Acronis

WHITEPAPER

Verteilte vs. zentrale Verwaltung von Cyber Protection für Unternehmen mit mehreren Standorten

Wie eine verteilte Verwaltung von Cyber Security und Data Protection die Cyber-Resilienz Ihres Unternehmens stärken kann

Unternehmen jeder Größe haben Schwierigkeiten, die Verfügbarkeit ihrer Systeme und die Integrität ihrer Daten gegen eine Vielzahl von Bedrohungen zu schützen, wie z. B. KI-gestützte Cyberangriffe, Hardware-Fehler, Softwareprobleme und menschliches Versagen. Viele Unternehmen entscheiden sich dafür, ihre IT und Cyber Security zu zentralisieren. Es gibt jedoch auch andere Anwendungsfälle, in denen eine teilweise Übertragung der Kontrolle an IT- und Cybersicherheitspersonal an entfernten Standorten zu einer besseren Cyber-Resilienz führen kann.

Dieses Whitepaper untersucht Szenarien, in denen ein Unternehmen durch die Delegierung von Aufgaben an regionale und entfernte Standorte eine höhere Verfügbarkeit, einen effektiveren Schutz vor Datenverlusten und geringere Kosten für die Verwaltung und Sicherung der IT-Infrastruktur und Geschäftsdaten erreichen kann. Es wägt die Vor- und Nachteile dieses Ansatzes ab und zeigt auf, wie Unternehmen ihre Compliance- und Governance-Ziele auch ohne ein vollständig zentralisiertes Management der Cyber Security und des IT-Betriebs erreichen können.

Viele Unternehmen haben mehrere Standorte

Etwa ein Viertel der US-Unternehmen hat mehrere Standorte. Auch wenn in der Europäischen Union (EU) keine spezifischen Daten über Unternehmen nach der Anzahl ihrer Standorte erhoben werden, deutet die Verbreitung von Einzelhandel, Hotel- und Gaststättengewerbe, Gesundheitswesen, Finanzdienstleistungen und anderen Wirtschaftszweigen, die in der Regel über mehrere Standorte verfügen, darauf hin, dass Unternehmen mit mehreren Standorten auch in der EU-Wirtschaft einen bedeutenden Anteil ausmachen. Größere Unternehmen haben noch häufiger mehrere Standorte, einschließlich regionaler Büros, Produktionsstätten, Lager und Vertriebszentren.

Unternehmen, die in ihrer Branche, in anderen Geschäftsbereichen und in anderen geografischen Regionen durch Fusionen und Übernahmen expandieren, dürften ebenfalls eine große Zahl von Standorten haben, die räumlich weit von den zentralen IT- und Cybersicherheitsabteilungen entfernt sind.

Beispiele für dezentralisierte Unternehmen

Der Einzelhandel ist ein gutes Beispiel für stark dezentralisierte Unternehmen. Ein typischer Einzelhändler verfügt über eine globale und regionale Firmenzentrale, Vertriebslager und Geschäfte mit Kundenkontakt. Aber auch viele Nicht-Einzelhandelsunternehmen sind räumlich wie Einzelhandelsunternehmen organisiert, d. h. sie verfügen über eine große Anzahl geografisch verteilter Geschäfte oder Büros, wie die folgenden Beispiele zeigen:

- Anbieter von Gesundheitsdienstleistungen wie Optiker, Hausärzte, Zahnärzte, Notaufnahmen, Apotheken und Tierkliniken.
- Verbraucherorientierte Banken, Versicherungs- und Finanzdienstleistungsunternehmen mit vielen Zweigstellen.
- Paketdienste, Transport- und Logistikunternehmen mit zahlreichen Auslieferungslagern und eine Vielzahl von Einzelhandelsgeschäften für Versand- und Unternehmensdienstleistungen.

- Glücksspielunternehmen mit mehreren Standorten für Casinos, Bingohallen, Wettbüros, Pachinko-Salons und ähnliche Einrichtungen.
- Rast- und Tankstellen, die häufig das Tanken oder Aufladen von Fahrzeugen mit Einzelhandelsgeschäften und Schnellrestaurants kombinieren.
- Unternehmen, die in einer föderierten Architektur organisiert sind, in der ein zentrales Team möglicherweise den unternehmensweiten IT-Betrieb, die Cyber Security und die Compliance überwacht, die einzelnen Standorte jedoch über eigene Budgets verfügen, für die Einstellung von Personal verantwortlich sind und lokale Autonomie bei der Verwaltung der IT-Infrastruktur der Geschäftseinheit haben.

Die zentrale Verwaltung von IT und Cyber Security kann eine Herausforderung sein

Ein typisches, stark dezentralisiertes Unternehmen verfügt über eine heterogene Mischung aus Hardware, Virtualisierung und Betriebssystemen sowie Applikationen wie Lagerverwaltungs- oder Kassensysteme von verschiedenen Technologieanbietern. Die Zusammensetzung der technischen Infrastruktur und die Versionsstände der Software können von Standort zu Standort stark variieren. Die Notwendigkeit, veraltete Applikationen, maßgeschneiderte Software und Computer zu erhalten, um eine stabile Technologieumgebung zu gewährleisten, kann die unternehmensweite IT-Standardisierung erschweren und zu einem Wildwuchs von IT- und Cybersicherheitstools führen.

Für zentralisierte Mitarbeiter:innen kann es schwierig sein, alle Tools zu beherrschen, die für den Schutz, die Verwaltung und die Sicherung von Applikationen und Daten im gesamten Unternehmen erforderlich sind. Gleichzeitig nimmt die Komplexität und Vielfalt der Applikationen und der für ihre Verwaltung und ihren Schutz erforderlichen Tools ständig zu.

An entfernten Standorten mit hohen Sicherheitsanforderungen, z. B. in Produktionsstätten, kann es erforderlich sein, eine eigene Offline-Umgebung einzurichten, d. h. sie physisch vom Unternehmensnetzwerk und dem öffentlichen Internet zu isolieren, um die Anfälligkeit für Cyberbedrohungen zu minimieren. Dies schränkt die Möglichkeiten des IT-Personals in der Zentrale zur Diagnose und Behebung von Problemen mithilfe von Remote-Desktop-Verwaltung und anderen netzwerkbasierten Tools ein und kann dazu führen, dass zur Behebung von Problemen tatsächlich der Standort aufgesucht werden muss.

Bei schwer zugänglichen Standorten wie Wüstenraffinerien, Offshore-Ölplattformen, Bergbauanlagen und anderen Standorten, die weit von kommerziellen Luft- und Bodenverkehrsknotenpunkten entfernt sind, kann dies zu inakzeptablen Kosten und einem enormen Zeitaufwand führen.

Es ist einfacher und zeitsparender, Data Protection und Cyber Security in einem großen Unternehmen mit einem einzigen Standort zu verwalten, als die gleiche Anzahl von Applikationen und Endpunkten an mehreren geografisch getrennten Standorten zu schützen. Wenn Backup-Daten nicht nach Standorten getrennt

werden, kann die Wiederherstellung von einem Backup an einem Standort die Leistung an allen Standorten beeinträchtigen.

Die WAN-Konnektivität (Wide Area Network) und die Netzwerkgeschwindigkeiten an Remote-Standorten können je nach geografischer Lage stark variieren, wodurch die Wiederherstellungszeiten sowohl unvorhersehbar als auch potenziell zu langsam sind, um die Wiederherstellungszeitstandards zu erfüllen.

Um Remote-Standorte zu verwalten, muss sich das IT-Personal möglicherweise wiederholt und separat bei lokalen Datenablagen und Sicherheitsverwaltungskonsolen anmelden, was ineffizient, fehleranfällig und langsam sein kann. Herkömmliche Backup-, Disaster Recovery- und Sicherheitssoftware ist oft auf bestimmte Programmumgebungen spezialisiert, was eine unternehmensweite Vereinheitlichung von Software erschwert.

Dieser Wildwuchs an IT-Betriebs- und Sicherheitstools ist teuer und treibt die Kosten für die Einarbeitung und Schulung des technischen Supportpersonals in die Höhe – ein wachsendes Problem in einer Welt, in der die Kosten für IT- und Cyber Security-Personal nach wie vor hoch sind.

Zentralisierte Compliance kann schwierig sein

Die Compliance-Anforderungen unterscheiden sich erheblich von Land zu Land und in einigen Fällen zwischen Bundesländern, Provinzen und Kommunen. Unternehmen, die beispielsweise in den USA tätig sind, müssen unter Umständen die Datenschutzbestimmungen der US-Regierung, mehrerer Bundesstaaten und sogar einiger Städte einhalten.

Auch die Wahrung der Datenhoheit stellt eine zunehmende Herausforderung dar. Diese Vorschriften beschränken die physischen Standorte, Datenzentren und Netzwerke, in denen sensible Daten gespeichert oder über ein Netzwerk übertragen werden dürfen. Damit soll sichergestellt werden, dass Regierungen in bestimmten Ländern nicht durch verdeckte Überwachung gegen Datenschutzbestimmungen verstoßen. Die Einhaltung dieser Anforderungen in einem Unternehmen mit weit verteilten Standorten ist eine komplexe Aufgabe und kann sich negativ auf die Leistung von Applikationen auswirken.

Den Überblick darüber zu behalten, welche Daten auf welchen Geräten geschützt werden müssen, welche Teile der IT-Infrastruktur für die Einhaltung verschiedener Sicherheits- und Regulierungsstandards zertifiziert sind und welche Teammitglieder autorisierten Zugriff auf diese Daten haben, kann zu Verwirrung und kostspieligen Compliance-Lücken im gesamten Unternehmen führen. All diese Komplexitäten kommen zu einer Zeit, in der die meisten Unternehmen mit stagnierenden oder sinkenden Budgets für IT- und Cyber Security-Personal konfrontiert sind, während die Anzahl der Applikationen und Datenmengen, die sie verwalten und schützen müssen, weiter zunimmt.

Die Aufsichtsbehörden verhängen inzwischen empfindliche Strafen, um die Einhaltung der Vorschriften zu fördern. So verhängt die EU beispielsweise routinemäßig Bußgelder in Höhe von 2 % bis 4 % des Jahresumsatzes von Unternehmen, die wiederholt gegen den Schutz von Verbraucherdaten verstoßen.

Dies kann für einige dezentralisierte und auf mehrere Standorte verteilte Unternehmen erhebliche Probleme mit sich bringen, einschließlich potenzieller Netzwerkprobleme und Schwierigkeiten bei der Suche nach konformen und sicheren Hosting-Anbietern für Applikationen und Storage mit Funktionen wie sicherer Zugangskontrolle und Unveränderlichkeit.

Acronis stellt sich der Herausforderung, verteilte Unternehmen zu verwalten und zu schützen

Acronis Cyber Protect stellt sich den Herausforderungen von Data Protection und Cyber Security in verteilten Umgebungen durch die Integration von Remote-Verwaltung, Backup, Disaster Recovery und Schutz in einer einzigen Plattform. Einzelne Remote-Standorte können von lokalen Teams über eine standortspezifische Konsole, die entweder vor Ort installiert oder in der Cloud gehostet ist, separat konfiguriert und verwaltet werden.

Data Protection- und Backup-Pläne können für jeden Standort individuell angepasst oder in standardisierter Form für mehrere Standorte implementiert werden. Die Data Protection und der Schutz aller lokalen Ressourcen können von einer einzigen Konsole aus verwaltet werden, ohne dass zwischen verschiedenen Bildschirmen oder Applikationen gewechselt werden muss.

Alle Sicherheits- und Data Protection-Funktionen werden über einen einzigen Agenten verwaltet, der auf jedem Endpunkt installiert ist. Die vollständige Verschlüsselung der Daten und die sichere Übertragung über Transport Layer Security (TLS) gewährleisten die Sicherheit der Daten bei der Übertragung. Darüber hinaus werden Datenkomprimierung, Deduplizierung und Bandbreitenbegrenzung automatisch verwaltet, um den Datenverkehr bei jeder vernünftigen Verbindungsgeschwindigkeit zu optimieren und gleichzeitig die Auswirkungen auf den laufenden Betrieb so gering wie möglich zu halten.

Gleichzeitig kann das IT- und Cyber Security-Team in der Firmenzentrale die Remote-Standorte von einem zentralen Dashboard aus überwachen, um das allgemeine Cyberrisiko, den Data Protection-Status und die Compliance im gesamten Unternehmen zu bewerten (siehe Abbildung 1).

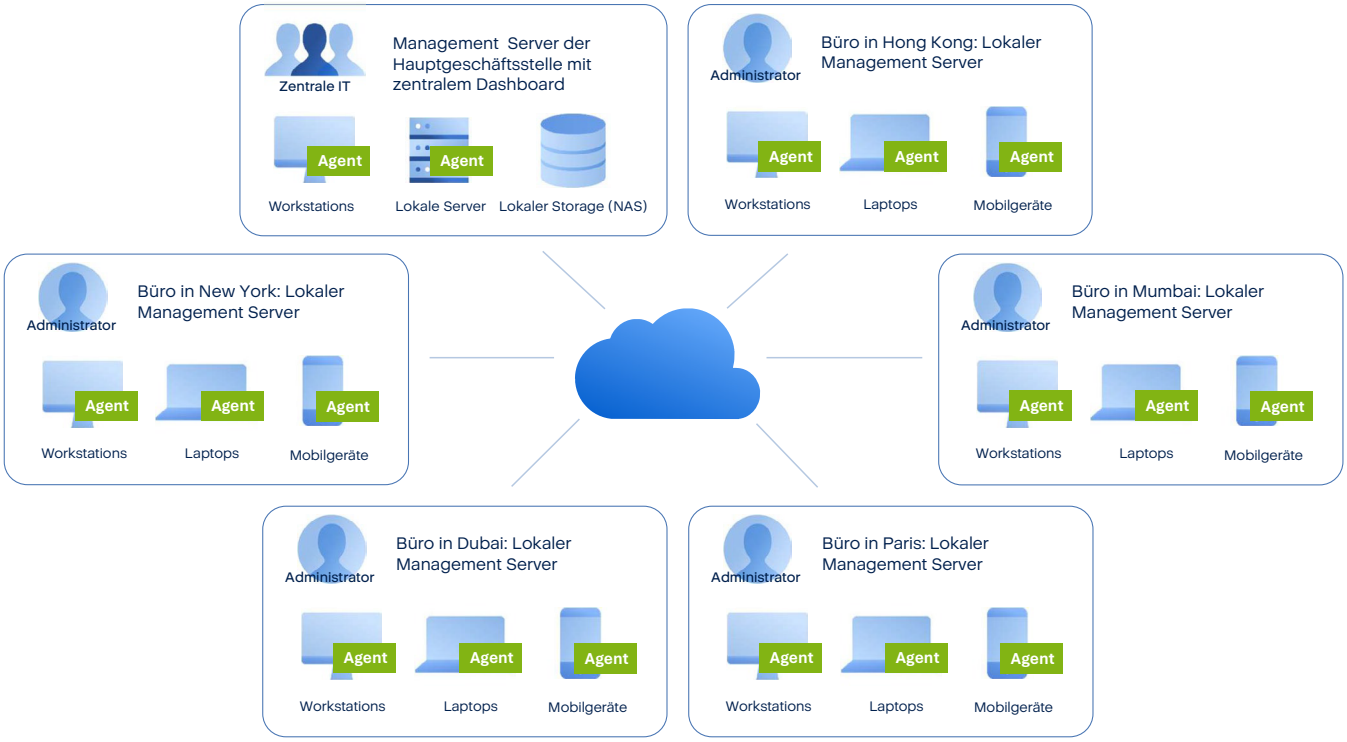

Abbildung 1. Lokal gesteuerte und zentral überwachte Verwaltung der Cyber Security und des IT-Betriebs in Unternehmen mit mehreren Standorten

Hauptvorteile von Acronis Cyber Protect

- Speichert und sichert Daten nach Standort.
- Reduziert oder beseitigt Kompatibilitätsprobleme bei Hardware, Software und Virtualisierung, die die Cyber Security beeinträchtigen.
- Löst Probleme mit der Datenhoheit und erleichtert die Einhaltung von Compliance-Vorschriften.
- Beseitigt Probleme im Zusammenhang mit unterschiedlichen Netzwerkkonfigurationen und -verbindungen.
- Reduziert oder beseitigt die Notwendigkeit von mehreren Hosting-Umgebungen für Data Protection.
- Einheitliche und vorhersehbare Kosten für alle physischen Standorte.
- Optimiert die Implementierung von Geo-Redundanz.
- Ermöglicht eine zentrale Überwachung für die unternehmensweite Bewertung von Cyberrisiken sowie Data Protection- und Compliance-Status.

Die Lösungen von Acronis sind image- und dateibasiert und verwenden einen plattformübergreifenden Agenten, der mit den meisten IT-Systemen in Geschäfts- und Produktionsumgebungen kompatibel ist. Acronis schützt auch Cloud-basierte E-Mail- und Kollaborationsplattformen wie Microsoft 365 und Google Workspace sowie standortbasierte Plattformen wie lokale Microsoft Exchange Server.

Von Acronis unterstützte Umgebungen

VMWare vSphere 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Microsoft Hyper-V Server 2022, 2019, 2016, 2012/2012 R2, 2008/2008 R2

Citrix XenServer / Citrix Hypervisor 8.2 – 4.1.5

Linux KVM 8 – 7.6

Scale Computing HyperCore 8.8, 8.9, 9.0

Red Hat Enterprise Virtualization (RHEV) 3.6 – 2.2

Red Hat Virtualization (RHV) 4.0, 4.1

Red Hat Virtualization (oVirt) 4.2, 4.3, 4.4

Virtuozzo 7.0.14 – 6.0.1.0

Virtuozzo Infrastructure Platform 3.5

Oracle Linux Virtualization Manager (Oracle LVM) 4.3

Nutanix Acropolis Hypervisor (AHV) 20160925x – 20180425x

Virtuozzo Hyper Server 7.5

Virtuozzo Hybrid Infrastructure 4.3 – 3.5

Datenhoheit und Compliance für verteilte Umgebungen

Acronis betreibt ein globales, unabhängiges Netzwerk von Datenzentren mit Standorten in der ganzen industrialisierten Welt, das dezentralisierten Unternehmen ein hohes Maß an Flexibilität bei der sicheren Datenspeicherung bietet, um die Data Protection-Performance zu optimieren und die Einhaltung von Vorschriften zur Datenhoheit zu unterstützen. Einzelne Remote-Standorte können ihre Data Protection und Security nach Standort verwalten und ihre Server-, Endpunkt-, E-Mail- und Kollaborationsdaten in den Ländern speichern, in denen dies aus Compliance-Gründen erforderlich ist.

Durch die Integration von Endpunktverwaltung, Data Protection und Cyber Security in einer einzigen Plattform mit lokalen Konsolen können die IT-Betriebskosten um bis zu 60 % gesenkt werden. Die Unternehmen sparen zusätzlich, da sie weniger Gemeinkosten für die Schulung von Personal und die Wartung mehrerer IT- und Cyber Security-Tools aufwenden müssen und geringere Kosten für die Geo-Compliance bei der Datenspeicherung und -übermittlung durch Drittanbieter entstehen.

Unternehmen mit mehreren Standorten stehen bei der Implementierung und Wartung von Sicherheits-, Backup- und Disaster Recovery-Lösungen vor besonderen Herausforderungen. Dazu gehören die Verwaltung von Lösungen an mehreren Standorten, die Steuerung und Wartung von Diensten über unzählige Kombinationen von Hardware- und Softwaretechnologien hinweg, die Einhaltung von Datenschutz- und Datenhoheitsvorschriften sowie die Bereitstellung dieser Dienste in einer Umgebung mit begrenzten Ressourcen und Budgets. Diese Herausforderungen werden noch größer, wenn Unternehmen über internationale Grenzen hinweg tätig sind.

Vorteile der Verwaltung mehrerer Standorte

Lokale Konsolen für Remote-Standorte mit unabhängigen Agenten

- Eine lokal oder in der Cloud gehostete Konsole für jeden Standort, jede Abteilung, jeden Geschäftsbereich oder jede Marke.
- Bandbreitenbegrenzung, Datenkomprimierung und Deduplizierung, immer inkrementell, mit optionalem physischem Laufwerktransport.
- Agent an der Quelle mit Datenverschlüsselung und sicherer Datenübertragung über TLS. Die Nutzung des Unternehmensnetzwerks ist nicht erforderlich.

Zentrales Dashboard in der Firmenzentrale zur Überwachung aller Acronis Konsolen an Remote-Standorten

- Überwachen Sie alle Acronis Konsolen an Remote-Standorten gemeinsam oder einzeln.
- Verschaffen Sie sich einen konsolidierten Überblick über alle Geräte, Alarme und Aktivitäten an den Remote-Standorten.
- Laden Sie Daten von Acronis Remote-Konsolen mithilfe von Widgets herunter.
- Navigieren Sie auf jeder beliebigen Acronis Remote-Konsole zu bestimmten Geräten.

Konsolidierung mehrerer Tools

Verwaltung über einen einzigen Agenten und eine einzige Konsole:

- Backup und Disaster Recovery.
- E-Mail- und Endpunktschutz mit Endpoint Detection and Response (EDR).
- Patching, Inventarisierung, Remote-Unterstützung, Skripting und Überwachung.

Geschützte Workloads

- Server, VM, Cloud-VM und Workstations.
- Desktops, Laptops und mobile Geräte.
- Windows (zurück bis 2003/XP), Mac, Linux.
- Microsoft 365 und Google Workspace.

Verbesserte lokale Compliance

Über 50 globale Datenzentren.

- 11 europäische Datenzentren.
- 2 deutsche Datenzentren.

Die Daten werden an der Quelle mit AES-265 und unternehmensinternen Passwörtern verschlüsselt.

Die Daten werden bei der Übertragung über SSL/TLS verschlüsselt.

Unveränderlicher Speicher.

Mehrfaktor-Authentifizierung.

Rollenbasierte Zugriffsverwaltung.

Globale Compliance-Zertifizierungen.

Geringere Kosten und weniger Komplexität bei Anbietern

Die Konsolidierung mit Acronis ermöglicht Einsparungen von bis zu 60 % im Vergleich zum Einsatz mehrerer Tools von verschiedenen Anbietern.

Ressourcenengpässe werden verhindert

Eine einzige Management-Konsole.

KI und Machine Learning (ML) zur Unterstützung bei alltäglichen Aufgaben.

- Geräteüberwachung und automatische Fehlerbehebung.
- KI-gestützte Untersuchung und Behebung von Sicherheitsvorfällen.
- Automatische Backup- und Disaster Recovery-Tests.
- Automatisierte Skriptbibliothek für Wartungsaufgaben.

Schlussgedanken

In den meisten Unternehmen werden der IT-Betrieb und die Cyber Security von zentralen IT-Abteilungen verwaltet. Einige Unternehmen werden jedoch feststellen, dass die Delegierung bestimmter IT- und Sicherheitsverwaltungsaufgaben an Teams in regionalen und/oder Remote-Standorten die Cyber-Resilienz verbessern kann.

Die dezentrale Verwaltung der Schutzmaßnahmen eines Unternehmens gegen Cyberbedrohungen und andere Ursachen von Ausfallzeiten und Datenverlusten sowie die Fähigkeit, Daten und Verfügbarkeit nach einem Vorfall schnell wiederherzustellen, können das Geschäftsrisiko wirksamer verringern als eine zentrale Verwaltung.

In diesen Szenarien mit mehreren Standorten und lokaler Verwaltung sollten Unternehmen ihre regionalen und Remote-Teams mit Tools ausstatten, die Cyber Security, Data Protection und Endpunktverwaltung nativ integrieren. Durch die zusätzliche zentrale Überwachung der regionalen und Remote-Konsolen können die IT- und Cyber Security-Teams in der Unternehmenszentrale die IT-Governance- und Compliance-Standards des Unternehmens überprüfen und durchsetzen.

Die Kombination aus zentraler Überwachung und dezentraler Verwaltung von IT-Betrieb und Cyber Security kann die Reaktionsfähigkeit des Supports optimieren (insbesondere bei Einrichtungen, die vom Rest des Netzwerks getrennt sind, und sehr abgelegenen Einrichtungen), die Einhaltung regionaler Sicherheits- und IT-Vorschriften verbessern und das Geschäftsrisiko insgesamt verringern.

Mehr erfahren

Kontaktieren Sie Acronis hier, um ein unverbindliches Beratungsgespräch mit dem Acronis Team zu führen und zu erfahren, ob eine zentral überwachte, geografisch verteilte Verwaltungsstruktur für Cyber Security und IT-Betrieb für Ihr Unternehmen sinnvoll ist.

Holen Sie sich hier eine kostenlose 30-tägige Testversion von Acronis Cyber Protect.

Über Acronis

Acronis ist ein globales Unternehmen für Cyber Protection, das direkt integrierte Cyber Security, Data Protection und Endpunktverwaltung für Managed Service Provider (MSPs), kleine und mittlere Unternehmen (KMU) sowie IT-Abteilungen von Unternehmen bereitstellt. Die Lösungen von Acronis sind hocheffizient und darauf ausgelegt, moderne Cyberbedrohungen zu identifizieren, zu verhindern, zu erkennen, darauf zu reagieren, sie zu beseitigen und sich mit minimalen Ausfallzeiten von ihnen zu erholen. Dank diesem vollständigen Ansatz werden die Datenintegrität und Kontinuität des Geschäftsbetriebs gewährleistet. Acronis bietet MSPs die umfassendste Sicherheitslösung auf dem Markt und erfüllt auf einzigartige Weise die Anforderungen vielfältiger und verteilter IT-Umgebungen.

Das im Jahr 2003 in Singapur gegründete Unternehmen Acronis hat seinen Hauptsitz in der Schweiz und 45 Standorte weltweit. Acronis Cyber Protect Cloud ist in 26 Sprachen sowie in über 150 Ländern verfügbar und wird bereits von über 20.000 Service Providern zum Schutz von mehr als 750.000 Unternehmen eingesetzt. Weitere Informationen finden Sie auf www.acronis.com.

Acronis

Weitere Informationen auf **www.acronis.com.**