Security is complicated: How modern MSPs turn chaos into opportunity

Here's a question. How many tools does it take to secure a network?

When you add everything up, a comprehensive approach requires a minimum of 15 different MSP tools:

Remote Monitoring and Management (RMM)	Ticketing System	Backup/Disaster Recovery (DR)
Continuity	Antivirus (AV)	Help Desk
Advanced Endpoint Protection	Sandboxing	Data Loss Prevention (DLP)/Continuous Data Protection (CDP)
Unified Threat Management (UTM)	Vulnerability Scanning	Patch Management
End-user Security Training	Incident Detection and Response	Security Information and Event Management (SIEM)

New requirements for the MSP stack

Yesterday's managed services provider (MSP) had a typical stack at the core of their managed services offering. The main goal was uptime and reliability. This stack consisted of RMM, professional services automation (PSA), AV, backup and DR, network operations center (NOC), and help desk. Some MSPs now include a managed security services provider (MSSP) stack that consists of eight to 10 more solutions – including advanced endpoint protection, advanced email filtering, DLP/CDP,

vulnerability scanning, SIEM, incident response and remediation, and security awareness training for the end-user.

For an MSP, that means 10 to 20 different vendors, software, and dashboards to manage, none of which are designed to work together. MSPs have to train their techs, manage their vendors, and just hope that nothing falls through the cracks that would put their clients at risk.

Many in the channel simply aren't experts in the MSSP stack ... and that's ok. We can't be experts in everything. But how does a modern MSP deliver security and protection when they are the only things that matter?

What MSPs should consider

If I were an MSP today, I would not sell the stack mentioned above. Instead, I'd sell the protection outcome – the idea that, for a monthly fee, I will deliver five vectors of cyber protection to ensure that your data is safe, accessible, private, authentic, and secure so your organization can keep running.

The conversation is shifting away from "which tool is better" to "what is the best way for me to safeguard client data". We can agree that the only real MSP deliverable today is the outcome – protection. To deliver effective protection in today's environment, we must implement modern processes and tools that ensure comprehensive security. And the research backs up that opinion.

We can also agree that there is no silver bullet when it comes to protecting data; no one tool that will give us 100% protection at all times. But Acronis comes close.

Cyber protection designed for MSPs

Acronis Cyber Protect Cloud is a comprehensive protection solution that covers you from end-to-end. With Acronis Cyber Protect Cloud, you get a unique integration of backup and recovery, real-time antimalware protection, and endpoint management. It creates regular, reliable backups automatically and securely stores them so they're available wherever and whenever.

The integrated design is aimed at helping both MSPs and their clients win. For businesses, Acronis Cyber Protect Cloud improves downtime prevention and accelerates remediation. For service providers, it enhances their security offering and eliminates the complexity of using multiple solutions. As a result, they can expect improved profitability, easier SLA compliance, and greater cost control.

MSPs that already offer Acronis appreciate the platform's easy integrations with RMM/PSA tools, efficient consumption-based billing, comprehensive white labelling, and seamless scalability to deliver the outcomes their clients demand – complete cyber protection.