



MSP stack consolidation guide: Reduce tool sprawl and improve your bottom line



Tool sprawl is unsustainable. When managed service providers (MSPs) use multiple tools to administer services for clients, they face challenges: overtaxing staff with routine tasks, adding complexity to processes and struggling to maximize operational efficiency. Product managers have difficulty scoping and pricing managed services. Technicians, managing multiple tools, have to repeat many common, critical and time-consuming processes for each vendor or system. It's an expensive issue that consumes resources.

Tool consolidation is a global business trend

Inefficiency costs money and limits growth, so it's no wonder tool consolidation is a global business trend. According to IDC,¹ more than half of respondents to a survey were already consolidating security tools and vendors in 2023, and more than 85% planned to pursue consolidation by the end of 2025.

> 50%

2024

> 85%

2025

Signs it's time to consolidate tools

Expanding client services becomes increasingly difficult as you try to make new tools work together. Finding and hiring experts to manage disparate tools becomes a major cost issue. Alert fatigue sets in as multiple tools deliver multiple warnings.

You must get tool sprawl under control before it erodes your bottom line. If you encounter any of these situations, it's time for consolidation:

Slow performance negatively impacts your clients' experience

Administering services with multiple tools can lead to a poor client experience. When metrics for your clients' workstations lag, you need to consolidate. Critical performance metrics to monitor include CPU and RAM performance, shutdown and boot times, application responsiveness and network latency.

¹ <https://www.cio.com/article/3496811/can-you-have-too-many-security-tools.html>

**Tool sprawl
doesn't get
better with time.
It gets worse.**



Using too many agents affects reliability

When you have too many agents deployed, conflicts are almost inevitable. Conflicting agents can force your technicians to deal with time-consuming problems. You also must allocate sufficient time to test new agent versions and agent deployments for compatibility with existing ones. Testing consumes time and resources.

Your tool stack impacts your ability to deliver services efficiently

Tool sprawl increases the amount of time necessary to deploy and configure a service on a new client endpoint. Deployment and configuration become difficult and time consuming. Deploying patches can cause conflicts between tools. Those issues make client onboarding or offboarding difficult. They also require considerable effort from your technicians to resolve.

3 factors to consider when consolidating tools

Even when you know you need to migrate, selecting a new platform is a big decision. There are important factors to consider in choosing a platform, including:

Integrations

Integration of tools in an MSP platform is not a given. Some platforms are nothing more than disparate applications loosely patched together. You need to know answers to some critical questions: What tool integrations are available? How well are the tools integrated? And how much work will you have to do to ensure that integrations work and maintain them? Natively integrated solutions that don't require manual integration make those questions irrelevant.

1

Ease of use

It's critical to make sure that you have a platform that's easy to maintain and enables you to add services quickly and easily. A natively integrated platform maximizes ease of use. You can control all your services through a single console. You can expand and improve services without adding staff. Minimizing the number of vendors you deal with also reduces complexity and simplifies management. And the fewer tools you have in your stack, the less training you need to give technicians on how to use tools.

2

Scalability

If a solution becomes a barrier to growth, you'll find that your business goals will be difficult to achieve. It's important to be confident that the solutions in your platform will scale as you grow. You can achieve scalability with a platform that enables you to easily add services and onboard clients as you expand your business. Juggling multiple tools makes both tasks riskier and more difficult.

3

The difference between integration and native integration

Most vendors combine disparate tools into a loosely integrated MSP platform with a different point of control for each tool. In many cases, vendors rely on manual integrations to make tools work together. MSP technicians have to monitor multiple tools and deal with issues when integrations break or don't work properly.

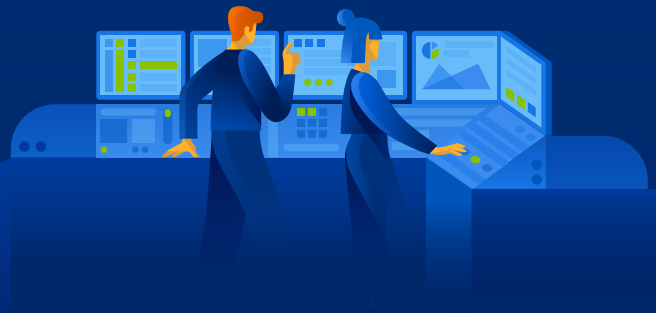
Native integration delivers solutions developed to work together seamlessly in a single, unified platform. With a natively integrated platform, MSP don't have to juggle tools.



Native integration brings together functions such as threat detection and remediation, remote monitoring and management (RMM), patch management and remote access and monitoring, enabling technicians to manage all in one place. Everything works together with a single point of control and without the need for manual integration.

Benefits of native integration for MSPs:

- Reduces the maintenance burden on technicians.
- Shrinks the surface of vulnerability for cyberattacks.
- Relieves MSPs of having to hire an expert to manage every tool in a stack.
- Empowers MSPs to get more work done with less effort.
- Enables easier deployment of client services.
- Eases client onboarding and offboarding.



All of these advantages put MSPs in a position to expand services, cut costs and increase profits.

Experts and MSPs appreciate the benefits of native integration

The Acronis Cyber Protect Cloud platform delivers the ease of use and native integration MSPs need. Third parties such as AV-TEST and Canalys have recognized Acronis Cyber Protect Cloud as the top platform in its category² and a “Champion” in its market space,³ respectively.

² <https://www.acronis.com/en-us/blog/posts/acronis-cyber-protect-cloud-earns-top-product-award-again-in-latest-av-test-evaluation/>

³ <https://www.acronis.com/en-us/blog/posts/canalys-names-acronis-a-champion-in-cybersecurity-leadership-matrix-report/>

Licensing is another important consideration. Some vendors don't offer flexible licensing models. Vendors often lock MSPs into contracts that last for years. **The Acronis pay-per-use licensing model doesn't lock MSPs into contracts or require long-term commitment.**

A lack of native integration erodes the value of RMM

RMM offers an example of the importance of native integration. Managing tools with RMM in a platform that doesn't offer native integration with tools like backup and disaster recovery, as well as critical security tools like EDR and XDR, is complex and time consuming. With native integration, all tools can be managed in a single console with only one agent.

For example, Kaseya VSA, an RMM tool, is one of five tools loosely integrated into the Kaseya 365 platform. So, you can't manage Kaseya VSA and the other Kaseya 365 tools from a single console. Each tool has a separate control panel. Plus, integrations between the tools in Kaseya 365 can break. Your technicians must fix and maintain them.

Acronis RMM, natively integrated into the Acronis Cyber Protect Cloud platform, delivers ease of use and a set of features Kaseya VSA can't match.



Native integration liberates MSPs from tool sprawl

With native integration, you can overcome tool sprawl while improving client service. Acronis Cyber Protect Cloud delivers all the advantages of a natively integrated platform:

- A comprehensive set of tools with a single agent and point of control.
- Faster and more reliable performance for clients.
- Simplified expansion of services and client management.
- A pay-per-use licensing model with no long-term commitment.

