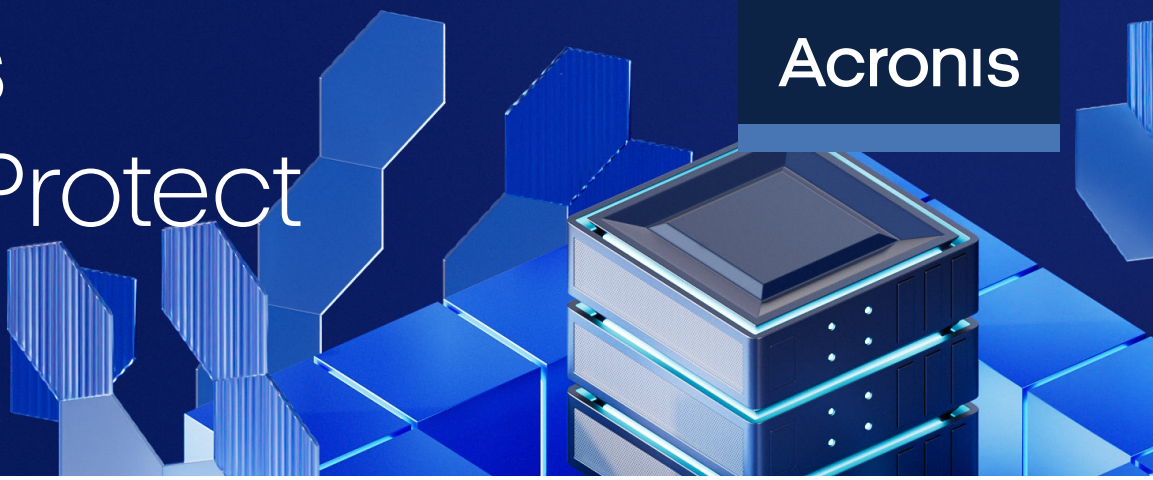
Acronis Cyber Protect



Integrierte Cyber Security, Data Protection und Endpunktverwaltung für Unternehmen

Zentrale Verwaltung und Automatisierung von Endpoint Detection and Response (EDR), Malware-Schutz, Backup und anderen wichtigen Funktionen über eine KI-gestützte Konsole – z. B. für Endpunkte, Ressourcen in Microsoft 365, Server und VMs.

Cyber Security …	… plus Data Protection	… plus Endpunktverwaltung	… plus Automatisierung
• EDR • Verhaltensbasierter Malware-/Virenschutz • Branchenführender Ransomware-Schutz • URL-Filterung • Backup-Scans finden und beheben Malware und Schwachstellen	• Backup: Image-basiert, Datei-basiert oder fabrikneue Wiederherstellung auf abweichender Hardware • Disaster Recovery • Unbegrenzter Storage für Backups von Google Workspace und Microsoft 365 Neu • Unveränderlicher Speicher • Agentenloses und agentenbasiertes Backup von VMs Neu • Agentenloses Backup für Azure-VMs • One-Click Recovery™ • Notarisierung und Validierung der Prüfsummenintegrität von Backups • Deduplizierung der Archive • Unveränderlicher Speicher zur Verhinderung der Korruption und Löschung von Daten • Backup-Replikation zu mehreren Standorten	• Sicherer Remote-Desktop-Zugriff und -Support Neu • Hardware- und Software-Inventarisierung Neu • Schwachstellen-Scans • Patch-Verwaltung mit ausfallsicherem Patching: Backup von Endpunkten vor der Installation von Patches • Verwaltung von Microsoft Defender und Security Essentials • Remote-Löschung von Geräten	• Automatische Erkennung von Endpunkten • Automatische Remote-Installation von Agenten • KI-gestützte Cyberskripte zur Automatisierung von Routineaufgaben Neu • Machine Learning-basierte Überwachung und Alarme für Hardware-, Software- und Netzwerk-Ressourcen Neu

Acronis Cyber Protect unterstützt die folgenden Plattformen und Applikationen

Microsoft

Azure | Windows-Server | Windows-PC | Exchange | SQL-Server | SharePoint | Active Directory | Hyper-V | Microsoft 365 | Google Workspace

Amazon EC2 | Linux-Server | Mac | iPhone | iPad | Android | SAP HANA | MariaDB | MySQL

VMware vSphere | Oracle x86 VM-Server | Oracle Database | Red Hat Virtualization | Linux KVM | Citrix XenServer | Virtuozzo | Nutanix | Synology

Umfassende, durchgängige Cyber-Resilienz für das gesamte NIST Cybersecurity Framework (CSF) 2.0

Governance				
Identifizierung	**Schutz**	**Erkennung**	**Reaktion**	**Wiederherstellung**
• Führung eines aktuellen Hardware- und Software-Inventars. • Automatische Erkennung neuer Geräte. • Erkennung von Schwachstellen mithilfe systemweiter Scans. • Überblick über den unternehmensweiten Data Protection-Status mithilfe von Data Protection-Karten. • Offline-Scans von Backups auf Malware und Schwachstellen verbessern die Leistung der Endpunkte.	• Schutz für alle Hardwareplattformen, Betriebssysteme, Applikationen, Datenbanken und Cloud-Ressourcen in Ihrem Unternehmen. • Schneller Schutz für neue Ressourcen durch automatische Remote-Installation von Agenten. • Erstellung und Anpassung von Richtlinien für die Gruppenverwaltung. • Patchen ohne Risiko durch automatisches Backup vor dem Patching, das bei Bedarf ein schnelles Rollback ermöglicht. • Unveränderlicher Speicher schützt Backups vor Verlust durch menschliches Versagen oder böswillige Angriffe.	• Erkennung unbekannter und fortschrittlicher Bedrohungen wie Ransomware durch Malware-Schutz mit Verhaltenserkennung. • Zustandsüberwachung für Hardware, Applikationen und Netzwerk-Ressourcen. • Optimale Nutzung der leistungsstarken Bedrohungserkennung durch Positivlisten für Applikationen.	• Automatische Entfernung von Ransomware-Bedrohungen und Zurücksetzen von Verschlüsselungsvorgängen aus dem lokalen Datei-Cache. • Erkennung heimlicher, permanenter Bedrohungen durch die Korrelation von Gefährdungsanzeichen über Endpunkte hinweg. • Rasche Priorisierung der Reaktionen auf Zwischenfälle. • Isolierung und Behebung von Bedrohungen. • Forensische Daten werden in Backups gesammelt, um Schwachstellen nach einem Vorfall analysieren zu können. • Automatisches Auslösen von Patches, Scans und Backups bei Eingang eines Alarms von einem Acronis Cyber Protection Operation Center.	• Schnelle und flexible Wiederherstellung nach Datenverlust. • One-Click Recovery™ ermöglicht eine lokale, benutzerinitiierte Wiederherstellung innerhalb weniger Minuten, wenn das IT-Team in der Zentrale nicht eingreifen kann. • Mit Disaster Recovery können Sie Ihre Geschäftsprozesse nach einem großflächigen Ausfall schnell wieder aufnehmen. • Backup-Scans finden und beheben Malware und Schwachstellen vor der Wiederherstellung, was ein sicheres Recovery gewährleistet.

Besondere Vorteile von Acronis Cyber Protect

Für Backup:

- **Flexible Storage-Optionen für Backups** – einschließlich lokaler Festplatten, SSDs, Bandlaufwerke, SAN, NAS, Private Cloud, Acronis Cloud und führender Public Cloud-Anbieter.
- **Image-basierte Backups und Wiederherstellung auf abweichende Hardware** ermöglichen den Schutz von Workstations und Servern mit veralteten Betriebssystemen.
- **Acronis Instant Restore ermöglicht Backups und Wiederherstellungen zwischen verschiedenen Systemtypen**. Mit dieser Funktion können ausgefallene physische Server innerhalb von Sekunden auf replizierte Standby-VMs umgeschaltet werden.
- **Acronis One-Click Recovery™** ermöglicht Benutzer:innen die Wiederherstellung eines ausgefallenen Endpunkts ohne Eingreifen der IT-Abteilung.
- **Durchsuchbare Backups von Microsoft 365 und Google Workspace** ermöglichen die Wiederherstellung einzelner Dateien, E-Mails, Chats und anderer Ressourcen, ohne dass ganze Postfächer oder Konten wiederhergestellt werden müssen.
- **Mit Acronis Cyber Protect erhalten Sie kostenlos unbegrenzten Storage für Microsoft 365- und Google Workspace-Backups** in der Acronis Cloud.

Für Cyber Security und Endpunktverwaltung

- **Ein einziger Agent auf jedem Endpunkt** für Cyber Security, Data Protection und Endpunktverwaltung verbessert die Leistung und beseitigt Konflikte zwischen verschiedenen Anbietern.
- **Eine Konsole für alle Verwaltungsaufgaben** ermöglicht einen effizienten IT-Betrieb, z. B. individuelle Schutzpläne und eine schnellere Einarbeitung neuer Techniker:innen.
- **Sicherer Remote-Desktop und -Support** ermöglichen es dem IT-Personal, Windows-, macOS- und Linux-Endpunkte aus der Ferne zu überwachen, zu konfigurieren und Fehler zu beheben.
- **Umfassende Inventarisierungstools** erkennen, verfolgen und melden automatisch alle Hardware- und Software-Ressourcen.
- **Cyber Scripting** entlastet Sie von monotonen IT-Wartungsaufgaben. Vorkonfigurierte Skripte können manuell oder mit KI-Unterstützung angepasst werden.
- **Machine Learning-basierte Überwachung und Alarme** unterstützen die IT-Abteilung bei der Vorhersage von Performance- und Verfügbarkeitsproblemen mit Ressourcen (Sicherheit, Storage, Netzwerk) von Acronis und Drittanbietern.
- **Flexible Schutzoptionen für VMs** mit agentenbasierter und agentenloser Verwaltung.

Acronis

Weitere Informationen finden Sie auf www.acronis.com.