Acronis Protected Workspace: Securing the weakest link

Laptops, desktops and workstations are all essential tools and enormous security risks. Employees use them everywhere, which opens them to a wide range of threats.

For managed service providers (MSPs), devices are both the most critical and the most vulnerable assets to protect. But securing them isn't easy because MSPs often use multiple tools to protect devices. And when those tools aren't natively integrated, getting them to work together can be difficult and leave gaps in coverage.

Moreover, managing multiple tools means dealing with disparate interfaces, which increases complexity, introduces risk and often requires specialized expertise. Ultimately, workspace security infrastructures cobbled together with multiple tools increase operational costs, create inefficiencies and diminish overall protection.

With cybercriminals weaponizing AI to create nearly endless attack variants, every day is now a zero day. The stakes are high: Successful attacks lead to downtime, lost productivity and reputational damage for both MSPs and their clients, not to mention creating compliance issues in many industries.

Natively integrated security, data protection and endpoint management for workspaces

The business challenges of protecting workspaces for MSPs

Many organizations don't have the resources to manage workspace security, so they turn to MSPs for help. They need service providers to secure every laptop and desktop everywhere in a way that protects data without sacrificing productivity.

The pace and global nature of business operations make that task difficult for service providers. Part of the problem is scale. Hundreds or thousands of devices create a vast attack surface for MSPs to protect. A single compromised endpoint can lead to a cyberattack that brings client operations to a standstill.

Clients also frequently have employees using devices at a variety of locations and sending data around the globe. Remote work adds to the challenge of protecting workspaces. Device mobility, global operations and expectations of rapid responses leave employees' devices wide open for cyberattacks. And in industries like health care and finance, poorly secured workspaces can put regulatory compliance at risk.

The challenge of workspace security for MSPs

Protecting workspaces is particularly challenging for MSPs because cybersecurity tools for keeping devices safe don't deliver the efficiency service providers need. Fragmented tools with antivirus in one application, backup in another and remote monitoring and management (RMM) in yet another make workspace protection expensive and error prone.

Every element of protection requires a unique app and configuration; the number of combinations across devices is effectively limitless. And MSPs must have people to run them all. They either must hire multiple technicians or take time to train technicians to use many disconnected applications and hope they get everything right.

Managing different tools in multiple consoles leads to slow response times as well as technician burnout and errors. It also leaves open the risk of broken integrations that can create huge security holes.

Workspaces are rarely "off," making them a constant target for cyberattacks. Plus, clients' employees often trust their devices too much, creating an additional layer of vulnerability. MSPs need a solution for workspace protection that provides comprehensive security capabilities but, critically, is also easy to manage.

> "A disjointed workspace security infrastructure in many organizations has resulted in increased operational costs and complexity and lower security effectiveness."
>
> **Gartner, 2025 Strategic Roadmap for Workplace Security**

Acronis Protected Workspace delivers services tailored to MSPs

Acronis Protected Workspace includes a series of natively integrated services that enables MSPs to protect clients' devices with minimal risk and maximum efficiency. They are available per workload or per gigabyte and include:

Services in Acronis Protected Workspace

Acronis Backup for Workstations	Stores and safeguards data for client laptops, desktops and workstations.
Acronis Advanced Backup for Workstations	Extends cloud backup capabilities to proactively protect clients' workspace data for more than 20 types of workloads, virtually eliminating downtime.
Acronis Endpoint Detection and Response (EDR)	Actively monitors endpoints, stopping attacks before they can do damage and enabling single-click recovery.
Acronis Extended Detection and Response (XDR)	Delivers complete, active protection built to swiftly prevent, detect, analyze, respond to and recover from incidents.
Acronis Remote Monitoring and Management (RMM)	Superior administration and monitoring services, with a security-first approach. Automate everything and accelerate with AI and ML coupled with a powerful scripting engine. Discover and protect connected workspaces with Device Sense.™
Acronis Data Loss Prevention (DLP)	Prevents data leaks from endpoints without requiring complex installation or privacy expertise.
Acronis Active Protection	Actively protects all of the data on clients' systems, including documents, media files, programs and more.
Acronis anti-malware	Proactively protects clients' systems from advanced cyberattacks in real-time with AI-based static and behavioral heuristic antivirus, anti-malware and anti-ransomware technologies.

MSPs also have the option of choosing solution-based packages, including:

Workstation Backup	Endpoint Security + RMM	Ultimate Protection
Acronis Backup for workstations with 300GB of storage included	Acronis Active Protection	Security + RMM package
	Acronis anti-malware	Backup + Cloud storage package
	Acronis EDR	Acronis Advanced Backup
	Acronis XDR	Acronis DLP
	Acronis RMM	

The power of natively integrated workspace protection

MSPs need a unified, efficient and profitable way to protect, manage and recover workspaces. Acronis Protected Workspace delivers all the services MSPs need for workspace protection into a single, natively integrated solution: one agent, one license and one console to manage everything. It's a simple but powerful idea that enables technicians to manage more workspaces with better security.

Acronis Protected Workspace also delivers:

- **Native integration** with endpoint security, RMM and backup in one console.
- **End-to-end protection:** AI-enabled anti-malware, endpoint detection and response (EDR), extended detection and response (XDR), ransomware detection and behavioral analysis aligned with the NIST Cybersecurity Framework.
- **Operational efficiency:** Faster ticket resolution, better client service and lower training costs.
- **Flexibility:** MSP-friendly licensing models with the ability to build custom protection packages.

"Acronis as our core platform covers everything. The efficiency it brings is unmatched, saving us time, reducing costs and minimizing training efforts. Having everything in a single console makes managing our stack seamless and streamlined."

– Joshua Aaronson, Co-founder, Panda Technology

Acronis Protected Workspace delivers what MSPs need to secure devices

With Acronis Protected Workspace, MSPs can meet the challenges of securing laptops, desktops and workstations without struggling to manage disparate security applications. Service providers can set themselves apart from the competition with better protection, faster response times and superior client service.

See Acronis Protected Workspace in action CONTACT US

Acronis

Learn more at
www.acronis.com