Acronis Cyber Protect Cloud vs. F-Secure

PRODUCTS COMPARED

ACRONIS	F-SECURE
Acronis Cyber Protect Cloud 9.0 (part of Acronis Cyber Cloud)	F-Secure Protection Service for Business (as of May 2020)

SOLUTION INTRODUCTIONS

F-Secure offers a cloud-based endpoint protection solution but it lacks critical security and MSP-related features. In order to receive full-stack protection you need to pay more to license multiple solutions. In general, F-Secure has an overly complicated product line that consists of many non-flexible solutions. Moreover, if there is no internet connection or if it is disrupted, F-Secure can't benefit from their cloud backend solution and loses some of its protection 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 that offers backup, anti-malware, security, and management functions all in a single agent. 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 itself.

HIGH-LEVEL COMPARISON

F-SECURE PAIN POINTS	ACRONIS CYBER PROTECT CLOUD ADVANTAGES
Not an MSP-ready solution F-Secure offers almost no service provider-oriented capabilities like reseller management, easy up-sell/cross-sell to different solutions, pay-as-you-go pricing, etc., impacting business profitability, productivity, and operational efficiency.	**A solution made specifically for MSPs** 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 F-Secure it offers: ✔ 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, which lets MSPs turn themselves into value-added resellers and sell beyond the end-customer market ✔ Pay-as-you-go pricing ✔ Customizable dashboard widgets and unified reporting ✔ One protection agent, which has low-performance impact
No tools to recover from cyberattacks When malware strikes service providers and their clients are exposed to backup deletion and data loss – F-Secure has no backup-defense functionality and data protection. (For additional data protection capabilities, Data Guard module, available in the Premium edition has to be licensed separately)	**Safe, fast, easy recoveries** 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.

No vulnerability assessments F-Secure doesn't offer vulnerability assessments, only 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 (F-Secure Radar).	**Integrated vulnerability assessments and patch management** Acronis Cyber Protect Cloud has built-in vulnerability assessments 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. As a result, service providers can: ✔ 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
No tool for forensic investigations In the event of a cyberattack, F-Secure cannot help you investigate what happened. You need to license F-Secure Rapid Detection & Response in order to access this support. Without ready-visibility into the problem, it takes longer to identify where an attack came from and what specifically caused it.	**Ready-access to revealing forensic data** 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. The built-in forensic data backup feature: ✔ Keeps key digital evidence secure in the backup ✔ Makes conducting future investigations easier and less costly
No ability to automatically recover from a cyberattack F-Secure doesn't support automatic file restore if ransomware manages to get through its defense, leading to data and financial losses. To overcome this gap, service providers need to license the premium solution with the Data Guard module.	**Auto-recovery from a ransomware attack** With Acronis Cyber Protect Cloud you can rely on technology that: ✔ Monitors your system in real time, examining the process stack to identify activities that exhibit behavior patterns 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 if they were altered or encrypted before an attack is stopped

No remote desktop access capabilities F-Secure doesn't have an integrated remote desktop functionality. A separate product is needed.	**Remote assistance and client management** 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: ✔ 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

	F-SECURE PROTECTION SERVICE FOR BUSINESS	ACRONIS CYBER PROTECT CLOUD
DEPLOYMENT OPTIONS		
Vendor's cloud (SaaS)	✓	✓
On-premises (software)	X Available in F-Secure Endpoint Security Suite	✓
FEATURES FOR SERVICE PROVIDERS		
Integration with RMM and PSA tools	Kaseya, SolarWinds MSP, Datto RMM	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	✓	✓
API for custom integrations	✓	✓
Reseller management	X	✓
Supported languages	27 languages	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	✓	✓
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 DataGuard module needs to be licensed	✓
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	✓
Prevents attacks and exfiltration of data from web activities that utilize HTTPS (intranets, CRMs, etc.)	✓	X
Email security	✓	Planned (Q3)
Firewall	✓	Planned (Q3)
IPS/HIPS	✓	X

	F-SECURE PROTECTION SERVICE FOR BUSINESS	ACRONIS CYBER PROTECT CLOUD
OTHER CYBER PROTECTION FEATURES		
Vulnerability assessments of systems	X	✓
Patch management	✓	✓
Automatic backups of endpoints before patching	X	✓
Data protection maps	X	✓
Compliance reporting	X	✓
URL filtering	✓	✓
Ability to manage Microsoft Windows Defender	X	✓
Two-factor authentication	✓	✓
Data Loss Prevention	X	Planned (Q3)
Endpoint Detection & Response (EDR)	X	Planned (Q4)
Device control	✓	Planned (Q4)
Application control	Limited Available in the Premium version	Planned (Q4)
Mobile VPN	✓	X
Integrity checking for Linux servers	✓	X
MANAGEMENT		
Unified portal for all workloads	✓	✓
Unified policies for cybersecurity and backup	X	✓
Auto-discovery of machines	X	✓
Remote agent installation	✓	✓
Remote access to machines via integrated RDP	X	✓
Hard drive health monitoring	X	✓