Acronis

#CyberFit

Acronis Cyber Protect Cloud

Modernisierung von Cyber Security und Backups
mit integrierter Cyber Protection

Die Bedrohungslandschaft wird komplexer

300 %

Steigerung bei Cyberkriminalität während der COVID-19-Pandemie

57 %

der Angriffe werden von herkömmlichem Virenschutz nicht erkannt

69 %

verbringen mehr Zeit mit der Verwaltung der Tools als mit der Abwehr von Bedrohungen

Quellen: Acronis Cyberthreats Report 2020, Acronis Cyber Readiness Report, 2020, FBI

Lösung: Integrierte und autonome Cyber Protection

Das Ziel von Acronis: Der Schutz aller Daten, Applikationen und Systeme (Workloads)

S

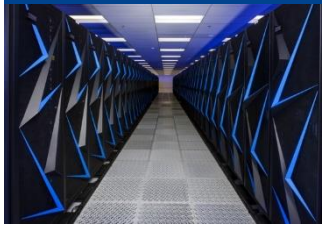
Safety (Verlässlichkeit)

Nichts geht verloren: Es steht jederzeit eine Kopie zur Wiederherstellung zur Verfügung

A

Accessibility (Verfügbarkeit)

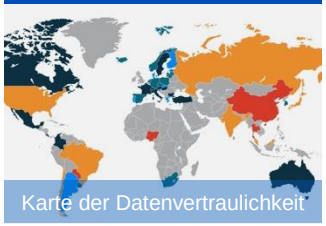
Datenabruf jederzeit und von überall möglich



P

Privacy (Vertraulichkeit)

Kontrolle über Sichtbarkeit und Zugriff



Karte der Datenvertraulichkeit

A

Authenticity (Authentizität)

Nachweis, dass Kopie exaktes Replikat des Originals ist

S

Security (Sicherheit)

Schutz vor böswilligen Akteuren

Was wäre, wenn Sie auf eine einzige integrierte Lösung vertrauen könnten?

Steigerung Ihrer monatlichen wiederholten Umsätze

Einfacheres Upselling mithilfe integrierter Lösungen

Vereinfachte Verlängerungen mit integrierten Berichten

Höherer ROI durch vorgefertigte Marketing-Kampagnen

Senkung der Cyber Protection-Kosten um bis zu 50 %

Eine Konsole, eine Lizenz, ein Agent

Integration ermöglicht umfassendere Automatisierung

Konsolidierung der Anbieter-Ausgaben

Bereitstellung hervorragender Cyber Protection

Weniger Risiken durch 100 % Abdeckung der Client-Workloads

Einzigartige Möglichkeiten bei Ihren aktuellen Sicherheitsanbietern nicht verfügbar

Bei unabhängigen Tests führend (VB100, AV-TEST, AV-Comparatives)

KI-gestützte Integration von Data Protection und Cyber Security

Schutz

Intelligente Sicherungspläne basierend auf Acronis Bedrohungsalarmen

Erkennung

KI/ML-Bedrohungserkennung und -Verhaltensanalyse

Reaktion

Reaktion auf Angriffe mit vollständiger KI-gestützter Transparenz am Edge

Recovery

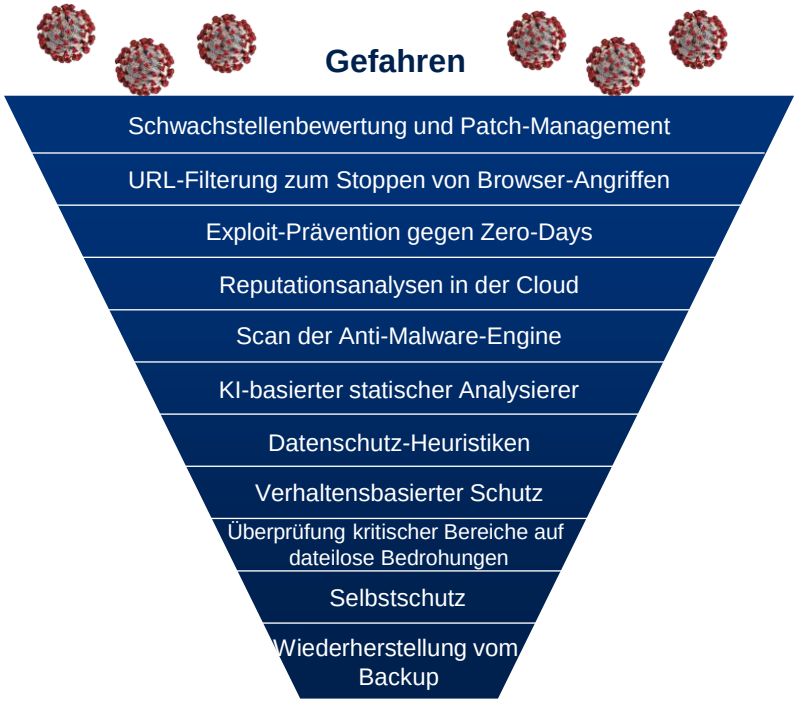
Wiederherstellung nach Angriffen ohne Datenverluste und mit integriertem Patching

Forensik

Schnelle und präzise Untersuchungen mit Backups und umfangreichen Forensikdaten

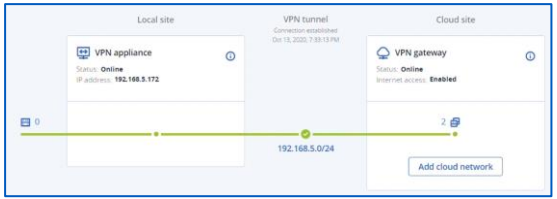
Acronis Cyber Protect

Ein komplettes und modernes Sicherheitspaket, das durch Backup-Daten ergänzt wird



Ransomware-Wiederherstellung - falls erforderlich

- **Geschützte Backup-Dateien**
- **Spin-up-Backups als virtuelle Maschinen**
- **Ausfallsicherung im Katastrophenfall**
- **Wiederherstellung sichern - Scannen/Patching von Sicherungen**
- **Versand von physischen Festplatten**
- **Forensische Daten in Backups**



Erstklassiges Backup mit integrierter Sicherheit und Verwaltung

Kostenloser Schutz aller Workloads

Inklusive erstklassiger Backups

Stärkung Ihres Virenschutzes bei Zero-Day-Bedrohungen

Beschleunigte Sicherheit und Verwaltung

Zusätzliche Advanced-Pakete: Security, Management, Backup, Disaster Recovery, Email Security, File Sync and Share

Optimierung für jeden Workload | **Einfaches Upselling** | **Anbieter-Konsolidierung**

Problembereiche von Service Providern bei der Verwaltung

Schließen offener Sicherheitslücken und Reduzierung des Verwaltungsaufwands

Angriffe über ungepatchte Systeme

- Im Durchschnitt erfolgen Patches erst nach **102** Tagen
- **60 %** der Angriffsopfer sagen, dass die Attacke über eine bekannte Schwachstelle erfolgte, für die es einen verfügbaren Patch gab, der jedoch noch nicht angewendet wurde
- Nur **44 %** aller Unternehmen nutzen Automatisierung, um Schwachstellenverwaltung und Patching zu vereinfachen

Ineffiziente Planung

- **76 %** der Sicherheits- und IT-Teams fehlt ein einheitlicher Überblick über Anwendungen und Assets
- **70 %** aller Unternehmen haben keinen vollständigen Überblick darüber, welche Assets wann gewartet oder aktualisiert werden müssen, wobei **50 %** aller Festplatten innerhalb von 5 Jahren ausfallen
- **30 %** Steigerung der Ausfallzeiten in Unternehmen aufgrund schlechter Patch-Verwaltung und Verzögerungen beim Patchen von Schwachstellen

Zu viele Lösungen

- **53 %** der IT-Teams geben zu, dass die enorme Anzahl an Sicherheitstools ihre Sicherheit beeinträchtigt und das Risiko erhöht

Quellen: „State of Endpoint Security Risk“ (Der Stand bei Endpunkt-Sicherheitsrisiken), Ponemon Institute; „Cost of Data Breach Report“ (Bericht zu den Kosten von Datenschutzverletzungen), Ponemon Institute, 2020; „After The Fall: Cost, Causes and Consequences of Unplanned Downtime“ (Nach dem Vorfall: Kosten, Ursachen Folgen ungeplanter Ausfallzeiten), VansonBorne; „Costs and Consequences of Gaps in Vulnerability Response“ (Kosten und Folgen von Lücken bei der Reaktion auf Schwachstellen), ServiceNow, 2019; „Security Technology Sprawl Report“ (Bericht zur Technologieflut), ReliaQuest, 2019

Acronis Cyber Protect Cloud mit Advanced Management

Verbessern Sie den Schutz Ihrer Kunden, indem Sie deren Systeme auf dem aktuellen Stand halten und gleichzeitig Verwaltungsaufwand und Gesamtbetriebskosten minimieren.

Erweiterte Patch-Verwaltung

Halten Sie Systeme auf dem aktuellen Stand und beheben Sie Schwachstellen proaktiv.

Automatisierte Patch-Verwaltung

Sparen Sie durch die automatisierte Patch-Verwaltung und die ausfallsichere Patch-Technologie Zeit und Aufwand.

Umfassende Verwaltungstools

Vereinfachen Sie die Planung durch Software-Inventarisierung, Berichtsplanung und Überwachung des Laufwerkszustands.

Problembereiche von Service Providern in Bezug auf Sicherheit

Zunehmende digitale Bedrohungen

- 80 % der Kompromittierungen sind neue oder unbekannte „Zero-Day-Angriffe“
- Ransomware, die Backups und VSS angreift, nimmt zu: HelloKitty, Cerber, DeroHE

Komplexe Verwaltung und Fachkräftemangel

- Automatisierung der Sicherheit reduziert die Gesamtkosten bei Datenschutzverletzungen auf fast ein Drittel, doch 41 % der Unternehmen haben noch nicht einmal mit der Implementierung begonnen
- 43 % der Unternehmen kämpfen bei 20 % der Erkennungen mit Fehlalarmen
- 53 % geben zu, dass die enorme Anzahl an Sicherheitstools ihre Sicherheit beeinträchtigt und das Risiko erhöht
- 84 % aller Organisationen berichten über einen Mangel an IT-Sicherheitsfachkräften

Komplexe Behebungsmaßnahmen

- 208 Tage – Zeitraum von der Identifizierung bis zur Eindämmung einer Sicherheitsverletzung
- 55 % der Service Provider-Kunden können die Ursachen für die festgestellten Sicherheitsverletzungen nicht vollständig beheben
- 80 % der Vorfälle betreffen personenbezogene Informationen (aufgrund gesetzlicher Vorgaben sind Analysen nach dem Zwischenfall erforderlich)

Quellen: „State of Endpoint Security Risk“ (Der Stand bei Endpunkt-Sicherheitsrisiken), Ponemon Institute; „Cost of Data Breach Report“ (Bericht zu den Kosten von Datenschutzverletzungen), Ponemon Institute, 2020; „After The Fall: Cost, Causes and Consequences of Unplanned Downtime“ (Nach dem Vorfall: Kosten, Ursachen Folgen ungeplanter Ausfallzeiten), VansonBorne; „Costs and Consequences of Gaps in Vulnerability Response“ (Kosten und Folgen von Lücken bei der Reaktion auf Schwachstellen), ServiceNow, 2019; „Security Technology Sprawl Report“ (Bericht zur Technologieflut), ReliaQuest, 2019

Acronis Cyber Protect Cloud mit Advanced Security

Verbessern Sie die Sicherheit, indem Sie mehr Bedrohungen erkennen, sparen Sie Kosten durch vereinfachte Sicherheitsverwaltung und bieten Sie durch integrierte Cyber Protection bessere Behebung.

Vollständiger Malware-Schutz

Zusätzlich zu Acronis Active Protection erhalten Sie Exploit-Schutz, URL-Filterung, Malware-Erkennung für Backup-Daten sowie eine verbesserte Erkennungsrate, um Bedrohungen noch schneller zu identifizieren.

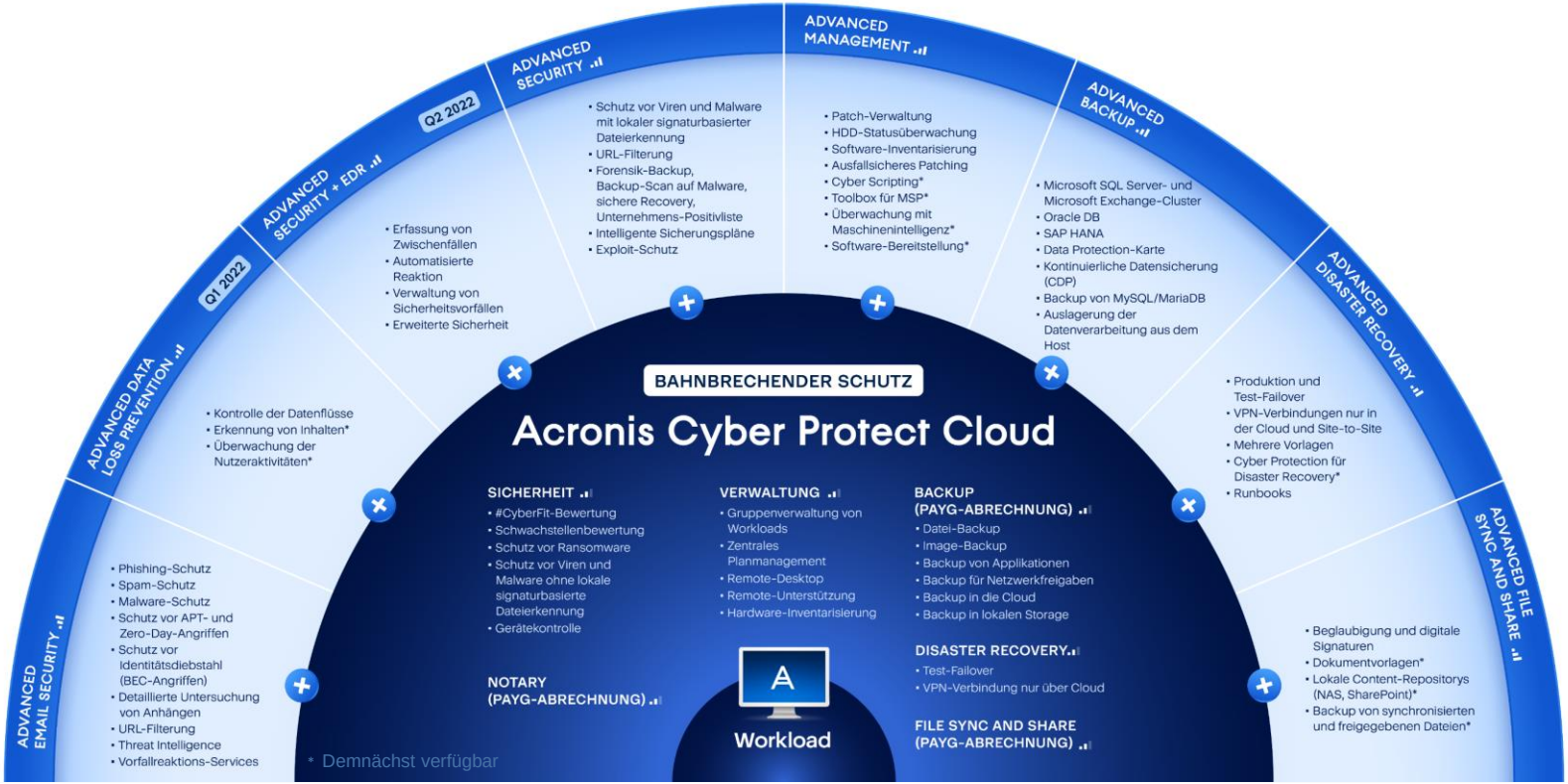
Sicherheitsautomatisierung

Intelligente Sicherungspläne, automatische Positivliste für kundenspezifische Apps, automatisierte Malware-Scans und Updates für Virenschutzdefinitionen im Rahmen des Recovery-Prozesses, damit Sie Services noch einfacher bereitstellen können.

Effiziente Forensik

Erfassen Sie digitale Beweise und speichern Sie sie in einem sicheren zentralen Repository, um gründliche Untersuchungen nach dem Zwischenfall und zuverlässige Behebung zu ermöglichen und gleichzeitig die Kosten niedrig zu halten.

Roadmap 2022 für Service Provider



Weniger Risiken für Ihre Kunden

Beseitigung von Lücken in Ihren Abwehrmaßnahmen

Bereitstellung umfassender Cyber Protection mit einzigartiger Integration von Data Protection und Cyber Security

Upgrade des Schutzes für alle Workloads

Besserer Schutz für alle Workloads durch grundlegende Cyber Protection

Sofortige Wiederherstellung ohne Datenverlust

Vermeidung von Ausfallzeiten mit minimalen RPOs und RTOs für alle Benutzer und Applikationen

Verkaufen Sie Backup? Upselling auf Acronis Cyber Protect

Mehr als nur Backup: Die sicherste, einfachste und zuverlässigste Backup-Lösung für MSPs

Proaktiver Schutz

- Schwachstellenbewertung und Patch-Verwaltung zur Vermeidung von Ausfallzeiten und Maintenance-Aufwand
- Entfernung von Malware aus Backups
- Verhinderung wiederkehrender Infektionen (Patch bei Wiederherstellung)
- Verhinderung, dass Backups gelöscht werden (unveränderliche Backups)

Aktiver Schutz

- Kontinuierliche Datensicherung (Continuous Data Protection, CDP) zur Vermeidung von Datenverlusten
- Active Protection zum Schutz vor Ransomware und anderer Malware zur Vermeidung von Ausfallzeiten
- Selbstschutz für den Agenten und den Backup Storage

Reaktiver Schutz

- Integrierte Disaster Recovery-Funktionen
- Sofortige Recovery: keine Datenverluste, minimale RTO & RPO
- Metadaten-Speicher für Forensik und Vorfalluntersuchungen

Verbesserte Produktivität

- Schutz der maximalen Anzahl an Workloads pro MSP-Techniker
- Integrierte Remote-Verwaltung für schnellen Zugriff auf geschützte Workloads
- Vorab konfigurierte Sicherungspläne für Remote-Mitarbeiter

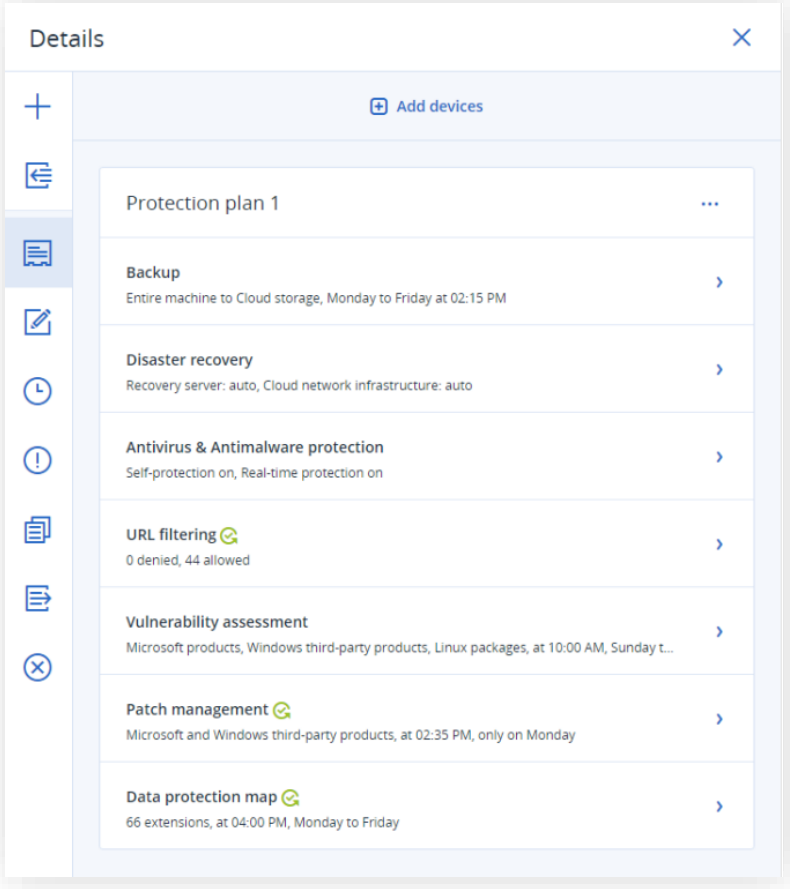
Umfassende Integration bietet neue Möglichkeiten

Integration auf allen Ebenen: Verwaltung, Produkte und Technologien

Die ganze Power der Einheitlichkeit:

- Vermeidet Komplexität
- Ermöglicht neue Sicherheitsfunktionen
- Senkt die Kosten
- Verwaltet alle Kunden von einer Konsole aus
- Effiziente Support-Eskalationen bei einem Anbieter

1 Agent • Richtlinie • UX/UI • Lizenz • Anbieter



Basierend auf erstklassigen Backup-Funktionen für MSPs

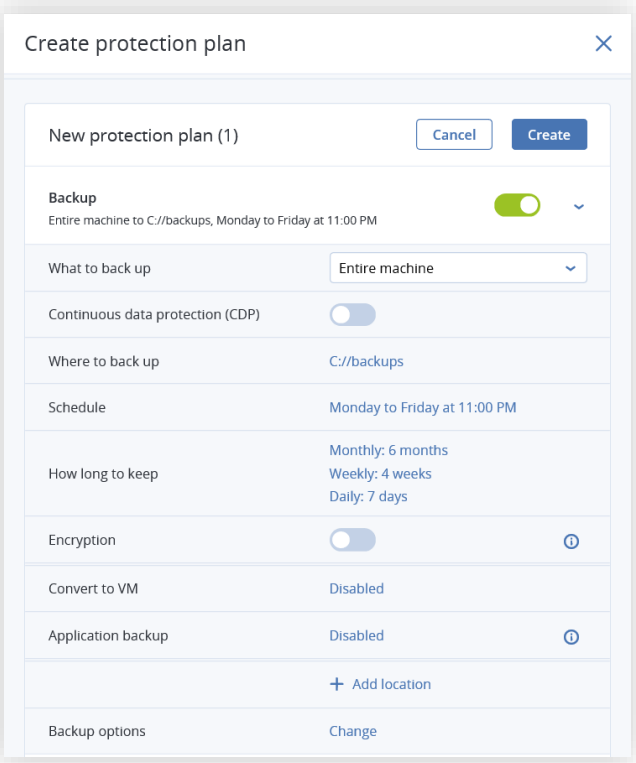
Hybrid Cloud-Architektur	**Mehr als 20 geschützte Workload-Typen**	**Datei- und Image-Backups**
Umgehende Wiederherstellung	**Flexible Speicherung**	**Für MSPs entwickelt**

Vorteile: Schnelleres Recovery und bessere RTOs

Backups vollständiger Images oder einzelner Dateien

Erstellen Sie Backups einzelner Dateien oder schützen Sie Ihr gesamtes Unternehmen mit wenigen Klicks.

- **Datei-Backups:** Nutzen Sie diese Option zum Schützen bestimmter Daten und reduzieren Sie dabei die Backup-Größe und den erforderlichen Speicherplatz.
- **Vollständige Image-Backups:** Sie können ganz einfach komplette Systeme als eine einzelne Datei sichern. Das ermöglicht Wiederherstellungen auf fabrikneue Hardware (Bare Metal Restore).
- Bei Bedarf können Sie alle gesicherten Informationen ganz einfach und konsistent wiederherstellen – auch auf neuer Hardware (Bare Metal Recovery).



Vorteile: Gewährleistung der Geschäftskontinuität mit flexiblen Backup-Optionen und gleichzeitig Vermeidung von Ausfallzeiten und Datenverlust

Flexible Storage-Optionen

Einhaltung gesetzlicher Vorschriften und der Kostenanforderungen

Cloud Storage

Google Cloud Platform
Acronis Cyber Cloud Storage
Azure

Drei direkt einsetzbare Cloud Storage-Optionen

Alibaba Cloud
aws
IBM Cloud
IIJ
wasabi

Andere Public Clouds *(über Acronis Backup Gateway)*

Eigener oder Drittanbieter-Cloud Storage

On-Premise-Storage

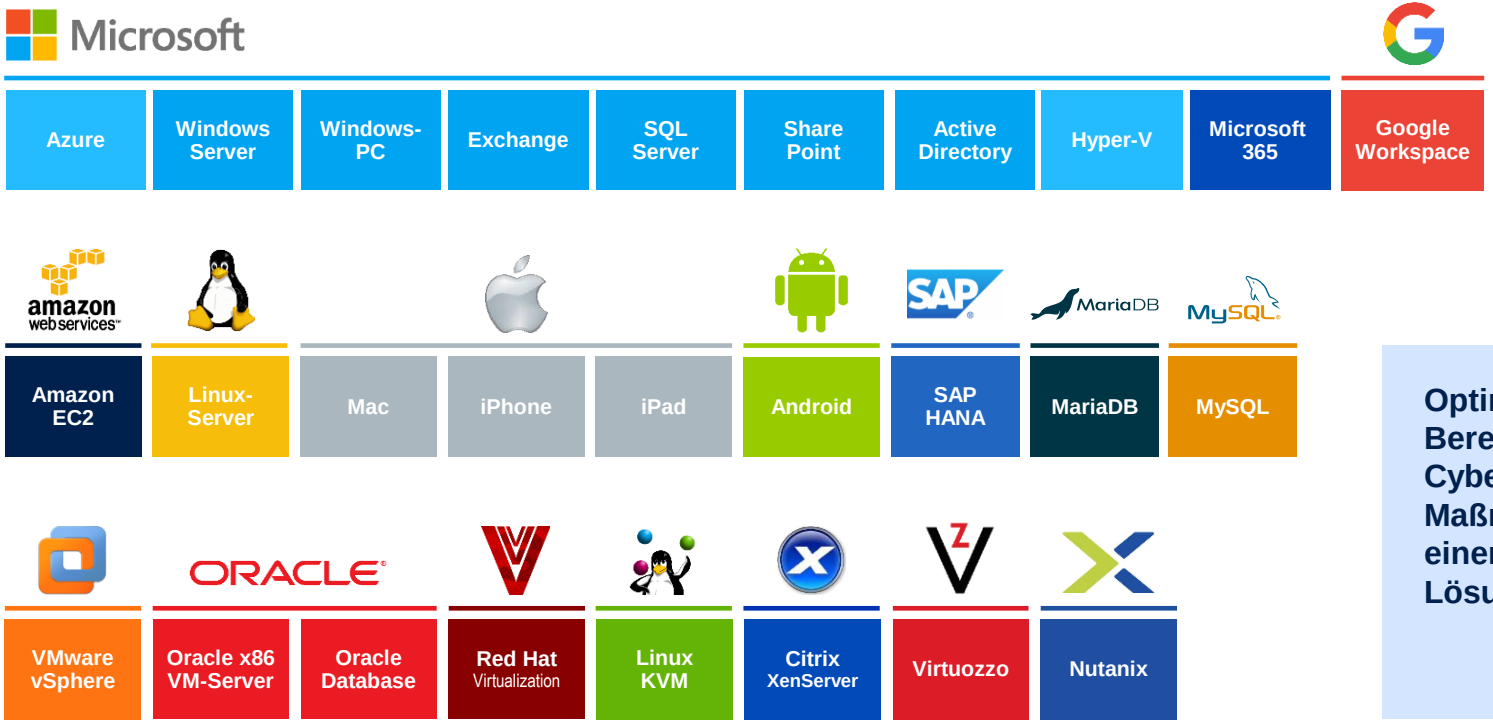
Lokale Laufwerke

SMB/CIFS/DFS und NFS-Freigaben

On-Premise Acronis Storage

> Bei anderen Lösungen mussten wir unseren Kunden sagen, dass bestimmte Dinge nicht möglich sind. **Bei Acronis genießen wir vollständige Flexibilität**, sodass wir eine hervorragende Benutzererfahrung bieten können.
>
> **Jason Amato,**
> Marketing Manager bei Centorrino Technologies

Schutz für mehr als 20 Workload-Typen von Infrastruktur bis SaaS-Apps

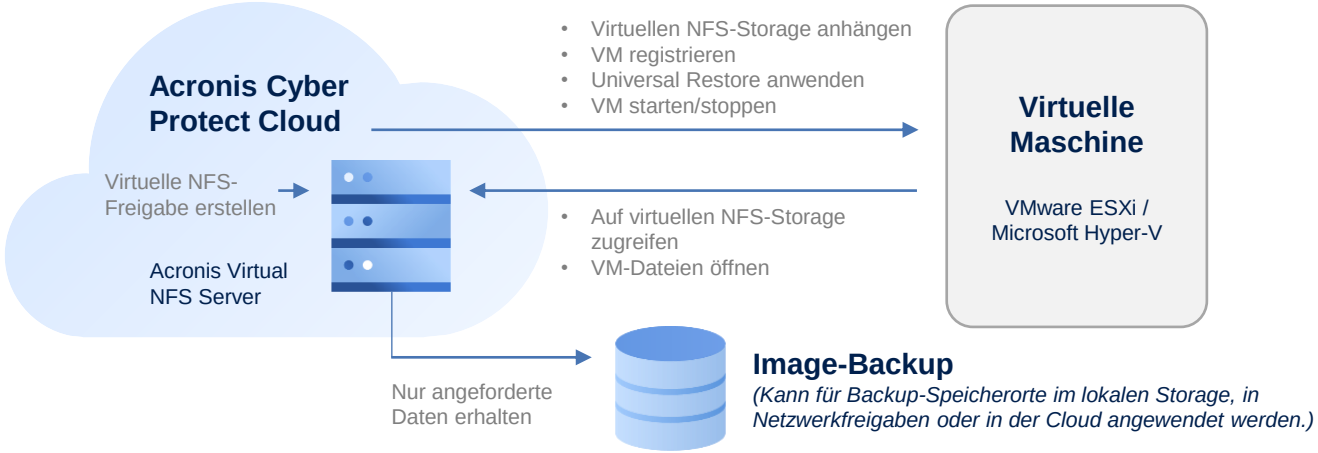


Optimierte Bereitstellung von Cyber Protection-Maßnahmen mit einer zentralen Lösung

Branchenweit beste RTOs dank Acronis Instant Restore

Mit der patentierten Acronis Instant Restore Technologie können Sie Systeme innerhalb von Sekunden wiederherstellen, indem ein beliebiges Windows- oder Linux-System (physisch oder virtuell) direkt aus dem Backup Storage Ihres bestehenden Microsoft Hyper-V- oder VMware vSphere ESXi-Hosts gestartet wird. Dafür müssen keine Daten bewegt werden.

Die Funktionsweise



Vorteile

- RTO von Sekunden
- Wiederherstellung aller virtuellen, physischen und Cloud-Systeme (Server, Windows und Linux)
- Reduzierte Ressourcen-Belastung

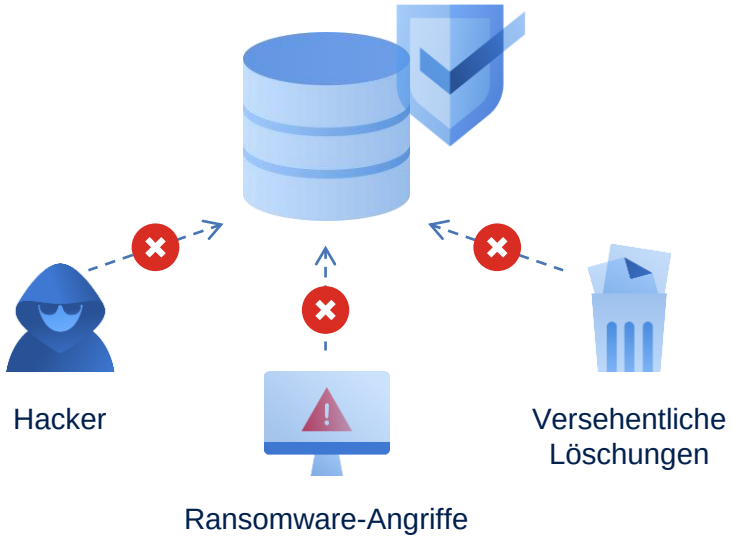
Unveränderliche Backups

Stärken Sie die Compliance und verhindern Sie durch verzögertes Löschen von Backups Datenverlust.

Stellen Sie sicher, dass keine Backups verloren gehen und Daten sich nach einem Malware-Angriff oder einer versehentlichen oder böswilligen Löschung von Backups leicht wiederherstellen lassen.

Anwendungsfälle:

- Externe böswillige Aktivitäten (z. B. Daten werden beschädigt oder kompromittiert)
- Versehentliche Datenlöschung
- Böswillige Insider-Aktivitäten (z. B. Modifizierung der Aufbewahrungsregeln für Backup-Aufträge oder Löschung von Wiederherstellungspunkten)

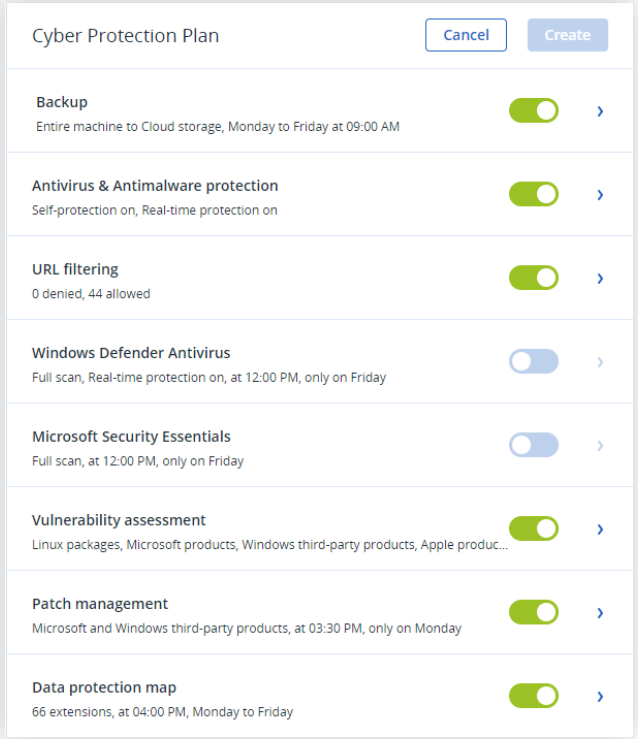


Vorteile: Stets wiederherstellbare und ausfallsichere Daten

Sicherungsplan

Effiziente Aktivierung, Deaktivierung und Konfiguration von Services und Richtlinien für einzelne Kunden oder auf Gruppenebene:

- Backup
- Malware-Schutz
- Disaster Recovery
- URL-Filterung
- Schwachstellenbewertungen
- Patch-Verwaltung
- Datenerkennung (Data Protection-Karte)
- Verwaltung von Microsoft Defender Antivirus und Microsoft Security Essentials



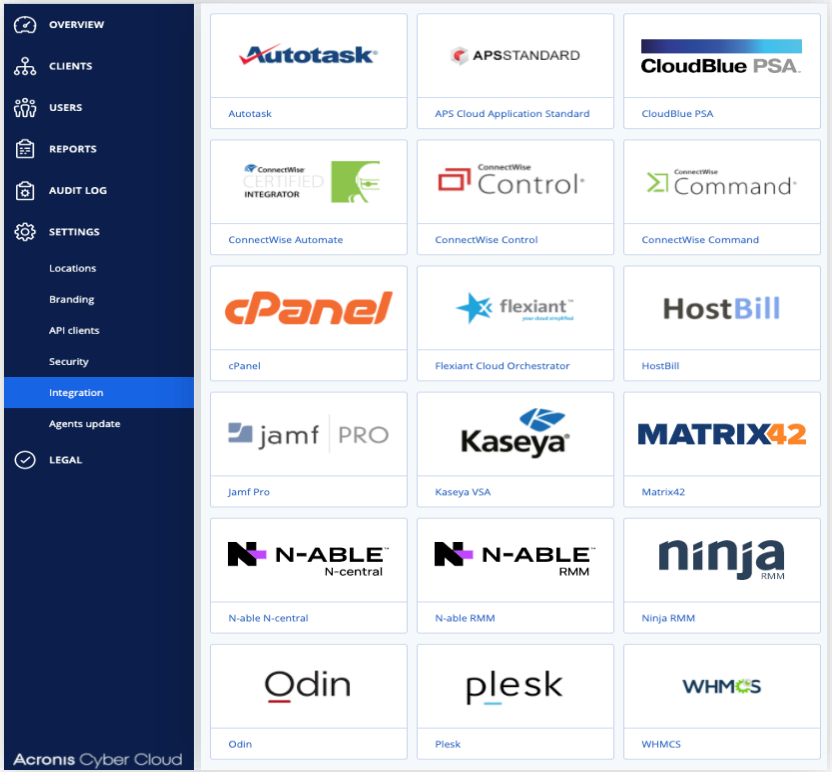
Vorteile: Besserer Schutz mit weniger Aufwand dank Automatisierung

Integration mit Service Provider-Tools

Benötigen Sie eine Lösung, die sich nahtlos in gängige Geschäftsautomatisierungssysteme integriert?

- **Konfigurieren Sie die Integration** mithilfe verschiedener Drittanbietersysteme, z. B.:
  - **RMM- und PSA-Tools:** ConnectWise (Automate, Manage, Control), Kaseya (VSA und BMS), Datto (Autotask und RMM), N-able (RMM und N-central), Jamf Pro, Addigy, Ninja, Tigerpaw und weitere
  - **Hosten Sie Überwachungskonsolen und Abrechnungssysteme:** cPanel, Plesk, WHMCS, HostBill
  - **Marketplace-Anbieter:** CloudBlue, AppDirect, interworks.cloud, Cloudmore, ALSO

- Nutzen Sie eine leistungsstarke **RESTful-Management-API** für eigene Integrationen



Gewährleistung von Compliance und lokale Präsenz

Sie können aus weltweit 26 Datenzentren wählen: von Acronis gehostet, Google Cloud und Microsoft Azure

40+7

DATENZENTREN

Starke Präsenz im Asien-Pazifik-Raum: Singapur, Japan, Australien

Sicherheit von Acronis in der Branche anerkannt

MVI-Mitglied	VIRUSTOTAL-Mitglied	Mitglied der Cloud Security Alliance
Mitglied der Anti-Malware Testing Standard Organization	Mitglied der Anti-Phishing Working Group	Teilnehmer und Testsieger bei MRG-Effitas
Teilnehmer und Testsieger bei Anti-Malware Test Lab	Zertifiziert durch ICSA Lab	Teilnehmer und Testsieger bei NioGuard Security Lab
Durch AV-Comparatives bestätigtes Business-Sicherheitsprodukt	VB100-zertifiziert	Teilnehmer und Testsieger bei AV-TEST

Zertifizierungen für Acronis Sicherheit

FIPS 140-2

Acronis AnyData Cryptographic Library wurde von NIST erfolgreich verifiziert

GDPR

Laut einer Selbstbewertung vom 25. Mai 2018 hält Acronis die GDPR-Bestimmungen ein.

GLBA (Gramm-Leach-Bliley Act)

GLBA gilt für Finanzinstitute, konform entsprechend Titel V, Zwischentitel A, Abschnitt 501.(b).

HIPAA

Eine unabhängige externe Lückenanalyse hat gezeigt, dass Acronis mit den HIPAA-Vorschriften konform ist.

ISO 27001

Acronis bietet ein Informationssicherheits-Verwaltungssystem entsprechend Standard ISO 27001:2013.

ISO 9001

Mit ISO 9001:2015 konform.

TAA

Acronis products Acronis Produkte sind „TAA-konform“ und wurden in der Schweiz produziert oder „im wesentlichen Maße transformiert“.

Privacy Shield

Acronis ist entsprechend dem EU-US und Swiss-US Privacy Shield zertifiziert.

MSPs über Acronis Cyber Protect Cloud

Das **Produkt bietet unglaublich viele intelligente Funktionen**. Es lohnt sich, den Data Protection-Ansatz zu verfolgen, da Sie dabei an Dinge denken, die anderen Anbietern gar nicht in den Sinn kommen. Das Produkt bietet einfach enorme Geschäftsmöglichkeiten und wir sind absolut begeistert davon.

> Unser Ziel (mit Acronis Cyber Protect) besteht darin, die Nutzerbasis bei unseren Kunden so weit wie möglich zu verbreitern.

Einer der größten Vorteile von Acronis Cyber Protect ist die Integration sowie die Möglichkeit, Kunden wirklich zum Sichern Ihrer Daten zu motivieren.

Parallel zu Symantec setzen wir auch Cisco Umbrella für DNS-Filterung und Panorama 9 für Remote-Überwachung und Patch-Verwaltung ein. Natürlich nutzen wir Acronis für das Backup. Wir würden gern **separate Sicherheitslösungen zu einer einzigen kombinieren** – und genau in diese Richtung geht Acronis. Damit bieten sich hervorragende Zukunftsperspektiven und Möglichkeiten, weil wir mit einem Tool viele Aufgaben erledigen könnten.

Wir freuen uns, dass dieses **Produkt so gut funktioniert** und sich so bequem benutzen lässt. Wir kommen gern zu Ihnen und schulen Sie vor Ort – wir wissen, dass Sie das Produkt großartig finden werden, weil wir ebenfalls begeistert sind!

Acronis

#CyberFit

Lizenzierung und Preise

Vereinfachter Ansatz

	Acronis Cyber Cloud C20.08	Acronis Cyber Cloud C21.03
Lizenzierungsmodell (pro GB/pro Workload)	Auf Kundenebene	Auf Kundenebene
Produkt/Editionen	**Zwei Editionen:** • **Acronis Cyber Backup** (pro GB): nur Backup • **Acronis Cyber Protect** (pro Workload): vier Editionen	**Nur ein Produkt: Acronis Cyber Protect Cloud** • Keine Editionen
Zusätzliche Funktionen	Höhere Edition (nur Pro-Workload-Modell)	Advanced-Pakete
Anzahl der SKUs	43	38
Kostenlos verfügbare Cyber Protection-Funktionen	Nein	Ja
Kostenloser Cloud-Storage	Ja (nur Acronis Cyber Protect Cloud)	Ja (Microsoft 365 und Google Workspace)

Acronis Cyber Protect Cloud: Cyber Protection kostenlos für alle Workloads ohne Zusatzkosten

Schützen Sie die Workloads Ihrer Kunden mit grundlegenden Cyber Protection-Funktionen ohne Zusatzkosten.

Funktionen		Acronis Cyber Protect Cloud
Sicherheit	#CyberFit-Bewertung	Enthalten
	Schwachstellenbewertung	Enthalten
	Schutz vor Ransomware	Enthalten
	Schutz vor Viren und Malware: signaturbasierte Dateierkennung ausschließlich über die Cloud (ohne lokale Dateierkennung anhand lokaler Signaturen)	Enthalten
	Schutz vor Viren und Malware: KI-basierte Analyse vor der Ausführung, verhaltensbasierte Cyber Engine	Enthalten
Cyber Protection-Verwaltung	Gruppenverwaltung von Geräten	Enthalten
	Zentrales Planmanagement	Enthalten
	Dashboards und Berichte	Enthalten
	Remote-Desktop und Remote-Unterstützung	Enthalten
	Hardware-Inventarisierung	Enthalten
DLP (Schutz vor Datenverlust)	Gerätekontrolle	Enthalten

Acronis Cyber Protect Cloud:
Funktionen mit nutzungsabhängiger Abrechnung (PAYG)

Gewährleisten Sie den Workloads Ihrer Kunden zusätzlichen Schutz. Sie können das Lizenzierungsmodell auf Kundenebene auswählen. Die Abrechnung ist pro GB oder pro Workload möglich.

Funktionen		Acronis Cyber Protect Cloud
Backup	Backup für Workstations, Server (Windows, Linux, Mac)	PAYG
	Backup virtueller Maschinen	PAYG
	Datei-Backup	PAYG
	Image-Backup	PAYG
	Unveränderliche Backups	PAYG
	Backup für Standard-Anwendungen (Microsoft 365, Google Workspace, Microsoft Exchange, Microsoft SQL)	PAYG
	Backup für Netzwerkfreigaben	PAYG
	Backup in lokalen Storage	PAYG
	Backup in die Cloud	PAYG
Disaster Recovery	Test-Failover in isolierter Netzwerkumgebung	32 Compute-Punkte/Monat*
	VPN-Verbindung nur über Cloud	PAYG
	Firewall-Richtlinienverwaltung	PAYG
File Sync and Share	Funktionen für Dateisynchronisierung und -freigabe	PAYG
Notary	Beglaubigung, digitale Signierfunktionen, Dokumentvorlagen	PAYG

* Partner erhalten 32 Compute-Punkte für Test-Failover, die für den Betrieb mehrerer virtueller Maschinen desselben oder eines anderen Typs verwendet werden können. Weniger VMs oder weniger leistungsfähige VM-Typen werden länger laufen.

Zwei Lizenzierungsmodelle

Pro Gigabyte (GB)

Das Pro-GB-Modell ist einfach: Sie zahlen nur für den genutzten Storage einschließlich des nativen Cloud Storage (Acronis Cloud, Google Cloud Platform, Microsoft Azure), Cloud Storage von Service Providern, Cloud Storage von Drittanbietern und lokalen Storage. Es gibt keine Begrenzung bei der Anzahl geschützter Geräte.

Pro Workload

Beim Pro-Workload-Modell bezahlen Sie für jedes geschützte Gerät (mit unterschiedlichen Preisen für die verschiedenen Gerätetypen) sowie für verwendeten nativen Cloud Storage (Acronis Cloud, Google Cloud Platform, Microsoft Azure). Es fallen jedoch keine Zusatzkosten an, wenn Sie lokalen Storage oder Cloud-Speicher beim Service Provider verwenden.

Vorteile für Service Provider

Schutz der Infrastruktur und Daten von Kunden über Backups hinaus

Höherer Umsatz pro Benutzer

- Verkauf von mehr Cyber Protection-Services
- Höhere Margen für nachgefragte Services
- Mehr Attach-Abschlüsse und höhere Umsätze

Bessere SLAs

- Proaktive Vermeidung von Ausfallzeiten
- Schnellere Behebung mit verbessertem Workload-Schutz
- Gewinnung von mehr Kunden mit besseren SLAs

Volle Kostenkontrolle

- Geringere Ausgaben durch Nutzung eines Tools für alle alltäglichen Aufgaben:
  - Onboarding
  - Überwachung
  - Verwaltung
  - Unterstützung
- Keine neue Hardware/Mitarbeiter erforderlich
- Verbessertes granulares Recovery

Bessere Kundenbindung

- Verbesserung der Kundenzufriedenheit und höhere Wahrscheinlichkeit, dass sie wieder bei Ihnen kaufen
- Demonstration des Mehrwerts und Vereinfachung von Verlängerungen
- Mehr Services – mehr bleibende Kunden

Angebote für Managed Security

- Einfache zusätzliche Umsätze:
  - Keine Investitionen
  - Kein Risiko
  - Keine Suche nach teuren Sicherheitsspezialisten
- Besserer Schutz für Kunden

Vielen Dank!

Noch Fragen?

LUKAS NESTER
Business Development Manager Channel, Acronis

Lukas.Nester@acronis.com
+49 160 95155051