Acronis

WHITE PAPER

MSP integration trends 2025

The shift to security-first operations

Table of contents

Executive summary 3

Acronis works the way you work 3

Trend 1: Security integration takes the lead 4

Why security integration matters now

XDR and MDR lead the way

The shift from monitoring to protection

Trend 2: Automation evolves beyond MSP-specific tools 6

Natively integrated workflow automation gains momentum

What this means for your MSP operations

Trend 3: The platform consolidation paradox 7

Why platformization matters

Why third-party integrations matter

The emerging pattern

Three strategic integration priorities for 2026 8

1. Make security integrations your competitive differentiator

2. Automate your entire business, not just IT operations

3. Expand visibility into client attack surfaces

The bottom line: Integration as strategy 9

About Acronis Cyber Protect Cloud 9

About Acronis 10

Executive summary

Your clients' technology environments are more complex than ever. The question isn't whether to integrate your tools; it's which integrations will drive the most productivity and value for your business in 2026 and beyond.

2025 marked a fundamental shift in how MSPs build their technology stacks. While traditional RMM and PSA integrations remain foundational, a new priority has emerged: **security integrations are now the fastest-growing category**, outpacing management tools by a wide margin. This trend reflects the reality MSPs face daily of escalating cyberthreats, mounting compliance requirements and clients who demand comprehensive protection, not just IT management.

The data reveals a clear story: MSPs are moving beyond tool sprawl toward strategic integration. Whether through native capabilities built directly into your platform or third-party connections with your existing tools, the goal remains delivering seamless, efficient service at scale.

This report examines the integration trends shaping MSP operations today and offers three strategic priorities for the year ahead.

Acronis works the way you work

MSPs typically manage 20+ tools across their operations. The challenge isn't the number – it's making them work together efficiently. Integration is what transforms a collection of tools into a cohesive service delivery engine.

With Acronis, there are two approaches to integration, and both matter:

- **Natively integrated** means capabilities built directly into the Acronis platform, managed by Acronis, working seamlessly together without additional setup. For example, when RMM, backup and XDR capabilities exist within the same console, technicians can respond to threats without switching contexts or losing critical time.
- **Third-party integration** connects your existing tools with new capabilities through APIs and connectors. If you've already invested in a particular RMM or PSA, integration lets you add advanced security and data protection without replacing your entire stack.

The key insight from 2025: **successful MSPs don't choose one approach over the other; they leverage both strategically**. Acronis' native integrations reduce complexity and accelerate response times. Integrations with third-party tools preserve existing investments and add specialized capabilities.

The goal remains constant: deliver comprehensive protection efficiently, regardless of the technical path.

Security integration takes the lead

The most significant shift in 2025 was unmistakable: security integrations emerged as the fastest-growing category, far outpacing traditional management tools.

This wasn't a modest uptick; security integration adoption more than doubled in growth (123%), while RMM and PSA integrations remained relatively flat in comparison.

Rank	Integration category	Activation growth
01	Security	123%
02	Data protection	99%
03	Management	34%
04	Automation	27%

Why security integration matters now

When we talk to MSPs, we hear a pattern emerge. There are three forces that drive this transformation:

- **Threat escalation:** Ransomware, supply chain attacks and sophisticated threat actors have made reactive security untenable. MSPs need integrated detection and response capabilities that work across their entire client base.
- **Compliance pressure:** Regulations continue to expand. Insurance requirements tighten. Clients demand proof of comprehensive security controls, not assurances that multiple disconnected tools exist.
- **Client expectations:** Your clients don't want to hear about your tools; they want outcomes. Integrated security enables you to deliver measurable protection without explaining why their data crosses five different systems.

XDR and MDR lead the way

Third-party extended detection and response (XDR) integrations saw phenomenal growth: on average, 162%, with native integrations also gaining traction.

Active partners who use Acronis XDR grew 136% during 2025. MSPs integrating Acronis' XDR capabilities can enhance visibility and response across endpoints, email, identity, and firewalls from a single view.

Top XDR integrations used by Acronis partners, 2025

Activations Rank	Integration with Acronis Cyber Protect Cloud
1	Fortinet FortiGate
2	Microsoft 365 for Acronis XDR
3	Fortinet FortiMail

Many MSPs building or expanding security practices find that EDR and XDR require additional security skills their existing team does not have. Building an entire security operations center (SOC) in house is often not an option. Instead, these MSPs leverage managed detection and response (MDR) partnerships, which enable 24/7 threat monitoring and response.

The shift from monitoring to protection

Traditional RMM tools remain essential; you can't manage what you can't see. 2025 data reveals that **60% of the top 10 most used integrations are with RMM tools**, but growth has shifted to integrations that actively defend, not just deploy and monitor. MSPs are investing in tools that:

- **Correlate security events** across multiple sources.
- **Automate threat response** to contain incidents in minutes, not hours.
- **Provide forensics and compliance evidence** clients increasingly require.
- **Enable proactive threat hunting** rather than reactive firefighting.

Automation evolves beyond MSP-specific tools

The second major trend reveals an interesting shift in how MSPs approach automation. While robotic process automation (RPA) integrations grew substantially, the main tool driving that growth might surprise you.

Zapier, a general purpose automation tool designed for SMBs, saw significantly higher growth than MSP-specific automation platforms. In fact, they saw a growth in activations of 146% during 2025. This signals an important insight: **MSPs want flexible, no-code automation that works across their entire business**, not just their technical stack.

MSP tools such as Rewst and MSPBots were not far behind in terms of growth, but this trend reflects a broader reality. MSPs need to automate client onboarding, billing workflows, sales processes and internal communications — tasks that extend well beyond traditional RMM or PSA capabilities. The providers finding the most success are those connecting their entire business operation, not just their technical tools.

Natively integrated workflow automation gains momentum

Alongside third-party automation tools, Acronis' native workflow automation capabilities, released in late 2025, gained significant traction. With automation built directly into the Acronis platform, you can create workflows that span backup, DR, RMM, EDR / XDR and PSA operations without managing API connections or worrying about version compatibility.

For example, when a new device is added, automatically applying a protection plan, triggering the first backup and running initial security checks becomes a predictable and reliable workflow when all capabilities operate within a single system.

What this means for your MSP operations

The automation story isn't about replacing technicians; it's about freeing them from repetitive tasks so they can focus on strategic work. MSPs leveraging automation report:

Faster incident response through automated remediation workflows.

Improved consistency by eliminating manual process variations.

Better scalability without proportional headcount increases.

Enhanced client satisfaction through faster resolution times.

The platform consolidation paradox

Here's the apparent contradiction in 2025 data: While third-party integrations continued to grow, native platform capabilities like RMM, PSA and XDR built directly into the Acronis platform saw exceptional adoption.

For Acronis RMM active users, 2025 growth in licenses was a phenomenal 96%. For Acronis PSA active users, 2025 growth in licenses was 50%.

This isn't a contradiction. It's MSPs being strategic and moving towards MSP 3.0 and platformization.

Why platformization matters

Managing 20+ disconnected tools creates compound complexity. Each tool requires:

- Separate training for technicians.
- Individual license management.
- Unique security considerations.
- Custom integration work.
- Distinct support relationships.

Platform consolidation addresses this by providing core capabilities like monitoring, backup and security in a unified environment. When these functions work together natively, response time drops from minutes to seconds. Context switching disappears. Knowledge transfer accelerates.

Why third-party integrations matter

At the same time, no single platform can be best in class at everything. Your existing billing system might integrate beautifully with your accounting software. Your clients might standardize Microsoft 365, requiring deep integration with their environment. You might have specialized compliance tools for specific verticals.

Strategic MSPs use platforms for core capabilities while integrating specialized tools where they add clear value. The key is intentionality; every integration should serve a specific business purpose, not just exist because it's possible.

The emerging pattern

The most successful MSPs are following a clear pattern:

- **Consolidate core capabilities** on platforms that integrate natively.
- **Integrate strategic tools** that serve specific client needs or vertical requirements.
- **Automate workflows** across both native and third-party capabilities.
- **Continuously evaluate** whether each tool in the stack still delivers value.

This approach reduces complexity while maintaining flexibility, giving you the best of both worlds.

Three strategic integration priorities for 2026

Based on the trends observed in 2025, three integration priorities stand out for MSPs planning their 2026 roadmap:

1 Make security integrations your competitive differentiator

Security is no longer a nice-to-have add on, it's becoming a baseline requirement for MSP contracts. However, most competitors are still assembling security from disparate point solutions. MSPs who integrate security deeply and correlate threats across backup, endpoints, email and identity can demonstrate measurably better protection.

Action step: Audit your current security stack. Can you detect a threat in one area and automatically respond across all areas? If not, security integrations should be your top priority.

2 Automate your entire business, not just IT operations

The Zapier trend reveals something important. Automation delivers the most value when it spans your entire operation. Client onboarding, billing, sales follow-up and internal communications all benefit from automation as much as IT operations.

Action step: Map your manual processes that consume the most time. Look for automation opportunities beyond your technical stack anywhere humans are copying data between systems, where data from one system could enrich and improve processes in another or where your staff is performing repetitive tasks.

3 Expand visibility into client attack surfaces

As remote work persists and cloud adoption accelerates, traditional perimeter security becomes insufficient. MSPs need integration with asset discovery and attack surface monitoring tools to help clients understand their actual exposure.

Tools that automatically discover devices, applications and cloud resources and assess their security posture, like Acronis Microsoft 365 Security Posture Management, saw significant growth in 2025. This trend will accelerate as cyber insurance requirements become more stringent.

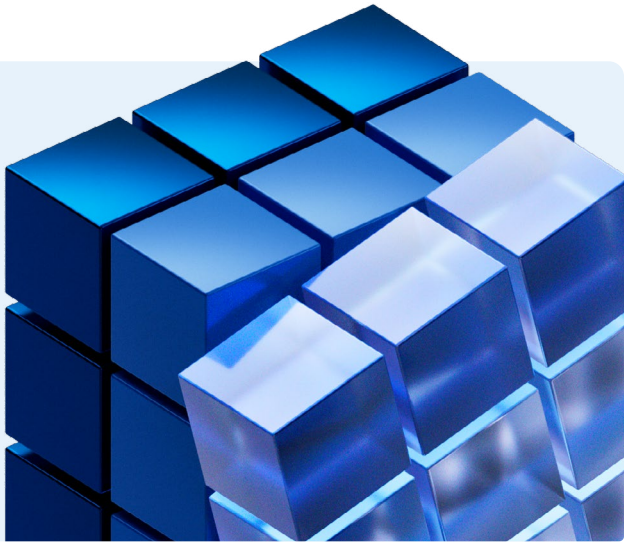
Action step: Evaluate how completely you understand each client's attack surface. Can you definitively answer what assets they have, where they're exposed and how they're protected? Integration with discovery and monitoring tools bridges this gap.

The bottom line: Integration as strategy

Integration isn't a technical detail; it's a business strategy. MSPs seeing the strongest growth in 2025 weren't necessarily the ones with the most tools. They were the ones whose tools worked together most effectively.

Whether through Acronis' natively integrated capabilities or third-party connections, integrations enable you to:

- Respond faster to threats and client requests.
- Operate more efficiently with smaller teams.
- Scale more effectively without linear cost increases.
- Compete more successfully against larger providers.
- Deliver better outcomes that clients can measure.



The shift toward security-first integration, flexible automation and strategic platform consolidation will define MSP success in 2026. The question isn't whether to invest in integration; it's which integrations will drive the most value for your specific business.

About Acronis Cyber Protect Cloud

Acronis Cyber Protect Cloud provides MSPs with natively integrated cybersecurity, data protection and endpoint management. The platform supports both native capabilities and free third-party integrations with leading RMM, PSA, security and automation tools.

With over 300 technology integrations and a global ecosystem of partners, Acronis enables MSPs to deliver comprehensive protection efficiently, whether through native features, third-party connections or strategic combinations of both.

For more information about integration capabilities or to explore the Acronis integration ecosystem, visit solutions.acronis.com. As the Acronis ecosystem continues to expand, MSPs and ISVs have more opportunities than ever to innovate, automate and secure their service offerings for 2026 and beyond. We invite ISVs to develop an integration and we are always happy to receive suggestions for new integrations to shape the future and continue to grow Acronis ecosystem.

Report methodology

This report analyzes integration adoption patterns across thousands of MSPs using Acronis Cyber Protect Cloud during 2025. Data includes both native feature activation and third-party integration usage. Growth rates reflect year-over-year changes. Categories are determined by primary integration function.

All percentage figures and growth rates reference internal Acronis data sources and have been reviewed for accuracy. Specific numerical values have been generalized to protect competitive information while preserving trend accuracy.

About Acronis

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs) and enterprise IT departments.

Founded in Singapore in 2003 and headquartered in Switzerland, Acronis operates in 50+ countries. Over 21,000 service providers use Acronis solutions to protect more than 750,000 businesses worldwide.

Acronis

Learn more at acronis.com