Optimizing your cyber security stack

The definitive guide for MSPs
Navigating security as an MSP

Managed service providers (MSPs) are powerhouses, and they need access to sophisticated technology and reliable partnerships that drive the business forward. An MSP’s tools should be highly functional, easy to manage, and cost effective so they can deliver the managed service their clients expect.

Unfortunately, much like the small and midsized companies they support, many MSPs are at the mercy of a cyber security industry that actively encourages stack bloat and unnecessary complexity. Vendors know exactly how busy MSPs are and that they might not have time to vet vendors or their products properly. After addressing support tickets and other operational work all day, there’s often little (if any) time left over to differentiate between cyber security tools and their features, or to spot exploitative sales tactics.

Another challenge MSPs had to face, and were largely unprepared for, is to take on their clients’ cyber security efforts. IT and cyber security are often seen as interchangeable. As businesses shifted rapidly to remote work models, they became increasingly concerned about their cyber security; MSPs were suddenly tasked with protecting their existing clients from cyber attacks.

MSPs now face the stark reality that they have too many cyber security tools that protect too little of their clients’ threat surfaces. These tools often struggle to integrate, forcing MSPs to flip between dashboards and investigate security alerts riddled with technical jargon.

This is not a sustainable approach to managed security, or to cyber security in general. Instead, MSPs need to build a technology stack that minimizes complexity, maximizes security, and drives business growth.

This eBook explores how the current cyber security industry and overabundance of tools has led to MSP burnout, shrinking margins, and more. Then, you’ll learn how to streamline, optimize, and differentiate your cyber security stack, so you can effortlessly deliver the managed service your clients rely on.
Table of contents

More tools, more problems 4
  Too many tools heighten cyber risk 4
  Complexity overwhelms teams 4
  Unnecessary costs thin your margins 5
  Absorbs too much of your time 5
  Unsustainable over the long term 5

Optimizing your security stack 6
  Step 1: Create an inventory 6
  Step 2: Find a framework 7
  Step 3: Identify flaws and fixes 7

Futureproof your managed security service 8
  Invest in a holistic cyber security solution 8
  Approach cyber security proactively 9
  Add value with professional services 9

Conclusion 10
More tools, more problems

There are more cyber criminals than ever before, with more attack opportunities available to them. Naturally, this has led to an increase in cyber security tools on the market. Many of these tools are point solutions, meaning they’re designed to address one specific concern. As each new problem arises, another tool emerges to solve it.

The result? The average security stack is now a sea of acronyms: EDR, MDR, XDR, NDR, AV, SIEM, SOC, SOAR, IDS, DLP—the list goes on. Considering that every tool has its own data, dashboards, notifications and alerts, costs, processes, vendor support teams, and dedicated training sessions, it’s easy to see why MSPs struggle to keep up.

Too many tools heighten cyber risk

While it’s common for MSPs to use multiple cyber security solutions to protect their clients’ threat surfaces, there’s a tipping point. MSPs can, and often do, have too many products.

With many tools working to keep threats out, it is easy to assume that your clients are fully protected. All these tools will collect a lot of data and generate a lot of alerts that, ironically, create a false sense of security.

On the contrary, layering software, hardware, applications, and tooling creates excessive noise that makes it harder to detect and respond to attacks. Tools often speak different “languages,” meaning they struggle to communicate, integrate, and identify true security problems.

Complexity overwhelms teams

More tooling leads to more work and room for error. Your team may struggle to toggle between reports or dashboards. If there is overlap among the tools in the MSP security stack, you’ll wind up with too much data and too many alerts needing attention.
Consider the effort it takes to investigate alerts—many of which will be duplicates or false positives due to overlapping functionality in your stack—and it becomes clear why less is often more. This noise isn’t just negatively affecting your team, either. An unchecked layering of tools is the best-case scenario for an attacker as they can hide safely in the noise.

What’s more, cyber security expertise is still rare. It’s challenging enough to find IT administrators, let alone cyber security experts with the knowledge and skills to manage the tools in your security stack.

Unnecessary costs thin your margins

Each added tool in the MSP security stack raises expenses—not just in the form of monthly or annual fees to the vendors, but also the cost to market, sell, and manage.

Unfortunately, your target market doesn’t have a lot of budget room for price increases. Asking your customers to pay more for what they may perceive as the same level of service is a particularly difficult sell. So, to serve this market, MSPs may lessen their margins to put their services within reach. This tactic negatively affects the return on investment.

Absorbs too much of your time

Your clients rely on you for a wide range of services, possibly including:

- General IT support
- Disaster recovery
- Compliance management
- Server configuration
- Cyber security

The problem with bloated security stacks is they take attention and effort away from your other money-making services.

32,644 IT professionals across 33 countries found that:

- 40% were at high risk of burnout
- 62% reported feeling physically and emotionally drained

Unsustainable over the long term

The final problem is that complicated tech stacks are just not sustainable. If you add a point solution each time a cyber attack technique emerges, regulations are enacted, or your clients’ threat surfaces change, you’re entering an exhausting game of catch-up that may eventually lead to burnout.

Burnout is rampant within the cyber security industry and, more generally, across IT workers. The State of Burnout in Tech [2022 Edition] surveyed 32,644 IT professionals across 33 countries and found that 40% were at high risk of burnout. More specifically, 62% of those surveyed reported feeling physically and emotionally drained.

Time for the good news: there are simple ways to optimize your tech stack, taking weight off your team’s shoulders and improving your clients’ defences at the same time.
Optimizing your security stack

There’s a natural impulse to resist change, even if the stack you’ve put together doesn’t work anymore (or never did). You’ve already invested in each tool, trained your team, deployed it in your customers’ networks, and probably gained significant hands-on experience.

However, it’s critical to assess and refresh your cyber security stack regularly. You may find there are tools you pay for but don’t even use. You may realize the tools you implemented aren’t meant for your clients, or that your team needs something more user-friendly.

There are a multitude of reasons to optimize your stack, and here’s how to do it.

STEP 1: CREATE AN INVENTORY

Step one is to create an inventory of existing security tools you use to protect your clients. Your exact list of tools will vary greatly, but remember to include things like:

- Threat monitoring, detection, and response for endpoints, networks, and cloud-based services
- Firewalls
- Password managers
- Multi-factor authentication (MFA)
- Virtual private networks (VPN)
- Data and device backups
STEP 2: FIND A FRAMEWORK

Step two is to find a framework that can help you keep things organized. By using a highly regarded industry standard, organizations can evaluate their cyber security service tangibly and unambiguously based on their organization’s specific circumstances, industry, and client needs.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), for example, shows how security solutions can be layered to minimize cyber risks. The framework focuses on five core components:

- **Identify**: determine business-critical functions and what security threats could disrupt them.
- **Protect**: reduce the likelihood and limit the impacts of security incidents (e.g., antivirus or firewall).
- **Detect**: the measures in place to pinpoint threats or risks (e.g., suspicious activity monitoring).
- **Respond**: the capability to address incidents effectively (e.g., incident response planning).
- **Recovery**: the controls in place to restore business after an incident (e.g., data backups).

According to NIST, an organization can “use the Framework to determine which activities are most important to assure critical operations and service delivery. In turn, that will help to prioritize investments and maximize the impact of each dollar spent on cyber security.”

STEP 3: FIND A FRAMEWORK

Step three is to map your inventory of tools to the five phases above and take note of where there are empty spaces (which would imply you have gaps) or overflowing sections (which would imply you have redundancies). Then you can begin taking steps to make sure your stack is well-balanced by removing and adding tools as needed.

Step three is also a convenient time to factor in the return on investment of your security stack—how much profit does each tool bring in? How does that compare to its costs? These calculations can be time-consuming, but help you make strategic business decisions that also improve your margins.
Futureproof your managed security service

While assessing your security stack, this is a good time to identify ways to differentiate your offerings—especially as the marketplace grows more crowded. Below are three key things that MSPs can do to set themselves (and their managed security service) apart from the competition.

Invest in a holistic cyber security solution

MSPs should consider a holistic cyber security solution that protects endpoints, networks, and cloud services equally from a single unified dashboard. A holistic solution consolidates a wide range of tools into a single, easy-to-use product:

- Endpoint detection and response
- Cloud workload monitoring
- Email protection and expert review of suspicious messages
- Network traffic monitoring
- External scanning
- DNS firewall
- Anti-virus functionalities
- Ransomware protection
- Active threat hunting and vulnerability reporting
- Triaged reporting

The inherent flexibility and scalability of a holistic solution make it easy for MSPs to fill out and deliver different tiers of service—an important selling point as your customers have unique needs and budgets. You can strategically choose security features for each tier, in turn helping you differentiate your service.

As you know, lower service tiers are often limited in functionality and scope. With a holistic solution, you can incorporate more impactful protections at a lower price point, raising the bar on even the most budget-conscious tier.

Approach cyber security proactively

Staying ahead of cyber threats is top-of-mind. Your ability to detect and respond to threats early is vital for keeping customers secure. To that end, looking ahead at the emerging cyber threat landscape should be a major component of any managed security provider’s offerings—but that’s easier said than done.
The expertise needed to identify emerging threats and apply that knowledge to a customer’s threat surface doesn’t develop overnight. The cost to hire a security expert often takes building an internal team off the table, but there’s still a way to offer this expertise to your customers.

Partnering with a cyber security firm outsources the heavy lifting of threat intelligence to a team of experts with the required skillsets. Your MSP team can focus on managing your clients’ IT operations, turning to outsourced security professionals for support with specialized tasks.

This sort of partnership provides immense benefits for MSPs. Vendors that own and maintain their own solution are invested in keeping their tools current with emerging threats. This means that MSPs can access an evolving solution with new features and capabilities, all at no added cost.

Add value with professional services

Being able to support your clients through cyber security incidents, post-mortem investigation, strategic planning, and maturity assessments helps ensure you have a competitive offering, today and tomorrow.

You can round out your cyber security service by offering some of the following services, and the right partnership makes it easy to do that.

INCIDENT RESPONSE AND PLANNING

Incident response (IR) and IR planning refer to activities that businesses undertake to prepare for a cyber security incident. These processes and their accompanying documentation are time-consuming but ultimately necessary for businesses in every sector. If you can guide your customers through these activities, you’ll deliver greater value and stay competitive.

Partnering with an experienced vendor can further simplify this process, giving your customers access to a wealth of cyber security expertise that may otherwise be out of reach. For you, the partnership route results in healthy profit margins, as you don’t need to invest in building that expertise internally.

INCIDENT RESPONSE AND PLANNING

Following a cyber security incident, digital forensics gathers and preserves evidence to aid in rebuilding defences or enhancing protection. In cases where the attacker is identified, digital forensics is necessary for prosecution.

Chances are that prospects coming to you for digital forensics services want to know:

- How they were attacked
- Ways to prevent it from happening again

Digital forensics investigations offer a wealth of information on the customer’s threat surface. Putting this information into practice—essentially translating it into concrete strategies and steps a business can take—allows you to tailor defences to a customer’s unique needs. This level of defence isn’t possible without the insights delivered by services like these.

MATURITY ASSESSMENTS AND STRATEGIC PLANNING

Many organizations understand the need to implement cyber security practices but lack the experience needed to incorporate them into strategic planning. Others may need an external perspective on their security program to find gaps and vulnerabilities.

In either scenario, they need help from a third party. MSPs that offer these services, whether through maturity assessments or virtual chief information security officer (vCISO) consultations, can solidify their standing as trusted partners and strengthen their competitive advantage.
Conclusion

It’s time to say goodbye to overcrowded, overcomplicated security stacks. Point solutions have already taken up too much of your time, effort, and budget.

Complexity is the enemy of effective security. By reducing this complexity, your team can focus its energy on what truly matters to your customers: effective, attainable security that provides true peace of mind.

Removing the clutter from your existing security stack will enable you to take a new approach to your managed security offerings. In turn, this will not only eliminate the challenges that result from traditional tech stacks but set your managed security service apart from the competition.

Cyber security made simple.

Sources
Covalence managed detection and response (MDR) platform

At Field Effect, we partner with MSPs like you to provide superior protection for clients with our all-in-one cyber security solution and our well-rounded array of professional services.

Covalence, our managed detection and response platform, provides continuous visibility of a company’s IT infrastructure to identify potential threats, vulnerabilities, and malicious activities. By providing easy-to-understand, actionable insights, Covalence helps you prioritize and resolve cyber security issues and improve security. The result is a powerful cyber security solution that delivers big business insights without the matching price tag.

About Field Effect

Field Effect, a global cyber security company, is revolutionizing the industry by bringing advanced cyber security solutions and services to businesses of all sizes.

After years of research and development by the brightest in the business, we have pioneered a holistic approach to cyber security. Our complete Managed Detection and Response (MDR) solution, flexible simulation-based training platform, and expert-led professional services form a unified defence that results in superior security, less complexity, and immediate value.

We build solutions that are sophisticated, yet easy to use and manage, so every business owner can get the hands-free cyber security they expect and the sleep-filled nights they deserve.

Contact our team today.

Email:
letschat@fieldeffect.com

Phone:
Canada + United States
+1 (800) 299-8986
United Kingdom
+44 (0) 800 086 9176
Australia
+61 1800 431418

fieldeffect.com