Acronis Cyber Protect

Cyber Security, protezione dati e gestione degli endpoint integrate per le aziende

Backup automatizzato e a gestione centralizzata, disaster recovery, cyber security e altre funzioni critiche da console basata su AI.

Cyber Security...	con protezione dati...	gestione proattiva degli endpoint...	... e automazione
• EDR — ora con supporto per Linux Novità • Anti-malware e antivirus basati su comportamento • Protezione dal ransomware leader di settore • Filtraggio degli URL • Scansione e correzione dei backup alla ricerca di malware e vulnerabilità • Esportazione dei dati SIEM per una visibilità unificata della sicurezza e trail degli eventi pronti per l'audit	• Backup: ripristino basato su immagine, file o bare-metal anche su hardware diverso • Disaster recovery • Storage illimitato per i backup di Google Workspace e Microsoft 365 • Backup di Microsoft Entra ID e ripristino point-in-time • Storage immutabile • Backup di VM con e senza agente • Backup agentless per VM Azure • One-Click Recovery™ • Autenticazione e convalida dell'integrità tramite checksum dei backup • Deduplica in archivio • Storage immutabile mirato a contrastare la compromissione/eliminazione dei dati • Replica di backup su più destinazioni • Archiviazione e-mail Novità • Backup senza agente per Nutanix AHV Novità	• Desktop remoto e assistenza remota sicuri • Inventario hardware e software • Analisi delle vulnerabilità • Gestione delle patch con applicazione sicura: backup degli endpoint prima dell'installazione delle patch • Gestione di Microsoft Defender e Microsoft Security Essentials • Cancellazione dei dati di dispositivi remoti	• Rilevamento automatico degli endpoint • Installazione automatizzata degli agenti da remoto • Cyber Scripting assistito da AI per l'automazione delle attività quotidiane • Monitoraggio e avvisi basati su machine learning per risorse hardware, software e di rete • Onboarding guidato di Microsoft 365

Acronis Cyber Protect supporta le seguenti piattaforme e applicazioni

Microsoft

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

Google Workspace

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

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

Resilienza digitale completa end-to-end basata sul framework di Cyber 2.0 NIST

Gestione				
Identificazione	**Protezione**	**Rilevamento**	**Risposta**	**Ripristino**
• Mantieni un inventario aggiornato di hardware e software. • Rileva automaticamente i nuovi dispositivi. • Scansiona i sistemi per rilevare le vulnerabilità. • Un'unica vista sullo stato della protezione aziendale, grazie alle mappe di protezione dei dati. • Migliora le prestazioni degli endpoint con la scansione offline dei malware nei backup.	• Proteggi ogni piattaforma hardware, sistema operativo, applicazione, database e risorsa cloud aziendale. • Proteggi subito le nuove risorse con l'installazione automatica in remoto dell'agente. • Crea e personalizza le policy di gestione dei gruppi. • Delega l'accesso amministrativo con ruoli granulari riutilizzabili e autorizzazioni specifiche. • Applica le patch senza rischi, grazie al backup automatico dei dati effettuato prima dell'installazione, per eseguire il rollback in caso di necessità. • Usa lo storage immutabile per evitare la perdita dei backup a causa di errori umani e attacchi dannosi.	• Rileva minacce sconosciute e avanzate, come il ransomware, con un sistema anti-malware comportamentale. • Monitora l'integrità dell'hardware, delle applicazioni e delle risorse di rete. • Esporta avvisi, eventi, attività e operazioni di sicurezza nelle piattaforme SIEM per un monitoraggio unificato. • Ottimizza il rilevamento delle minacce ad alte prestazioni utilizzando la whitelist delle applicazioni.	• Arresta in automatico le minacce ransomware e ripristina le operazioni di crittografia con il rollback dal file nella cache locale. • Rileva minacce furtive e persistenti tramite la correlazione degli indicatori di compromissione su tutti gli endpoint. • Assegna rapidamente le priorità di incident response. • Usa riepiloghi delle sessioni remote generati dall'AI e consigli in tempo reale per accelerare la risoluzione dei problemi e le escalation • Isola e correggi le minacce. • Raccogli i dati forensi nei backup per analizzare le vulnerabilità dopo l'incidente. • Esegui automaticamente patch, scansione e backup all'arrivo di avvisi dai centri operativi Acronis Cyber Protection. • Semplifica l'e-Discovery e la conformità grazie all'archiviazione delle e-mail per M365.	• Recupera in modo rapido e flessibile in caso di perdita di dati. • Attiva il ripristino locale avviato dall'utente in pochi minuti con One-Click Recovery™, quando il team IT centrale non può intervenire. • Torna rapidamente in attività dopo un'interruzione di ampia portata con il disaster recovery. • Garantisci un ripristino sicuro grazie alla scansione e alla correzione dei backup per individuare malware e vulnerabilità.

Vantaggi esclusivi di Acronis Cyber Protect

Per il backup

- **Opzioni di storage dei backup flessibili**, tra cui HDD locale, SSD, nastro, SAN, NAS, cloud privato, Acronis Cloud e i principali provider di cloud pubblico.
- **Backup basati su immagine e ripristino su hardware diverso** che consentono di proteggere workstation e server legacy che eseguono sistemi operativi non più supportati.
- **Backup e ripristino tra diversi tipi di sistema,** per utilizzare Acronis Instant Restore ed eseguire il failover dei server fisici malfunzionanti in pochi secondi su VM di replica in standby.
- **Acronis One-Click Recovery** permette a qualsiasi utente di ripristinare un endpoint malfunzionante senza l'intervento dell'IT.
- **Backup di Microsoft 365 e Google Workspace indicizzabili,** per recuperare singoli file, e-mail, chat e altre risorse senza dover ripristinare intere caselle di posta o account.
- **Acronis Cyber Protect include uno storage illimitato e gratuito dei backup di** Microsoft 365 e Google Workspace in Acronis Cloud.

Per la Cyber Security e la gestione degli endpoint

- **Un singolo agente su ogni endpoint** dedicato a Cyber Security, protezione dati e gestione degli endpoint, per migliorare le prestazioni ed eliminare i conflitti tra soluzioni di diversi vendor.
- **Una sola console per tutte le funzioni di gestione,** con cui incrementare l'efficienza dell'IT, ad esempio con piani di protezione personalizzati e onboarding rapido di nuovi tecnici.
- **Desktop remoto e assistenza remota** mettono a disposizione dei team IT strumenti potenti per monitorare, configurare e risolvere a distanza i problemi degli endpoint Windows, macOS e Linux.
- **Strumenti di inventario completi** per rilevare, tenere traccia e creare automaticamente report relativi a tutte le risorse hardware e software.
- **Cyber Scripting** per semplificare le attività di manutenzione IT di routine. Script predefiniti che è possibile ottimizzare manualmente o con l'aiuto dell'AI.
- **Monitoraggio e avvisi assistiti da ML** che consentono ai team IT di anticipare problemi prestazionali e di funzionamento con risorse di sicurezza, storage e networking di Acronis e di terzi.
- **Opzioni flessibili per la protezione delle VM**, inclusa la gestione con e senza agente.

Acronis

Maggiori informazioni su acronis.com