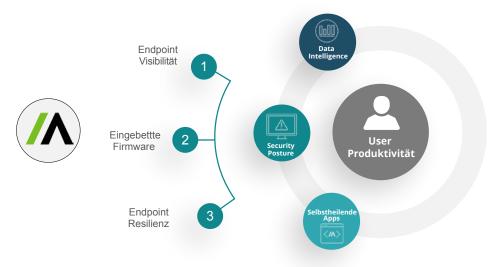


ABSOLUTE SECURE ENDPOINT

Endpunkt-Sichtbarkeit: Innerhalb und außerhalb des Netzwerks

Absolute Secure Endpoint bietet umfassende Einblicke in alle Endgeräte, unabhängig davon, ob sie sich innerhalb oder außerhalb des Firmennetzwerks befinden. Diese Rundumsicht ermöglicht es, Bedrohungen frühzeitig zu erkennen und effektiv zu neutralisieren.

Sie können Ihre Hardware- und Software-Inventare stets aktuell halten, das Gerätelebenszyklusmanagement optimieren, Ihre Audits und täglichen Abläufe beschleunigen und Benachrichtigungen erhalten, wenn sich Geräte in Bewegung setzen.



Platform Coverage







Data Intelligence

Bestandsverwaltung / Sicherheitslage Nutzung / Geolokalisierung / Zustand

Control

Sichere Endpunkte, um Daten und die Sicherheitslage zu konfigurieren

Resilience

Endpunkte wiederherstellen Selbstheilende Anwendungen

Key Facts:

Eingebettet und selbstheilend: Absolute ist die einzige Plattform, die durch eine selbstheilende Technologie betrieben wird und in die Firmware Ihres Geräts eingebettet ist. Sie ermöglicht Ihnen, Ihre gesamte Flotte von einem Dashboard aus zu sehen und zu kontrollieren, unabhängig von Plattform oder Netzwerk.

Hardware-Analysen: Behalten Sie jeden Endpunkt im Auge und erstellen Sie ein vollständiges, stets aktuelles Inventar aller Ihrer Endpunkte – mit Hunderten von Datenpunkten pro Gerät.

Geolokalisierung: Verfolgen Sie den physischen Standort jedes interessierenden Geräts jederzeit genau, sowohl innerhalb als auch außerhalb Ihres Netzwerks, einschließlich historischer Protokolle.

Remote-Lifecycle-Management: Optimieren Sie die Bereitstellung, Umverteilung und Stilllegung von Geräten aus der Ferne, einschließlich der Möglichkeit, regelmäßige Wartungen zu automatisieren, Geräteprobleme zu beheben und eine zertifizierte Löschung am Ende des Lebenszyklus durchzuführen.

Softwareberichte und -benachrichtigungen: Halten Sie Ihr Softwareinventar aktuell, eliminieren Sie Anomalien und ungeschützte Komponenten und erkennen Sie, wenn benötigte Anwendungen fehlen.

Gerätenutzung: Erkennnen Sie, wie Geräte genutzt werden, und identifizieren Sie inaktive Assets, um zu entscheiden, welche umverteilt werden sollen und welche ausgemustert werden müssen.



ABSOLUTE SECURE ENDPOINT

Sicherheitsvorfälle erkennen, darauf reagieren und erfolgreich wiederherstellen

Ihre Erfolgskriterien:

Endpunkt-Datenerkennung: Lokalisieren Sie sensible Daten – wie IP, PII, PHI oder PFI –, die gefährdet sind oder gegen Datenschutzvorschriften wie HIPAA, GDPR, CJIS oder CCPA verstoßen könnten.

Früherkennung von Vorfällen: Erhalten Sie Benachrichtigungen über deaktivierte Kontrollen und Hinweise auf Manipulationen an Geräten und wissen Sie, wann datenbeladene Geräte an den falschen Ort gelangen.

Berichte über fehlende Geräte: Erkennen Sie, welche Geräte seit einer bestimmten Zeit offline sind, und kennzeichnen Sie diese als fehlend, um benachrichtigt zu werden, sobald sie sich mit dem Internet verbinden.

Notfall-Datenschutz: Sperren oder löschen Sie kompromittierte Geräte aus der Ferne, erhalten Sie ein Zertifikat für die Datenbereinigung, verhindern Sie Datenübertragungen und führen Sie viele weitere Abhilfemaßnahmen im großen Maßstab durch.

Ermittlungsexperten: Nutzen Sie das Absolute-Team erfahrener Ermittler, die eng mit Strafverfolgungsbehörden zusammenarbeiten, um gestohlene Geräte zurückzubekommen oder den Benutzer mittels forensischer Werkzeuge zu identifizieren.

Nachweis der Compliance: Nutzen Sie historische Protokolle, um zu validieren, dass der Datenschutz während Vorfällen gewährleistet war, und erfahren Sie die Ursachen, um Ihre Sicherheitsrichtlinien weiterzuentwickeln.

Platform Coverage









Data Intelligence

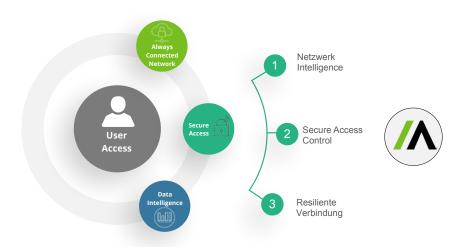
Netzwerkkonnektivität & Nutzung Benutzererfahrung / Geolokalisierung

Control

Zero Trust Zugriff Eingeschränkter Anwendungszugriff Sicheres Web-Gateway

Resilience

Netzwerkverbindung Kontinuität





Absolute Secure Access: Die perfekte Synergie von Endpunktschutz und Netzwerksicherheit

Secure Access von Absolute ist eine wichtige Ergänzung zu Secure Endpoint und bietet zusätzliche Sicherheit durch die Gewährleistung eines geschützten Zugriffs auf Netzwerke und Daten. Die technischen Vorteile von Secure Access umfassen:

Kontrollierte Zugriffsmöglichkeiten:

Absolute ermöglicht die Implementierung granularer Zugriffskontrollen, um sicherzustellen, dass nur autorisierte Benutzer auf sensible Daten und Netzwerkressourcen zugreifen können.

Netzwerkintegrität:

Durch kontinuierliches Monitoring und die automatische Wiederherstellung von Netzwerkverbindungen stellt Absolute sicher, dass die Netzwerkintegrität gewahrt bleibt und potenzielle Sicherheitsrisiken schnell identifiziert und behoben werden.

Verschlüsselung:

Absolute bietet eine robuste Verschlüsselungstechnologie, um Daten während der Übertragung und im Ruhezustand zu schützen, was die Sicherheit sensibler Informationen weiter erhöht.

Benutzer- und Geräteauthentifizierung:

Durch die Implementierung von mehrstufigen Authentifizierungsmethoden sorgt Absolute dafür, dass nur autorisierte Benutzer mit verifizierten Geräten auf das Netzwerk zugreifen können, wodurch das Risiko von unbefugtem Zugriff minimiert wird.

Ein Tag im Leben eines Außendienstmitarbeiter im Bau **Außendienstmitarbeiters** Cellular & Wi-Fi Dispatch Management Kunden Portal Work Order Management Fahrt zur Arbeit Nahtlose Verbindung in 5G Stop im Starbucks Baustelle Alle Apps bleiben verbunden Verlässlicher Auch in unsicheren WLAN- Startet automatisch Secure Access Automatisches Steigern des Netzwerken sicher Ermöglichen Sie den Zugriff auf Sicherheit ab Computer Start Arbeitplatz auch im Homeoffice Netzwerkdurchsatzes Upload/Downdload von Anhalten nicht kritischer Apps, um die Geschwindigkeit für persönliche Apps in den Pausen Sichere Datenübertragung im Geschäftsanwendungen zu erhöhen Hintergrund Bsp. Skype auch unter schlechtester Netzwerkbedingungen 0000 Aufzug im Büro Homeoffice Nächste Baustelle Büro Besuch Stabilisieren von Apps und Intelligente Verbindung zum schnellsten Netzwerk Aufrechterhaltung der Sicherheit in privaten Netzwerken Lösen Sie Kundenprobleme beim ersten Besuch Stabilisieren von Apps in zeitweiligen Betriebssystemaktivitäten bei Aktualisieren Sie das Betriebssystem • Netzwerken • Aufrechterhaltung von Produktivität Verbindungsabbrüchen / die App / die Sicherheit, wenn Sie mit schnellen Netzwerken Nichts stürzt ab keine verlorenen Daten Sorgen Sie für gute Kundeninteraktion verbunden sind /ABSOLUTE Verbindung, wenn ein Netzwerk verfügbar ist

Die All-in-One-Lösung für umfassende Endpunktsicherheit und Compliance

Absolute bietet eine umfassende Lösung, um Endpunktsicherheit zu stärken, Compliance zu beschleunigen und sensible Daten zu schützen. Von Sicherheitsprofis über IT-Asset-Manager bis hin zu Compliance-Beauftragten,

HR-Leitern und Geschäftsleitern ermöglicht Absolute ein vollständiges Situationsbewusstsein und hilft, höchste Compliance-Standards einzuhalten, um Risiken zu reduzieren.

Sicherheitsbeauftragte:

Nutzen Sie Absolute, um Endpunkt-Blindstellen zu schließen und Sicherheitsagenten zu stärken.

IT-Asset-Manager:

Sehen Sie alle Geräte und verbessern Sie die Endpunkthygiene effizient.

Compliance-Beauftragte:

Beschleunigen Sie Compliance und belegen Sie stets den Schutz sensibler Daten.

HR-Leiter:

Erkennen und stoppen Sie Insider-Bedrohungen mit umfassenden Benutzerverhaltensanalysen.

Geschäftsleiter:

Haben Sie vollständiges Situationsbewusstsein und halten Sie höchste Compliance-Standards ein, um Risiken zu reduzieren.

Volle Übersicht über eine Konsole

Über eine einzige, cloudbasierte Konsole können Sie Berichte über die Einhaltung von Standards oder Vorschriften erstellen und diese Informationen mit allen Beteiligten in Ihrer Organisation teilen.

Erkennen Sie Konfigurationsabweichungen und Schwachstellen, setzen Sie Sicherheitsanwendungen automatisch durch und führen Sie Befehle und Workflows aus der Ferne aus, um Sicherheitslücken zu schließen und notwendige Aufgaben zu automatisieren.

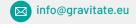


GRAVITATE

Über Gravitate GmbH

Gravitate ist führender Absolute-Partner für Deutschland mit Sitz in Nürnberg und spezialisiert auf die Unterstützung von Unternehmen und Organisationen im Bereich Endpoint Security Solutions und Endpoint Protection Platforms (EPP), Attack Path Management (APM) und Continuous Threat Exposure Management (CTEM). Gravitate arbeitet dabei eng mit der Absolute Software Corporation und ICOS Deutschland als Distributor zusammen und verfügt über umfassende Erfahrung im Bereich präventiver Sicherheitsmaßnahmen, insbesondere für KRITIS-Branchen.









Gravitate GmbH Fürther Straße 27 D-90429 Nürnberg

Tel. +49 155 666 40 734 info@gravitate.eu

www.gravitate.eu