

Acronis Cyber Protect Cloud vs. BlackBerry Cylance

PRODUCTS COMPARED

ACRONIS	BLACKBERRY CYLANCE
Acronis Cyber Protect Cloud 9.0 (part of Acronis Cyber Cloud)	CylancePROTECT v1560

SOLUTION INTRODUCTIONS

BlackBerry Cylance offers a cloud-based endpoint protection solution but it lacks critical security and MSP-related features. In February 2019, Cylance was acquired by Blackberry, meaning that the new ownership may impact the company's market position and ability to deliver required product updates and functionality.

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 that offers backup, anti-malware, security, and management functions all in 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

BLACKBERRY CYLANCE PAIN POINTS	ACRONIS CYBER PROTECT CLOUD ADVANTAGES
<p>Missing protection capabilities and high false alarm rate</p> <p>With BlackBerry Cylance, service providers are at high risk of being infected and compromised by malware because the solution lacks critical security features like behavioral analysis, vulnerability assessments, patch management, URL filtering, etc.</p> <p>In fact, according to third-party tests, BlackBerry Cylance has a high false positive detection rate, which may absorb the administrator's time.</p>	<p>The most advanced AI-based protection with top detection rates</p> <p>Acronis' approach delivers next-generation full-stack, AI/ML-powered protection against malware.</p> <p>Acronis Cyber Protect Cloud offers:</p> <ul style="list-style-type: none"> ✓ Proven, 100% detection rate and no false alarms ✓ Built-in AI-based protection against any type of malware ✓ The most advanced anti-ransomware technology – it is proactive, AI-based, and automatically recovers files ✓ A hardened agent for better self-protection against ransomware and malware – of both Acronis' software and customer backups ✓ Anti-malware scans of production systems and backups ✓ Vulnerability assessments of production systems ✓ Automatic endpoint backups before patching ✓ URL filtering ✓ Data protection maps and compliance reporting ✓ Unified protection plan for cybersecurity and backup

<p>Not an MSP-ready solution</p> <p>BlackBerry Cylance offers almost no service provider-oriented capabilities like reseller management, easy up-sell/cross-sell to different solutions, white-labeling, 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 BlackBerry Cylance it offers:</p> <ul style="list-style-type: none"> ✓ Simple integrations with more RMM and PSA tools – BlackBerry Cylance integrates only with ConnectWise Automate, while Acronis does with many more: Autotask, ConnectWise (Manage, Control), Kaseya, and Atera ✓ 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 ✓ White-labeling options and portal branding support that let service providers customize the solution and differentiate themselves ✓ Software in 25 languages, with user-based language settings and easy switching between them
<p>No tools to recover from cyberattacks</p> <p>When malware strikes service providers and their clients are exposed to backup deletion and data loss – BlackBerry Cylance has no backup-defense functionality and data protection.</p>	<p>Safe, fast, easy recoveries</p> <p>Acronis Cyber Protect Cloud lets you save time and energy equipped 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 reoccurring, without lifting a finger. During the recovery process, the solution delivers integrated anti-malware backup scans, installs the latest security patches, and updates anti-virus databases.</p>
<p>No vulnerability assessments and patch management</p> <p>BlackBerry Cylance doesn't have vulnerability assessment and patch management functionalities. This means service providers lack insight into any new vulnerabilities without hotfixes, thereby limiting risk visibility. To overcome this gap, service providers need to license another solution.</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 today's surge in cybercrimes, unpredictable natural disasters, etc. ✓ Reduce reaction times ✓ Avoid data loss

<p>No tool for forensic investigations</p> <p>In the event of a cyberattack, BlackBerry Cylance cannot help you investigate what happened. You need to license CylanceOPTICS in order to access this support.</p> <p>Without ready-visibility into the problem, it takes longer to identify where an attack came from and what specifically caused it.</p>	<p>Ready-access to revealing forensic data</p> <p>Acronis Cyber Protect Cloud helps you investigate and analyze an incident immediately with forensic backup capabilities already integrated. Acronis Cyber Protect Cloud can also record full memory dumps, so all insights are incorporated into its own backups. Alerts further help pinpoint the name of the file that contained the malware as well as its location.</p> <p>The built-in forensic data backup feature:</p> <ul style="list-style-type: none"> ✔ Keeps key digital evidence secure in the backup ✔ Makes conducting future investigations easier and less costly
<p>No remote desktop access capabilities</p> <p>BlackBerry Cylance doesn't have an integrated remote desktop functionality. A separate product is needed.</p>	<p>Remote assistance and client management</p> <p>With an embedded remote desktop client (readily available via the management console), Acronis Cyber Protect Cloud ensures users save time and money while helping clients. Without any additional software required, administrators can reach systems that are located in a private network with:</p> <ul style="list-style-type: none"> ✔ 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

	CylancePROTECT	ACRONIS CYBER PROTECT CLOUD
DEPLOYMENT OPTIONS		
Vendor's cloud (SaaS)	✓	✓
On-premises (software)	X Available in CylanceON-PREM	✓
FEATURES FOR SERVICE PROVIDERS		
Integration with RMM and PSA tools	ConnectWise Automate	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	✓	✓
White-labeling options and 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	Limited	X
ANTI-MALWARE FEATURES		
Real-time anti-malware and anti-ransomware protection	✓	✓
On-demand scanning and malware removal	✓	✓
Pre-execution AI-based analyzer	✓	✓
Behavioral analysis and dynamic detection rules	Limited	✓
Protection against zero-day attacks	✓	✓
Disk and master boot record protection	X	✓
Real-time malicious cryptominer protection	Limited	✓
Automatic file recovery after a ransomware attack	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	Add-on	Planned (Q3)
Firewall	X	Planned (Q3)
IPS/HIPS	✓	X

	CylancePROTECT	ACRONIS CYBER PROTECT CLOUD
OTHER CYBER PROTECTION FEATURES		
Vulnerability assessments of systems	X	✓
Patch management	X	✓
Automatic backups of endpoints before patching	X	✓
Data protection maps	X	✓
Compliance reporting	X	✓
URL filtering	Limited on Android only	✓
Device wipe	X	✓
Memory protection (e.g. Stack Pivot, Import Address Table Filtering)	✓	Planned (Q3)
Script management	✓	Limited
Ability to manage Microsoft Windows Defender	X	✓
Two-factor authentication	✓	✓
Data Loss Prevention	X	Planned (Q3)
Endpoint Detection and Response (EDR)	X Available in CylanceOPTICS	Planned (Q4)
Device control	✓	Planned (Q4)
Application control	✓	Planned (Q4)
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	✓