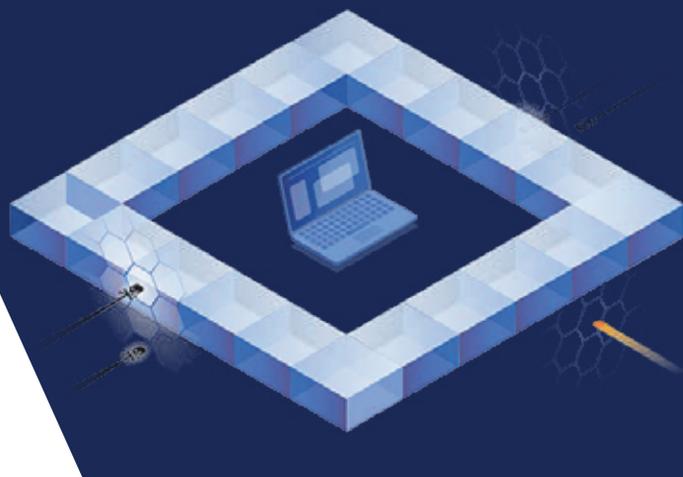


Acronis SCS

Cyber Protect Cloud for MSPs



EXPAND YOUR REACH AND GENERATE REVENUE WITH CERTIFIED PUBLIC SECTOR CYBER PROTECTION

Legacy IT systems, lack of network visibility, budget constraints, and access to sensitive constituent data make public sector organizations particularly vulnerable to cyberattacks and data loss. Managed Service Providers (MSPs) can fill these gaps—but only if they offer the right solutions at the right price. Acronis SCS Cyber Protect Cloud offers a revolutionary approach to drive operational efficiency, business differentiation, and revenue generation for MSPs.

Avoid compliance delays and generate public sector sales today with Acronis SCS Cyber Protect Cloud – our FIPS 140-2, CJIS, and HIPAA certified cloud solution run and supported in the US by 100% US citizens.

With full-stack anti-malware protection and comprehensive endpoint management, Acronis SCS Cyber Protect Cloud combats advanced cyberattacks with a unique integration of protection technologies while simplifying daily IT operations, endpoint deployments and management, and reporting. Now you can manage all cyber protection aspects from a single pane of glass.

With mix-and-match functionality, plug-and-play capability, and pay-as-you-go pricing, Acronis SCS Cyber Protect Cloud gives MSPs the flexibility to meet the unique needs facing public sector agencies and organizations.

SEIZE THE PUBLIC SECTOR OPPORTUNITY WITH CERTIFIED CYBER PROTECTION



<p>Deliver highest-grade encryption approved by the Federal Government</p>	<p>Serve criminal justice customers with ease with CJIS-compliant data security and encryption standards</p>	<p>Guarantee secure patient data with HIPAA-compliant data confidentiality and integrity standards</p>
<ul style="list-style-type: none"> ◆ Three Deployment Options ◆ Dedicated US Data Centers 	<ul style="list-style-type: none"> ◆ Multi-Tier Cloud Architecture ◆ Centralized Management 	<ul style="list-style-type: none"> ◆ Pay-as-You-Go Pricing ◆ White Glove Services

A la Carte Cyber Protection Features Management

ELIMINATE VULNERABILITIES, EXPLOITS, AND UNPREDICTABLE DATA LOSS

Ensure seamless business continuity for your clients thanks to top-level, best-in-class vulnerability assessments and patch management functionality via a single, centralized management console.

<p>Drive health monitoring</p>	<p>Get alerts about disk issues before they happen with machine learning applied to S.M.A.R.T. (Self-Monitoring, Analysis, and Reporting Technology) reports and various operating system parameters.</p>
<p>Network Optimization</p>	<p>Utilize delivery optimization to reduce bandwidth consumption by sharing the work of downloading patch update packages among multiple devices in a customer's deployment.</p>
<p>Fail-safe patching</p>	<p>Easily restore and rollback to a working state with automatic image backups and patch management support for Microsoft and third-party software on Windows.</p>
<p>Remote endpoint detection</p>	<p>Automatically detect and patch endpoints located outside of the organization's network, including remote and mobile users.</p>
<p>Inventory management</p>	<p>Discover and manage all software/hardware assets installed on customer machines through automatic or on-demand scans, and auto-delete records once a machine or tenant is removed.</p>
<p>Vulnerability and exploit prevention</p>	<p>Identify and remediate vulnerabilities and exploits with real-time vulnerability assessments, return-oriented programming protection, code injection protection, and privilege escalation protection.</p>

Data Protection

ENSURE CRITICAL DATA IS PROTECTED AND COMPLIANCE IS MAINTAINED AT ALL TIMES

Every system, all workloads, any format— you can deliver the continuous and comprehensive data protection public sector agencies and organizations require.

Better protection, fewer resources	Offload and enable more aggressive scans and vulnerability assessments in central storage, including cloud.
Data protection mapping	Ensure critical data is protected, get detailed information about stored data, and use automatic data classification to track the protection status of mission-critical or highly sensitive files.
Built-in forensic backup	Simplify future analysis by collecting digital evidence—like memory dumps and process information—from disk-level backups.
Network and content control	With advanced URL filtering, control website access through a HTTP/HTTPS interceptor, black and whitelists for URLs, and payload analysis for malicious URLs.
Remote wipe capabilities	Prevent data from being deleted, stolen, or distributed by ex-employees or accessed from lost or stolen devices with built-in remote wipe capabilities of any compromised or missing devices.
Global and local whitelisting	Support more aggressive heuristics by preventing false detections.

Cybersecurity

ADVANCED AI-BASED BEHAVIORAL DETECTION ENGINE FOR ZERO-DAY ATTACK PREVENTION

One integrated solution that delivers complete protection from today's threats—enabling you to streamline management, cut unnecessary administrative time, and lower TCO.

Leading-edge protection	Provide confidence and peace of mind with built-in, AI-based static and behavioral heuristic anti-virus, anti-malware, anti-ransomware, and anti-cryptojacking technologies.
Global threat monitoring	Take a more proactive security posture with real-time alerts on malware, vulnerabilities, and other global events that may affect data protection.
Remote workforce security	Proactively protect remote collaboration tools like WebEX, Zoom, and Microsoft Teams with vulnerability assessment, patch management, code injection prevention, and anti-malware capabilities.
Email security	Advanced email security features, including anti-spam, anti-phishing, and attachment scanning, mitigate email vulnerabilities and external attack vectors.
CyberFit Scoring	Identify security gaps and open attack vectors to endpoints and provide recommended actions for improvements with an in-depth #CyberFit report.

Backup & Recovery

BACKUP-AS-A-SERVICE SOLUTION FOR ANY WORKLOAD IN ANY ENVIRONMENT

Combining backup-as-a-service with AI-based anti-ransomware technologies and end-to-end encryption, you can offer robust data protection with secure backup and recovery to meet the needs of sensitive public sector clients.

Hybrid cloud backup and recovery	A seamless hybrid experience ensures ultimate data safety and accessibility by backing up and recovering customers' systems, applications, and data via both local and cloud storage.
Built-in real-time protection	Stop ransomware with advanced, AI-based anti-ransomware technology, which protects files, backups, and the backup agents in real-time.
Protection for any workload	A single solution supports 20+ platforms, including Windows and Linux servers and VMs, eight major hypervisors, PCs, Macs, iOS and Android mobile devices, Microsoft on-premises apps, SAP HANA, Microsoft 365, and G Suite.
Disaster recovery orchestration	Automate critical disaster recovery scenarios and ensure your systems recover in the correct order to address interdependencies between applications.
Easy, scalable management	Simplify orchestration using the web-based multi-tenant management console—a single spot for accounts provisioning, user and reseller management, reporting, monitoring, and other tasks.
Pay-as-you-go-pricing	Pay only for the servers you are protecting based on your actual usage. There are no charges for compute resources if the recovery server is not running.

File Sync & Share

FILE SYNC AND SHARE WITH UNCOMPROMISED SECURITY AND FLEXIBLE STORAGE

Easy to implement, quick to deploy, and affordable to scale, file sync and share features are designed to help MSPs attract new clients, discover incremental revenue, and reduce client churn.

Secure access from any device	Empower users to securely create, edit, and share content using their own smartphones, tablets, PCs, Macs, or web-enabled devices.
Rich mobile experience	Ensure the productivity of mobile users with complete support of Microsoft Office mobile apps, as well as convenient PDF editing and annotation.
Comprehensive privacy and control	Supports complete end-to-end encryption, enterprise-class audit trails, and sophisticated policy controls for content, users, and devices.
Complete file transparency	Comprehensive security and privacy with FIPS 140-2 encryption, control over files and folders, as well as policy controls for users, applications, and data
Easy and secure collaboration	Easy, remote collaboration for internal and external stakeholders, a simple user experience, and comprehensive security and compliance.
Quick to deploy, easy to scale	Easy-to-use interface with no training required, enabling you to expand your product portfolio and generate new revenue streams.