RAPID7

The Case for Security Vendor Consolidation

A Guide to Reducing Costs and Increasing ROI

Contents

Why consolidate?

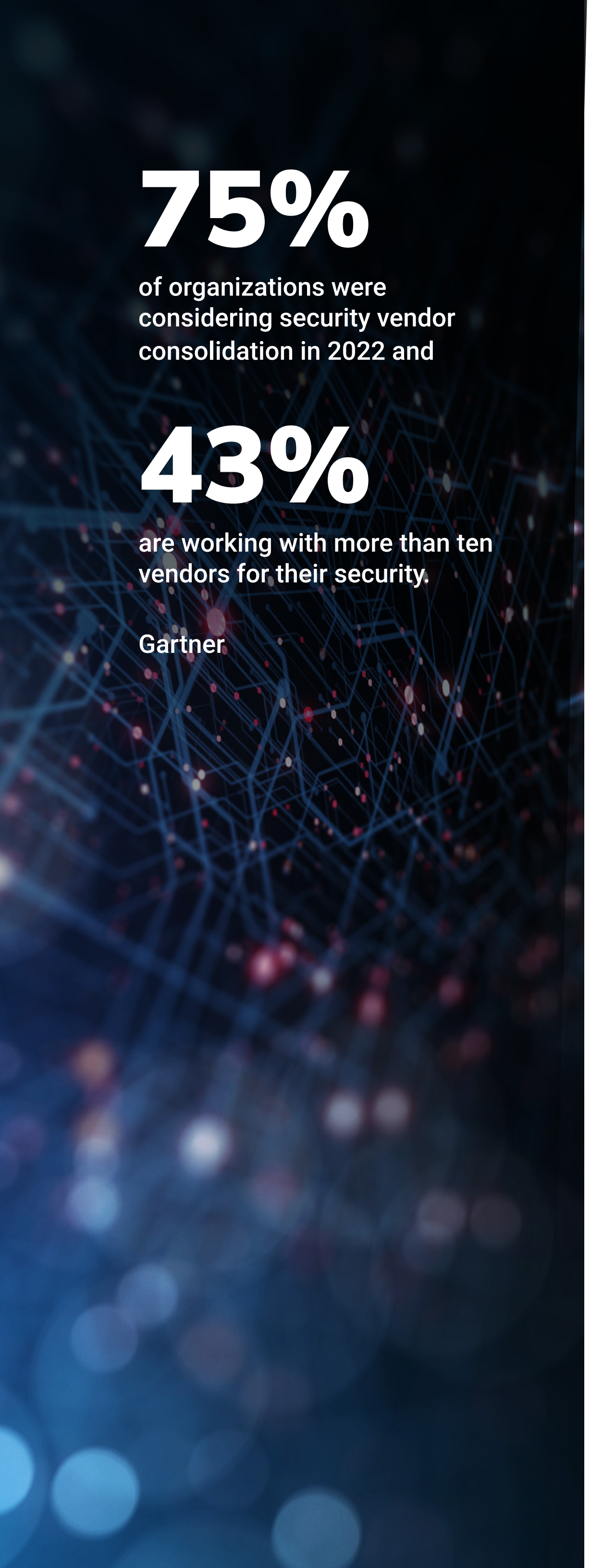
When it comes to efficiency, nothing beats consolidation. We're constantly consolidating in our personal and professional lives — our assets, data, streaming subscriptions, and even our insurance — in an effort to make our lives simpler. Why should an organization's security vendors be any different?

In a recent survey, Gartner found that 75% of organizations considered security vendor consolidation in 2022, an increase of nearly 50% from 2020. Many companies are dealing with a glut of security vendors — in the same Gartner survey, 43% of organizations revealed they were working with more than ten vendors for their security.

This second statistic is concerning for a few reasons: a large number of vendors is costly, drives operational inefficiencies, and creates a fragmented picture of risk across your environment. Teams dealing with a surplus of tools may also struggle to develop a consistent definition of risk, which may result in poor risk prioritization and failure to respond to risks properly.

In the past few years, the global economic climate has been in a state of flux — inflation is high, spending is down, and layoffs have increased — leading most organizations to reevaluate spending habits. The recent wave of layoffs across industries has also highlighted and exacerbated the skills gap that most organizations are facing. There simply aren't enough resources for organizations to have experts in each of its security solutions or navigate relationships with so many vendors.

Companies need the efficiency, efficacy, and productivity of consolidation. In this eBook, we'll dive into the benefits of consolidation, the most common barriers to consolidation, and how to get started.



75%

of organizations were considering security vendor consolidation in 2022 and

43%

are working with more than ten vendors for their security.

Gartner

Benefits of consolidation

An organization considering security consolidation often looks at what it's trying to avoid — redundant solutions, skills gaps, and rising costs — but fails to consider what it'll gain. The prevailing wisdom used to center around cherry-picking solutions from various vendors and cobbling together a security toolkit stuffed to the gills with "best-of-breed" products. Now, companies are finding that this approach created more problems than it solved. Let's look at a few of the biggest benefits of consolidation.

Improved security posture

In 2021, IBM released the results from its sixth annual Cyber Resilient Organization Study. In the study, they found that 45% of security teams used more than 20 tools when investigating and responding to a cybersecurity incident. You'd think that a proliferation of tools could only help when responding to a cybersecurity incident, but that's not the case. Too many tools from disparate security vendors can create confusion. Each tool provides a slightly different but crucial interpretation of system events or timelines, as well as different definitions of risk and risk severity, which diffuses precious attention and exacerbates swivel-chair syndrome. Thus, teams often find themselves spending considerable time corroborating bits of data across products, rather than focusing on the core objective of mitigating risk.

Consolidating security vendors helps teams create a more holistic, end-to-end view of risks and threats. With consolidation, teams can eliminate the frustration of multiple data sets and platforms. Not only does this allow teams to respond faster to risks and vulnerabilities within their infrastructure, but it also encourages greater collaboration between teams. Working from a unified, single source of truth can help teams develop a proactive approach to security, manage threats more effectively, and prioritize risk. This both strengthens the organization's overall security posture and creates a more resilient IT infrastructure.

77%

of organizations are using or exploring the use of AI and

30%

of organizations are specifically using AI for security and threat detection.

IBM

Reduced costs and improved ROI

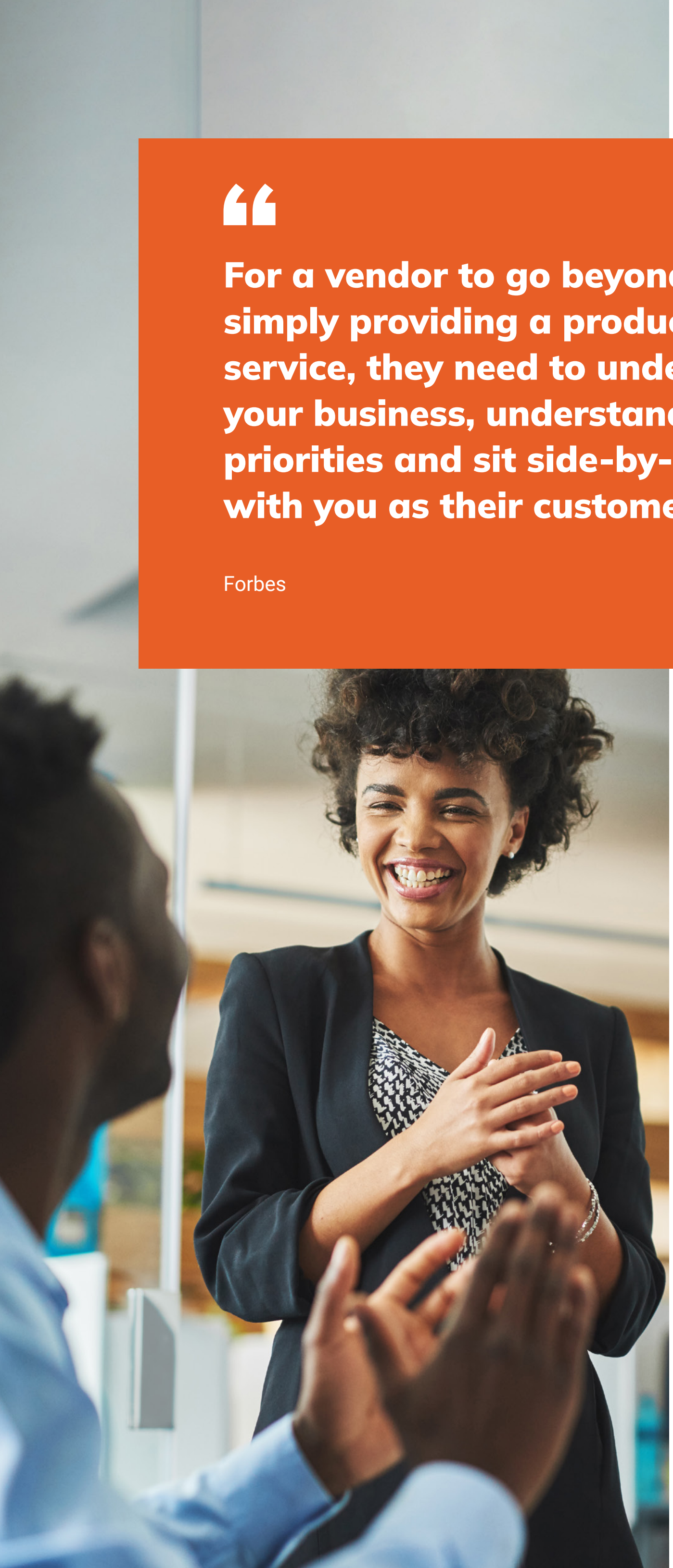
Less equals more when it comes to consolidating your organization's security posture. That same sentiment applies to money saved and ROI gains. Evaluating and eliminating redundancies in your organization's security solutions is one of the easiest ways to save money. Moreover, the average organization finds that reducing solution sprawl can help it take advantage of consolidation discounts from its preferred vendors.

With the money saved from consolidating your security solutions, your organization will be better positioned to grow and protect itself from evolving cyber threats. Money saved from streamlining services and reducing vendors can be redirected into other departments, used to train up your staff, or invested in the latest technology from the security vendors you've chosen to continue working with. For example, IBM found that 77% of organizations are using or exploring the use of artificial intelligence (AI). AI has a multitude of uses, but the same study found that almost 30% of organizations are specifically using AI to aid in security and threat detection. Leveraging the money saved from consolidation can give your IT teams the wiggle room needed to research how to utilize AI, machine learning, and other emerging technologies without exposing your organization to unnecessary risk.

Consolidation can also save your organization time in investigating and responding to threats. Organizations dealing with multiple tools across a variety of vendors often have to toggle back and forth between them to resolve a security event. Precious time is wasted logging into separate systems, shifting data between tools, and investigating false positives and duplicative alerts. Consolidating tools allows for streamlined data transfer, convenient access to single platforms, and a reduction in "noisy" alerts. The time saved by consolidation can increase productivity and employee satisfaction, and improve the ROI of your security program.

Improved operational efficiency

Speaking of employee satisfaction, juggling multiple vendors is a complex and time-consuming task. Reducing the overall number of vendors means that your team can spend less time on contracts, chasing down vendors, reporting issues, and requesting support on new features.



> **For a vendor to go beyond simply providing a product or service, they need to understand your business, understand your priorities and sit side-by-side with you as their customer.**
>
> Forbes

Your teams will also have an opportunity to build better relationships with your preferred vendors. According to Forbes, “For a vendor to go beyond simply providing a product or service, they need to understand your business, understand your priorities and sit side-by-side with you as their customer.” It’s much easier to build this type of deep, collaborative relationship — which can also lead to product discounts, earlier access to new products, and more comprehensive product support — when you’re not juggling a dozen other vendors.

With fewer vendors, your team can develop a better understanding of how to use your security solutions and adapt them to your organization’s specific needs. For example, fewer vendors simplifies and reduces the time needed for the configuration and setup of new products. Consequently, your team can spend more time with each product, learning the ins and outs and how to optimize each for your infrastructure.

Beyond configuration and setup, when there’s an issue with your tech stack, it’s easier to find and fix the cause when you’ve consolidated your security solutions. Organizations with a large number of vendors and products often find it difficult to track the performance of individual applications. This means that a product could be performing suboptimally and the IT team is unaware until it becomes a larger issue, often with broader security ramifications, like a data breach or unchecked vulnerability.

A less complicated tech stack with improved visibility makes it easier to ensure that your applications are compliant with industry and regulatory frameworks, which is crucial for organizations in highly regulated sectors like financial services and healthcare. Consolidation enables you to better manage your tech stack’s updates and data audits to achieve and maintain compliance.

Perceived issues with consolidation

41%

of organizations surveyed by Gartner say consolidating security solutions improved their risk posture.

While the benefits of consolidation are clear, some organizations may still find the perceived downsides of consolidation as reason enough to avoid. However, many of the objections to consolidation are rooted in misunderstanding or a lack of context. There are two major concerns that are often raised when consolidation is discussed.

The fear of losing "best of breed"

The first is potentially losing "best of breed" when it comes to your security solutions. "Best of breed" refers to the best product of its type. Organizations conduct research to find the right products for each application area, and often find that a particular vendor excels in one area and offers less-than-stellar products in another. Consequently, this leads organizations to believe that consolidation is a compromise in quality.

This concern is understandable. However, an increasing number of practitioners believe that the benefits of consolidation outweighs those of a "best of breed" approach. In a recent Gartner survey, 41% of respondents said an improvement in their organization's risk posture was the primary benefit of consolidating their security solutions. As we discussed above, consolidation offers major improvements in security posture, operational efficiency, and end-to-end visibility consolidation offers. This is why experts now believe that the sum of these parts actually adds up to far greater security than cobbling together a group of individually excellent, but disjointed solutions.

The fear of vendor lock-in

The second issue raised with consolidation is the fear of being locked in with a certain vendor. In other words, organizations fear consolidating only to find that the vendor is subpar or ends up proving unreliable in meeting their roadmap promises. Then, they'll be forced to suffer through the duration of their contract or subscription period before beginning the search all over again for a satisfactory solution.

The best way to combat the fear of consolidating with subpar vendors is to carefully assess vendors. Researching vendors can help ensure that each potential partner will meet your product needs, is unlikely to be compromised, and won't be outpaced by competitors in terms of innovation.

Here are a few questions to ask when vetting potential vendors.

1. **How does the vendor approach security?** This can include asking if they use third-party vendors to handle security and if any of your data will be stored on the vendors' systems, and researching how they've responded to security threats in the past.

2. **What are all of the cost considerations?** Often vendors will quote a price that doesn't include maintenance, additional subscription fees, licensing additions, or other necessary add-ons to your service. Asking about all of the potential costs can not only help you stick to your budget, but also keep your team from feeling bamboozled by hidden fees.

3. **How well do their tools integrate with your organization's systems?** While you may be impressed with their offerings, you may want to reconsider consolidating with a vendor whose tools don't integrate well with your existing systems. It can take considerable time and effort to adjust a tool to fit your needs versus purchasing one that's designed to support and complement the various elements of your IT infrastructure.

4. **How difficult will it be to onboard them or to change vendors later on?** Nothing lasts forever, and you may find that your organization needs to change vendors somewhere down the road. When you do, you want the process to be seamless and uncomplicated. Asking crucial questions about onboarding and offboarding when shopping for vendors is the best way to ensure that both transitions are smooth.

Confronting where your organization may be leaning into misconceptions around consolidation can help break down the barriers to adopting a more efficient and secure approach to security. It can also help you start the conversation with executives and other departments interested in consolidation but wary of its perceived drawbacks. Once you've crossed this bridge, it's time to start consolidating!

Consolidation — where to start

Untangling the Gordian knot of your current security solutions and vendors can feel overwhelming. Don't worry! We can show you how to get started on your consolidation journey. As you begin consolidation, it's important to understand all of your current tools and solutions and gather information on the vendors who provide them.

In the same way that you need end-to-end visibility in your system to make solid security decisions, you'll need a thorough knowledge of your existing tech stack to identify where you can most benefit from consolidation.

Avoid consolidating across layers

After cataloging your current resources, you'll want to consider the right way to consolidate. We suggest consolidating across functions and not layers. In other words, your infrastructure has layers of security, or redundancies to catch vulnerabilities, in a strategy many refer to as "defense in depth." For example, this could look like a security solution that monitors endpoints and a separate solution that manages threats across the entire ecosystem.

So why shouldn't you consolidate across layers? Consolidating across layers can actually weaken your security posture, eliminating good redundancies within your system. Secure design principles manage the risk of a "failed" control through redundancy. In consideration of the complexity of modern hybrid infrastructure, defense in depth is not only a good practice; it is entirely a necessity. For example, trusting the security of your operating systems (as well as the associated maintenance and update solutions) to the same vendor that provides your endpoint detection and response solution not only blurs division of duty lines, but might lead to unmitigated systemic risk. Not only are the organization's endpoints vulnerable, but you're also dependent on the same provider to fix "their" weakness.

Consolidating across functions

Consolidating across functions is the preferred approach. When considering which functions to consolidate, it's a good idea to consider your security needs in a particular area. For example, an organization struggling with the growing attack surface created by its drive for cloud innovation may want to consider consolidation in the following functions: cloud security, vulnerability management, and application security. Combining these functions under a single vendor can provide better visibility and monitoring for more comprehensive cloud risk management.

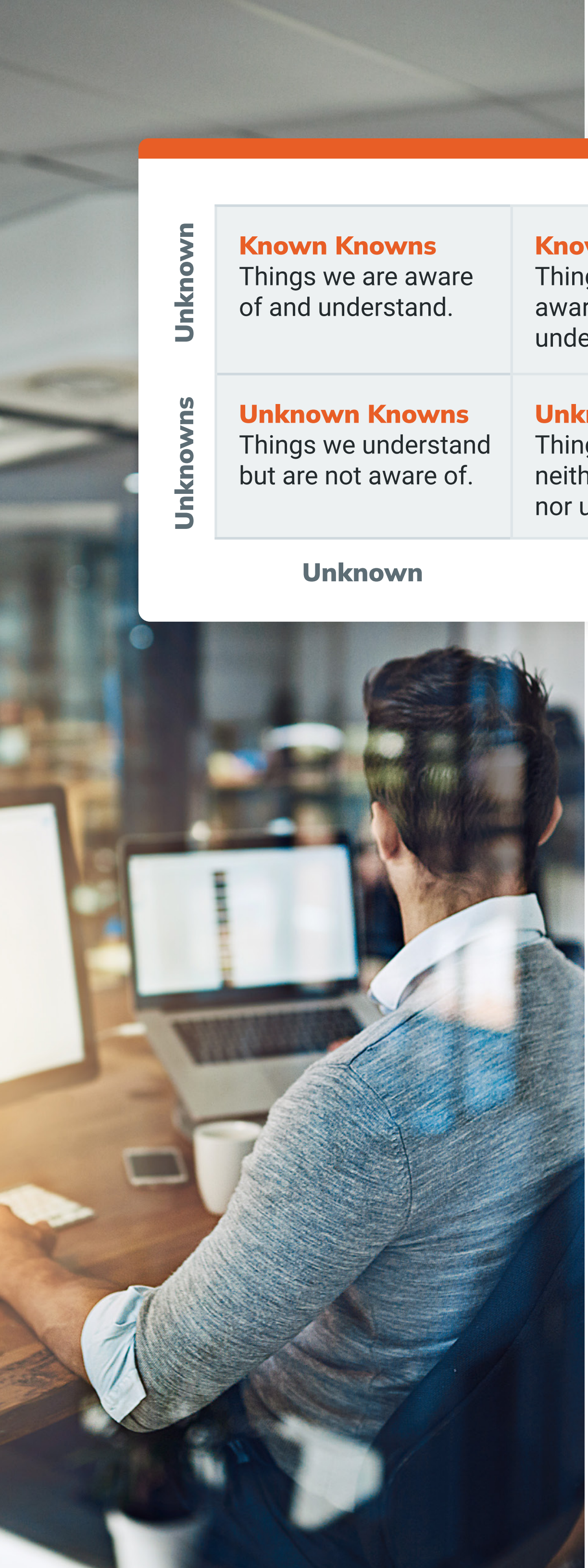
It can also be helpful to consolidate functions within a layer. Instead, look at an organization's goals within a particular layer and identify functions to consolidate. This could look like an organization operationalizing or maturing its detection and response program by consolidating in the following functions: detection and response, threat intelligence, and vulnerability management. The result is a more comprehensive approach to managing risk.

Finding the right tools

Once you've identified the best functions to consolidate, or how you'd like to approach consolidating functions within layers, you'll want to consider which consolidation packages and tools are best for your organization.

If you're looking to secure your migration to the cloud, here are a few of the most important features to look for in consolidation packages and solutions:

- **Automated workflows:** If the purpose of security consolidation is to make your organization's security efforts simpler, then automation is key. Ensuring that your consolidation package includes automated workflows and controls, such as ensuring no S3 buckets are set to public, will help your team respond to threats faster and reduce overall risk in your infrastructure.
- **Risk prioritization:** Consolidation can eliminate the confusion of multiple data streams from various solutions, but you'll also want to look for tools that offer context to help you prioritize risk signals across your ecosystem. This includes solutions that help your team determine which of your public-facing assets have undesirable ports open.



Unknown	**Known Knowns** Things we are aware of and understand.	**Known Unknowns** Things we are aware of but don't understand.
Unknowns	**Unknown Knowns** Things we understand but are not aware of.	**Unknown Unknowns** Things we are neither aware of nor understand.
	Unknown	Unknowns

- **Compliance automation:** Your consolidated solution should help you meet internal and external compliance regulations by detecting and remediating compliance drift. Bonus points if the tools track and support your industry's specific compliance regulations and work hand-in-hand with workflows to ensure continuous compliance.
- **Security scanning:** The threat landscape is always changing, so continuous scanning and testing of your infrastructure's applications is key to your security strategy. An ideal consolidation offering should provide your organization with real-time security assessments, in-depth reports for better cross-team collaboration, and actionable insight into evolving risks. The best tools will also ensure that your team is aware of the four main risk types across your system: known knowns, known unknowns, unknown knowns, and unknown unknowns.

On the other hand, if your priority is maturing your detection and response program via outsourcing, here are some critical features to look for:

- **Complete coverage:** As you consolidate your detection and response program, you need to be able to trust that your entire attack surface is under control. That means tools with full coverage across your endpoints, network, users and the cloud, so you can eliminate threats across your entire environment.
- **Transparent partnership:** A good managed consolidation offering should truly be a partnership. You'll want to look for frictionless collaboration with experts, so you can get answers whenever you need them and the ability to see exactly what the external SOC team is seeing.
- **End-to-end detection and response:** A consolidated detection and response offering needs to go beyond the word-for-word basics of just detection and response. You should look for a solution that supports you through the entire process, with end-to-end digital forensics and full incident response.

Once you've identified the right consolidation packages and tools, you can match them to the areas in your organization that you've identified as most in need of consolidation. It's wise to discuss your goals around consolidation with potential vendors, so they can help you identify the best existing offerings or even help you create a customized solution.

Conclusion: security solution Jenga®

When it comes to consolidation, some organizations may be clinging to the status quo. While the benefits of consolidation are clear, teams are concerned with the potential disruption of introducing new products into their environments or removing existing solutions. It's like a game of Jenga®. Instead of wooden blocks, organizations construct a precarious security solution, and though it's leaning a little to the left and overburdened by inefficiencies, redundancies, and ballooning costs, it's still difficult to part with.

The threat landscape, however, is changing rapidly, and consolidation offers the security improvements an organization needs to tip the scales in its favor. It's time to simplify and streamline your organization's security solution, and that begins with gaining visibility into your tech stack and identifying where consolidation can improve your team's productivity and effectiveness in detecting and mitigating risk.

Ready to start consolidating your tech stack? Consider consolidating with Rapid7.

Rapid7's Cloud Risk Complete (CRC) offers comprehensive cloud management by securing cloud, on-prem, and hybrid environments with a single subscription and unlimited opportunity. Automated workflows? Unlimited. Vulnerability management? Unlimited. Application security? Unlimited. You get the idea. Analyze, respond to, and remediate risks without a patchwork of solutions or additional costs.

Experience unlimited risk management everywhere with **Cloud Risk Complete**.

Rapid7's Managed Threat Complete (MTC) helps your organization streamline the threat detection and response process. Leverage Rapid7's MDR analysts and digital forensics and incident response experts to supercharge your team. Your environment is monitored 24/7/365, and threats are acted on, end to end. Data collection is unlimited. Incident response, unlimited. Vulnerability management, unlimited. You proactively handle your risks, and Rapid7 reacts for you when a threat gets real.

Discover unlimited threat coverage with **Managed Threat Complete**.

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/