

Acronis Cyber Protect Cloud vs. SentinelOne

PRODUCTS COMPARED

ACRONIS	SentinelOne
Acronis Cyber Protect Cloud 9.0 (part of Acronis Cyber Cloud)	SentinelOne Singularity Complete Platform

SOLUTION INTRODUCTIONS

SentinelOne is focused mainly on enterprises and pays little attention to service providers. It offers an endpoint protection solution that lacks critical MSP-related features and some important security capabilities. The product has two editions: Core, which offers basic detection/threat hunting and suite features, and Complete, which offers advanced detection/threat hunting and suite features.

Acronis Cyber Protect Cloud is a part of the powerful **Acronis Cyber Cloud** platform, designed exclusively for service providers. With Acronis Cyber Protect Cloud, partners can count on a complete cyber protection solution, which offers backup, anti-malware, security, and management functions all through a single agent. Its integration of data protection and cybersecurity delivers unique capabilities, better performance, compatibility, and the shortest recovery times – plus, multi-layered anti-malware technology minimizes the need for recovery.

HIGH-LEVEL COMPARISON

SENTINELONE PAIN POINTS	ACRONIS CYBER PROTECT CLOUD ADVANTAGES
<p>Not an MSP-ready solution</p> <p>SentinelOne offers almost no service provider-oriented capabilities like integration with RMM and PSA tools, reseller management, pay-as-you-go pricing, white-labeling options, easy up-sell/cross-sell to different solutions, pay-as-you-go pricing, etc., impacting business profitability, productivity, and operational efficiency.</p>	<p>A solution made specifically for MSPs</p> <p>Part of the powerful Acronis Cyber Cloud platform, Acronis Cyber Protect Cloud is designed with a service provider's technical and business needs in mind. Unlike SentinelOne it offers:</p> <ul style="list-style-type: none"> ✓ Simple integrations with RMM and PSA tools ✓ A suite of services via a single portal, enabling easy up-sell/cross-sell to backup, disaster recovery, file sync and share, notarization, and eSignature services ✓ Reseller management functionality that lets MSPs turn themselves into value-added resellers and sell beyond the end-customer market ✓ Straightforward pay-as-you-go pricing ✓ White-labeling options and portal branding support that enable MSPs to customize the solution and differentiate themselves ✓ Software in 25 languages, with user-based language settings and easy switching between them ✓ Unified portal for all workloads

<p>No efficient tools to recover from cyberattacks</p> <p>When malware attacks service providers and their clients are exposed to backup deletion and data loss – SentinelOne has no backup-defense functionality, nor data protection, and relies on VSS (Volume Shadow Copy Service) copies, available in Microsoft's Windows Operating Systems only.</p>	<p>Safe, fast, easy recoveries</p> <p>Acronis Cyber Protect Cloud lets you save time and energy, equipping you with the tools needed to avoid cyberthreats outright – and quickly and easily recover from any data loss event. It has a robust safe recovery feature built in, so you can prevent dangerous infections from recurring. During the recovery process, the solution delivers integrated anti-malware backup scans, installs the latest security patches, and updates anti-virus databases.</p>
<p>Expensive, unsecure VSS snapshots to recover from a ransomware attack</p> <p>SentinelOne has the ability to restore files that have been maliciously encrypted or deleted to their previous state via the VSS (Volume Shadow Copy Service) feature, available only in Windows environments.</p> <p>Although the VSS snapshots provide the complete data set and are application consistent, they are rather expensive, plus the whole system activity is frozen when VSS snapshots are acquired.</p> <p>Moreover, more advanced ransomware families target shadow copies created via VSS, to prevent recovery.</p>	<p>Affordable auto-recovery from a ransomware attack</p> <p>With Acronis Cyber Protect Cloud, you can rely on technology that is more affordable, less intrusive, more lightweight, granular from the start, and better performing. The built-in Acronis Active Protection technology:</p> <ul style="list-style-type: none"> ✓ Monitors your system in real time, examining the process stack to identify activities that exhibit behavior patterns that are typically seen in ransomware and cryptojacking attacks ✓ Stops any process that tries to encrypt your data or inject malicious code and instantly notifies you when something suspicious is found, enabling you to choose whether to block the activity or allow it to continue ✓ Restores files from the backup cache automatically should they have been altered or encrypted before an attack is stopped
<p>No integrated patch management</p> <p>SentinelOne doesn't have integrated patch management, only vulnerability assessments. This means service providers lack insight into any new vulnerabilities without hotfixes, thereby limiting risk visibility.</p> <p>The patch management functionality comes at additional cost via partnership with Automox.</p>	<p>Integrated vulnerability assessments and patch management</p> <p>Acronis Cyber Protect Cloud has built-in vulnerability assessment and patch management capabilities that mitigate risks from upcoming or existing threats: Acronis Cyber Protection Operation Centers (CPOCs) monitor the cybersecurity landscape and release alerts. In turn, Acronis CPOCs adjust protection plans, issuing more frequent backups, deeper anti-virus scans, specific patch installs, etc. Meanwhile, automated backups occur before new patches are installed, ensuring a quick rollback option.</p> <p>As a result, service providers can:</p> <ul style="list-style-type: none"> ✓ Streamline daily administrative tasks ✓ Minimize business downtime when facing issues like a malware epidemic, natural disaster, etc. ✓ Reduce reaction times ✓ Avoid data loss

No remote deployment and management capabilities

SentinelOne doesn't provide any capabilities for remote deployment or management of endpoints, greatly increasing service providers' administrative efforts.

Remote deployment, assistance, and client management

Acronis Cyber Protect Cloud allows for easy remote deployment with automatic machine discovery and remote agent installation capabilities.

With an embedded remote desktop client (readily available via the management console), Acronis Cyber Protect Cloud ensures service providers save time and money while helping clients. Without any additional software required, administrators can reach systems that are located in a private network with:

- ✓ No need to change firewall settings nor establish additional VPN tunnels
- ✓ No need to open new incoming ports - the remote desktop itself creates a secure tunnel between the administrator and endpoint stations, based on existing outgoing connections

FEATURE-BY-FEATURE COMPARISON

	SENTINELONE SINGULARITY COMPLETE	ACRONIS CYBER PROTECT CLOUD
DEPLOYMENT OPTIONS		
Vendor's cloud (SaaS)	✓	✓
On-premises (software)	✓	✓
FEATURES FOR SERVICE PROVIDERS		
Integration with RMM and PSA tools	X	Autotask, ConnectWise (Automate, Manage, Control), Kaseya, Atera
Multi-tenant management portal	✓	✓
A platform for multi-service management (security, backup, disaster recovery, file sync and share, notarization, and eSignature services)	X	✓
Pay-as-you-go pricing	X	✓
White-labeling	X	✓
Portal branding support	X	✓
API for custom integrations	✓	✓
Reseller management	X	✓
Supported languages	English only	25 languages
SUPPORTED OPERATING SYSTEMS		
Windows	✓	✓
Mac	✓	✓
Linux	✓	✓
SUPPORTED MOBILE DEVICES		
Android	✓	X
iOS	✓	X
ANTI-MALWARE FEATURES		
Real-time anti-malware and anti-ransomware protection	✓	✓
On-demand scanning and malware removal	✓	✓
Pre-execution AI-based analyzer	✓	✓
Exploit prevention	✓	✓
Behavioral analysis and dynamic detection rules	✓	✓
Protection against zero-day attacks	✓	✓
Disk and master boot record protection	✓	✓
Real-time malicious cryptominer protection	✓	✓
Automatic file recovery after a ransomware attack	Limited via VSS snapshots, Windows only	✓
Single-click to remove malicious files	✓	X
Self-protection	✓	✓
Malware scanning of backups	X	✓
Anti-virus updates of OS images before recovery	X	✓
Installation of the latest security patches before recovery	X	✓
Email security	X	Planned (Q2, 2021)
Firewall	✓	Planned (Q1, 2021)
IPS/HIPS	✓	X

	SENTINELONE ENDPOINT PROTECTION CORE	ACRONIS CYBER PROTECT CLOUD
OTHER CYBER PROTECTION FEATURES		
Vulnerability assessments of systems	✓	✓
Patch management	X Available through partnership with Automox	✓
Automatic backups of endpoints before patching	X	✓
Data protection maps	X	✓
Compliance reporting	X	✓
URL filtering	X	✓
Forensic investigations	✓	✓
Device wipe	X	✓
Memory protection (e.g. Stack Pivot, Import Address Table Filtering)	✓	✓
Script management	✓	Limited
Ability to manage Microsoft Windows Defender	X	✓
Two-factor authentication	✓	✓
Data loss prevention	X	Planned (Q3, 2021)
Endpoint detection and response (EDR)	✓	Planned (Q4, 2021)
Device control	✓	Planned (Q1, 2021)
Application control	X	Planned (Q1, 2021)
MANAGEMENT		
Unified portal for all workloads	✓	✓
Unified policies for cybersecurity and backup	X	✓
Auto-discovery of machines	X	✓
Remote agent installation	X	✓
Remote access to machines via integrated RDP	X	✓
Hard drive health monitoring	X	✓