

Acronis Cyber Protect


Acronis

Integrated cybersecurity, data protection and endpoint management for business









Centrally manage and automate EDR, anti-malware, backup and other critical functions — for endpoints, Microsoft 365 resources, servers, VMs and more — from one AI-powered console










Cybersecurity plus data protection	... plus endpoint management	... plus automation
<ul style="list-style-type: none"> • EDR • Behavioral anti-malware / AV • Industry-leading ransomware protection • URL filtering • Scanning and remediation of backups for malware and vulnerabilities 	<ul style="list-style-type: none"> • Backup: image-based, file-based or bare-metal recovery to dissimilar hardware • Disaster recovery • Unlimited storage for Google Workspace and Microsoft 365 backups New • Immutable storage • Agentless and agent-based backup of VMs New • Agentless backup for Azure VMs • One-Click Recovery™ • Notarization and checksum integrity validation of backups • In-archive deduplication • Immutable storage to thwart corruption / deletion attacks • Backup replication to multiple destinations 	<ul style="list-style-type: none"> • Secure remote desktop access and assistance New • Hardware and software inventory New • Vulnerability scanning • Patch management with fail-safe patching: backup of endpoints before installing patches • Microsoft Defender and Security Essentials management • Remote device wipe 	<ul style="list-style-type: none"> • Endpoint auto-discovery • Automated remote agent installation • AI-powered cyber scripts to automate routine tasks New • Machine learning-based monitoring and alerts for hardware, software, and network resources New

Acronis Cyber Protect supports the following platform and applications



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
---	---	--	---	--	---	--	--	---

Comprehensive, end-to-end cyber resilience across the NIST Cybersecurity Framework (CSF) 2.0

Govern				
Identify	Protect	Detect	Respond	Recover
<ul style="list-style-type: none"> • Maintain up-to-date inventory of hardware and software. • Automatically discover new devices. • Scan systems to detect vulnerabilities. • Get business-wide protection status at a glance via data protection maps. • Improve endpoint performance with offline malware and vulnerability scanning of backups. 	<ul style="list-style-type: none"> • Protect every hardware platform, OS, application, database and cloud resource across the business. • Protect new resources quickly with automated remote agent installation. • Build and customize group management policies. • Patch without risk via prepatch automatic backup that enables fast rollback if needed. • Use immutable storage to thwart the loss of backups to human error and malicious attacks. 	<ul style="list-style-type: none"> • Detect unknown and advanced threats like ransomware with behavioral anti-malware. • Monitor the health of hardware, applications, and network resources. • Optimize high-performance threat detection via application allowlists. 	<ul style="list-style-type: none"> • Automatically terminate ransomware threats and roll back encryption operations from local file cache. • Detect stealthy, persistent threats via IOC correlation across endpoints. • Rapidly prioritize incident response. • Isolate and remediate threats. • Collect forensic data in backups for post-incident vulnerability analysis. • Auto-trigger patching, scanning and backups on receipt of alerts from Acronis Cyber Protection Operations Centers. 	<ul style="list-style-type: none"> • Recover from data loss with rapid, flexible recovery. • Enable local, user-initiated recovery in minutes with One-Click Recovery™ when central IT cannot intervene. • Resume business operations quickly in the wake of a widespread outage with disaster recovery. • Ensure safe recovery with pre-restoral scanning and remediation of backups for malware and vulnerabilities.

Unique advantages of Acronis Cyber Protect

For backup

- **Flexible backup storage options** include local HDDs, SSDs, tape, SAN, NAS, private cloud, Acronis Cloud and major public cloud providers.
- **Image-based backups plus restore to dissimilar hardware** enables protection of legacy workstations and servers running sunsetted operating systems.
- **Backup and restore between different system types** enables Acronis Instant Restore, with which failed physical servers can failover in seconds to standby replica VMs.
- **Acronis One-Click Recovery** enables any user to rebuild a failed endpoint without IT intervention.
- **Searchable Microsoft 365 and Google Workspace backups** enable recovery of individual files, emails, chats and other resources without having to restore entire mailboxes or accounts.
- **Complimentary, unlimited storage of backups for Microsoft 365 and Google Workspace** in the Acronis Cloud is included in Acronis Cyber Protect.

For cybersecurity and endpoint management

- **A single agent on each endpoint** for cybersecurity, data protection and endpoint management improves performance and eliminates multivendor conflicts.
- **One console for all management functions** yields IT efficiencies like customized protection plans and faster onboarding of new technicians.
- **Secure remote desktop and assistance** gives IT staff powerful tools to remotely monitor, configure and troubleshoot Windows, macOS and Linux endpoints.
- **Comprehensive inventory tools** automatically discover, track and report all hardware and software assets.
- **Cyber Scripting** offloads rote IT maintenance tasks. Prebuilt scripts can be tuned manually or with AI help.
- **ML-powered monitoring and alerts** help IT predict performance and viability issues with Acronis and third-party security, storage and network resources.
- **Flexible VM protection options** include agent-based and agentless management.