DELL Technologies

Dell SafeData

Die Absolute-Plattform

SICHTBARKEIT UND SCHUTZ FÜR IHRE GERÄTE

Einzige firmwarebasierte Lösung für Endpunktintelligenz und -ausfallsicherheit

Sie haben alle richtigen Strategien implementiert, aber die herkömmlichen Tools für das Management und die Sicherheit von Endgeräten weisen Einschränkungen und „blinde Flecken“ auf, werden von den EndnutzerInnen deaktiviert oder konkurrieren um Geräteressourcen – am Ende funktionieren sie einfach nicht wie vorgesehen.

Infolgedessen wird es schwierig, Ihre Endpunkte sichtbar zu halten, zu kontrollieren und zu schützen. Das führt zu Ungenauigkeiten, betrieblichen Ineffizienzen und Sicherheitslücken, die wiederum Ihre Fähigkeit beeinträchtigen, Probleme zuverlässig zu erkennen und souverän auf Bedrohungen zu reagieren. Das unausweichliche Ergebnis: unsichere Audits, Ressourcenverschwendung, Datenschutzverletzungen und Complianceverstöße.

Dell integriert die patentierte Persistence®-Technologie von Absolute in die Firmware, bevor die Geräte das Werk verlassen. Mit Persistence® wird der Absolute-Agent bei jeder Startreihenfolge automatisch korrigiert und neu installiert, selbst wenn das Gerät ein neues Image erhalten hat oder die Festplatte getauscht wurde.

Sobald Absolute aktiviert ist, bietet das Tool durch eine unzerstörbare digitale Verbindung die benötigte Ausfallsicherheit, sodass Ihre Geräte in jeder Situation stets sichtbar und kontrollierbar bleiben.

Weitere Informationen finden Sie unter DellEMC.com/endpointsecurity

ABSOLUTE®

BESTANDSINTELLIGENZ

Persistente Endpunktsichtbarkeit: im und außerhalb des Netzwerks

Absolute stellt sicher, dass Ihre digitale Verbindung zu jedem Gerät intakt bleibt, damit Sie zuverlässige Informationen zu allen Endpunkten erhalten – und zwar im Unternehmensnetzwerk oder außerhalb davon.

Sie können Ihren Hardware- und Softwarebestand immer auf dem neuesten Stand halten, das Lebenszyklusmanagement der Geräte optimieren, Audits und den täglichen Betrieb beschleunigen, Warnmeldungen über den Standort wechselnde Geräte erhalten, nicht ausgelastete Ressourcen erkennen, um Verschwendung zu vermeiden, und basierend auf all diesen Informationen kostengünstigere Entscheidungen treffen.

Ihre Erfolgskriterien:

Integrierte automatische Fehlerkorrektur: Dank der einzigen Plattform mit Technologie zur automatischen Fehlerkorrektur, die in die Firmware Ihres Geräts integriert ist, können Sie Ihre gesamte Flotte über ein Dashboard anzeigen und steuern, unabhängig von Plattform oder Netzwerk.

Hardwareanalyse: Behalten Sie jeden Endpunkt im Auge und erstellen Sie einen vollständigen, stets aktuellen Bestand aller Endpunkte – mit Hunderten Datenpunkten pro Gerät.

Geolokalisierung: Sie können den physischen Standorts jedes Geräts jederzeit präzise im oder außerhalb Ihres Netzwerks nachverfolgen, einschließlich Verlaufsprotokollen.

Remote-Lebenszyklusmanagement: Optimieren Sie die Remotebereitstellung, -neuzuweisung und -außerbetriebnahme von Geräten und nutzen Sie die Möglichkeit, regelmäßige Wartungstätigkeiten zu automatisieren, Geräteprobleme zu beheben und eine zertifizierte Löschung am Ende der Nutzungsdauer durchzuführen.

Softwareberichte und Warnmeldungen: Halten Sie Ihren Softwarebestand auf dem neuesten Stand, löschen Sie Schatten-IT und erkennen Sie, wenn erforderliche Anwendungen fehlen.

Geräteauslastung: Erfahren Sie, wie die Geräte verwendet werden, und ermitteln Sie inaktive Ressourcen, um zu entscheiden, welche neu zugewiesen oder stillgelegt werden sollen.

AUSFALLSICHERE ENDPUNKTSICHERHEIT

Bewerten Ihres Sicherheitsstatus und Erzwingen von Sicherheitskontrollen

Melden Sie über eine einzige, Cloud-basierte Konsole die Compliance mit Standards oder Bestimmungen und geben Sie diese Informationen an alle StakeholderInnen in Ihrem Unternehmen weiter. Erkennen Sie Konfigurationsabweichungen und Sicherheitslücken, nutzen Sie die automatische Erzwingung von Sicherheitsanwendungen und stellen Sie Befehle sowie Workflows remote bereit, um die Sicherheitslücken zu schließen und notwendige Aufgaben zu automatisieren.

Absolute ist die erste und einzige Lösung für Endpunktsichtbarkeit und -kontrolle, die auch bei anderen Sicherheitskontrollen persistiert. Indem Sie die Ausfallsicherheit von Absolute auf andere Anwendungen erweitern, können Sie die automatische Fehlerkorrektur für Ihren gesamten Sicherheitsstack nutzen und diese verstärkte Sicherheit auf Ihre gesamte Flotte ausdehnen, ohne die Geräte einzubringen. Falls Endpunkte von Ihrem gewünschten Image abweichen, werden sie von Absolute wieder „in die Reihe“ gezwungen, um verheerende Datenschutzverletzungen zu vermeiden und die Business Continuity aufrechtzuerhalten.

Ihre Erfolgskriterien:

Benchmarking für Standards: Sie können Complianceberichte für Cybersicherheitsstandards oder Datenschutzbestimmungen erstellen, Geräte mit fehlender Verschlüsselung oder Anti-Malware kennzeichnen und Compliancelücken schließen.

Gehärtete Konfiguration: Erkennen Sie Schwächen und Abweichungen von den gewünschten Endpunktkonfigurationen und passen Sie diese nach Bedarf an.

Weitere Informationen finden Sie unter DellEMC.com/endpointsecurity

ABSOLUTE®

Anwendungskontinuität: Eliminieren Sie Unterbrechungen der Nutzerproduktivität und der Business Continuity durch Anwendungen mit automatischer Fehlerkorrektur.

Gesicherte Data Protection: Stärken Sie die Data Protection, indem Sie Sicherheitskontrollen wie z. B. Verschlüsselung, Anti-Malware, VPN, Endgerätemanagement persistieren – ganz ohne menschliches Eingreifen.

Erkennen und Beheben von Sicherheitslücken: Ermitteln Sie Endpunkte, auf denen anfällige Betriebssystemversionen ausgeführt werden, und führen Sie dringende Updates per Push-Übertragung durch oder implementieren Sie schützende Workarounds im oder außerhalb des Unternehmensnetzwerks.

Automatisierte Workflows: Stellen Sie Befehle und automatisierte Workflows remote bereits, um Sicherheitslücken schnell und nach Bedarf zu schließen.

ZUVERLÄSSIGE RISIKOREAKTION

Erkennen von und Reagieren auf Sicherheits-Incidents sowie erfolgreiche Recovery

Mit Absolute können Sie umfassende Details zu Ihren Geräten anzeigen, um gefährdete sensible Daten zu erkennen und fehlende Geräte oder verdächtige Verhaltensweisen zu identifizieren. Absolute bietet in jeder Incident-Phase – Auffälligkeit, Sicherheitslücke, Sicherheitsverletzung oder Recovery – eine Suite an persistenten Tools für die zuverlässige Reaktion und Recovery.

Sie erhalten unverzüglich Warnmeldungen zu Sicherheitslücken, Gefährdungen oder neuen Aktivitäten auf fehlenden Geräten. Sie können diese sperren und die darauf befindlichen Daten löschen. Weisen Sie gegenüber den regulierenden Organen nach, dass die Daten während des Incidents stets geschützt waren. Nutzen Sie Verlaufsprotokolle, um Benachrichtigungen zu Sicherheitsverletzungen zu vermeiden, mehr über die Ursache zu erfahren und weitere ähnliche Incidents zu verhindern.

Ihre Erfolgskriterien:

Erkennung der Daten auf Endgeräten: Lokalisieren Sie sensible Daten – wie geistiges Eigentum, personenbezogene Daten, geschützte Gesundheitsdaten oder persönliche Finanzinformationen –, die gefährdet oder anfällig für Verstöße gegen Datenschutzbestimmungen wie HIPAA, DSGVO, CJIS oder CCPA sind.

Frühzeitige Incident-Erkennung: Sie erhalten Warnmeldungen zu deaktivierten Kontrollen sowie nachgewiesenen Gerätemanipulationen und wissen stets, wann sich Geräte mit vielen Daten am falschen Ort befinden.

Berichte zu fehlenden Geräten: Ermitteln Sie, welche Geräte für einen bestimmten Zeitraum offline waren, und kennzeichnen Sie diese als fehlend, damit Sie sofort benachrichtigt werden, wenn sie sich mit dem Internet verbinden.

Notfall-Data-Protection: Kompromittierte Geräte lassen sich remote sperren oder löschen. Sie erhalten dann ein Bereinigungszertifikat, verhindern die Datenübertragung und können etliche andere Korrekturmaßnahmen nach Bedarf durchführen.

Ermittlungsprofis: Nutzen Sie das Absolute-Team mit erfahrenen ErmittlerInnen, die sehr eng mit den Strafverfolgungsbehörden zusammenarbeiten, um ein gestohlenes Gerät zurückzuholen oder die/den BenutzerIn mit forensischen Tools zu identifizieren und rechtlich zu belangen.

Compliancenachweis: Nutzen Sie Verlaufsprotokolle, um zu validieren, dass die Data Protection auch während der Incidents gewährleistet war, und bringen Sie die Ursache in Erfahrung, um Ihre Sicherheits-Policies zu iterieren.

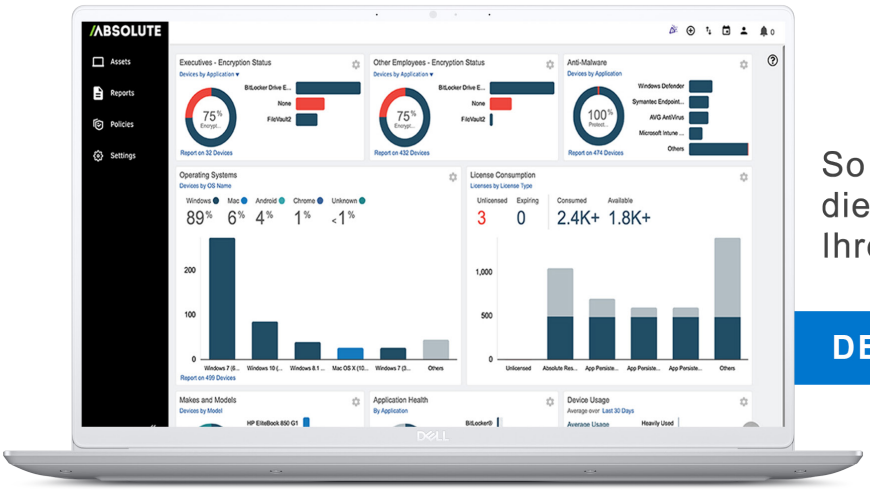
Weitere Informationen finden Sie unter DellEMC.com/endpointsecurity

ABSOLUTE®

KEINE ZWEIFEL MEHR AN DER SICHERHEIT IHRER ENDPUNKTE

Die verteilten Unternehmen von heute benötigen persistente Endpunktsichtbarkeit und -kontrolle. Um mit einer mobilen Belegschaft Schritt zu halten und die Ausfallsicherheit für das Unternehmen zu realisieren, verlassen sich die IT- und Sicherheitsteams auf die leistungsstarke Kombination aus Bestandsintelligenz, ausfallsicherer Endpunktsicherheit und zuverlässiger Risikoreaktion. Sie vertrauen auf die Absolute-Plattform.

Weitere Informationen darüber, wie Absolute Ihnen helfen kann, finden Sie unter absolute.com/platform.



So transformiert Absolute die IT und Sicherheit in Ihrem Unternehmen

DEMO ANFRAGEN

Absolute Resilience – für unzerstörbare Anwendungen und Sicherheitstools

Absolute Resilience bietet alle Funktionen für Sichtbarkeit und Kontrolle, einschließlich eines persistenten Datenstroms, automatisierter Bestände und der Möglichkeit, Daten auf gefährdeten Geräten zu löschen oder zu sperren.

Anwendungspersistenz

Nutzen Sie die Funktion zur automatischen Fehlerkorrektur und anschließenden Neuinstallation für Ihre geschäftskritischen Anwendungen, nachdem versucht wurde, diese zu deaktivieren, zu entfernen oder neu zu konfigurieren.

Erkennung der Daten auf Endgeräten

Legen Sie Policies fest, um Ihre Windows- und Mac-Geräte oder gefährdeten sensiblen Daten – darunter person enbezogene Daten, geschützte Gesundheitsdaten, persönliche Finanzinformationen, Sozial-versicherungsnummern, geistiges Eigentum und der DSGVO unterliegende Daten – in oder außerhalb Ihres Netzwerks zu scannen und dann die Kosten der Gefährdung einzuschätzen.

Absolute-Reichweite

Sie können all Ihre Windows- und Mac-Geräte anhand einer Bibliothek aus vorgefertigten und benutzerdefinierten Skripten bewerten und Korrekturmaßnahmen durchführen.

Ermittlungen

Lassen Sie das Absolute-Team aus ehemaligen Strafverfolgungsprofis Ihre verloren gegangenen oder gestohlenen Geräte aufspüren und arbeiten Sie dann mit den lokalen Behörden zusammen, um sie zurückzuholen.

Weitere Informationen finden Sie unter DellEMC.com/endpointsecurity

ABSOLUTE®

	Absolute Visibility	Absolute Control	Absolute Resilience
Absolute-Konsole	●	●	●
Nachverfolgung von Hardware	●	●	●
Messung der Gerätenutzung	●	●	●
Monitoring der installierten Software	●	●	●
Bewertung des Sicherheitsstatus	●	●	●
Monitoring der Integrität kritischer Anwendungen	●	●	●
Drittanbieterintegrationen	●	●	●
Erkennung von unautorisierten Gerätebewegungen		●	●
Remotesperrung von Geräten		●	●
Remotelöschung von Daten		●	●
Aktivierung des Firmwareschutzes		●	●
Automatische Fehlerkorrektur für kritische Anwendungen			●
Erkennung von vertraulichen Informationen auf Geräten			●
Remoteabfrage und -korrektur von Geräten nach Bedarf			●
Untersuchung und Wiederherstellung gestohlener Geräte			●

Unterstützte Plattformen:

Wenden Sie sich noch heute unter endpointsecurity@dell.com an Ihren Dell Endpoint Security Specialist, um zu erfahren, wie Sie mit Dell SafeData-Produkten Ihren Sicherheitsstatus verbessern können.

Weitere Informationen finden Sie unter DellEMC.com/endpointsecurity

ABSOLUTE®

DELL Technologies