eBook

ThreatDown™
Powered by Malwarebytes

The Cost of Complexity

7 ways to improve security by doing less not more

ThreatDown™ Powered by Malwarebytes

Contents

Ransomware raises the stakes

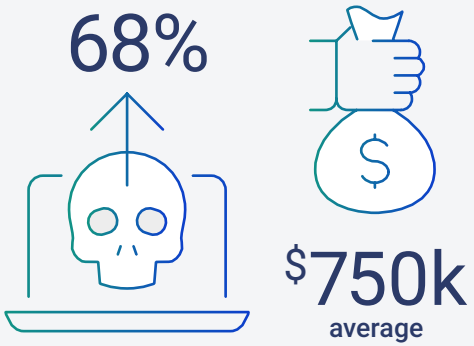
The rise of "big game" ransomware since 2018 has altered the landscape of computer security considerably, increasing the complexity of security stacks and ramping up the demands on hard-pressed IT teams. And cybersecurity's biggest headache continues getting worse. In 2023, the number of known big game attacks increased by 65%,[1] and the average ransom payment was $750,000.[2]

Unlike traditional malware that targets individual computers, big game attacks are designed to disable entire companies by targeting their high value servers, or even whole networks. And no organization is safe, big or small: LockBit, the most active and dangerous ransomware group in the world has targeted everything from multi-nationals to local law firms.

To make the switch from targeting computers to companies, ransomware groups adopted new tactics—hacking into networks, exploring them, making themselves all-powerful administrators, and spreading their ransomware manually. Cybercriminals could take days or even weeks to carry out a single attack, but the payoffs were enormous.

The implications for cybersecurity were profound. Generalist IT staff in small and medium-sized businesses had to create a security infrastructure that could defend their organizations against patient, experienced and sophisticated threat actors with a global reach and unfathomably deep pockets.

The result was a steep rise in the complexity of security stacks, and it is increasingly clear that this complexity itself can have a negative impact on security outcomes.



In 2023, the number of known big game attacks increased by 65%, and the average ransom payment was $750,000.

[1] 2024 ThreatDown State of Malware, https://try.threatdown.com/2024-state-of-malware
[2] Ransom Monetization Rates Fall to Record Low Despite Jump In Average Ransom Payments, https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments

Why complexity is a security issue

The arrival of big game ransomware forced a switch from focusing on network boundaries to looking for stealthy intruders inside networks. To do this IT teams adopted technologies that supported advanced threat detection and response strategies such as continuous monitoring, threat hunting, and incident response.

Tools like Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), and next-generation firewalls offered organizations much better visibility of events on their networks. But all the information they produced had to be digested, cross-checked, and acted on by staff who were already hard-pressed.

And while thought leaders postulated about zero-trust networks, IT teams wrestled with folding ever more systems into Identity and Access Management solutions, and multi-factor authentication rollouts.

Everything had its own implementation, configuration, training requirements, alerts, maintenance, and compliance obligations. And absolutely everything had a console demanding attention.

A recent survey showed that organizations with fewer than 1,000 employees have on average 450 devices to maintain and just three IT staff members. For them, security is one task among many, and they don't have time to waste. 68% of them say managing limited time and resources is their biggest challenge, and they're losing an average of one day a week to unnecessary complexity.

64% reported that the harder a security solution is to use, the less likely it is to be effective, and 78% believe that the more complex their IT environment is, the harder it is to secure.

The survey reinforces a key finding of IBM's 2022 annual Cyber Resilient Organization Report—complex security stacks are bad for security.

> The study revealed that the number of security solutions and technologies an organization used had an adverse effect on its ability to detect, prevent, contain and respond to a cybersecurity incident.

Why complexity is a security issue (continued)

The reasons will be obvious to anyone working in a resource-constrained IT department: Each new tool needs to be rolled out and configured, and staff need to be properly trained in how to get the best out it. Many organizations struggle to do that effectively, and adding more tools to an environment where the existing tools aren't properly integrated compounds the problem.

Different tools from different vendors also come with their own ecosystem of consoles, concepts, terminology, and alerts, forcing IT staff to perform cognitive gymnastics every time they switch from one tool to another. More vendors also mean more regulatory and compliance overhead for standards like SOC 2.

Complex security stacks not only create blind spots and false positives, but they also make it hard to see the big picture, gather critical information, and take action. And every new tool increases the chances of problematic interactions with other tools.

"Complexity slows things down, the more complex a tool is to use the slower it is to react," says Mary Arakiri, Malwarebytes' Senior Director, Information Security. "If you're dealing with a breach, the breach is getting worse."

The problem is exacerbated by complexity in the broader IT environment—78% of IT teams agree that the more complex an IT environment is, the harder it is to secure.

Complex environments are harder to monitor and harder to protect. Combining multiple operating systems or cloud services, for example, often requires additional layers of security and additional management consoles. They're also harder to manage, which squeezes the time left over for proactive security.

Complex environments can make recovering from a cyberattack harder too.

In October 2023, the British Library, the national library of the UK, suffered a devastating ransomware attack. In March 2024, it published an incident review that makes it clear that the library's complex IT environment "both contributed to the severity of the impact of the attack" and was a "primary contributor to the length of time that the library required to recover from the attack."

ThreatDown Powered by Malwarebytes

Why ease-of-use is an antidote to complexity

One of the most important antidotes to complexity in the security stack is ease-of-use.

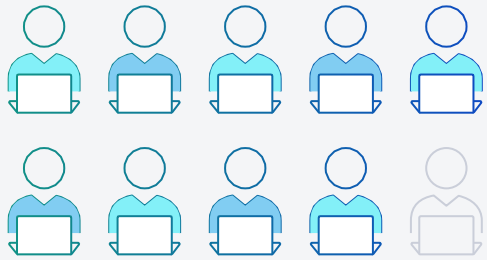
The security cost of poor usability was demonstrated as far back as 1999, in the seminal research paper Why Johnny Can't Encrypt. The researchers challenged cryptography novices to secure an email message by signing and encrypting it with PGP 5.0, which was reckoned to have a "good user interface by general standards." Participants had 90 minutes to perform the task — but most of them couldn't complete it.

The takeaway? Software is only as effective as the functionality its users can make sense of. Ease-of-use makes the full power of security tools available to hard-pressed IT staff, helps them focus on what's important, and saves them time.

"The more complex a tool is to use, the slower you will react," says Mary Arakiri. "You don't want to be digging to find out how to get the information you need."

Arakiri also believes IT staff will avoid using software that's hard to use. "The human tendency is that if it's hard to use then you push it to the back burner. The easier we make our tools the better it is. The fewer clicks the better."

She's not alone in thinking that way. 64% of IT teams believe the harder a security solution is to use, the less likely it is to be effective, which is why 89% say ease-of-use is a significant consideration when buying security software.



89%

of IT teams say ease-of-use is a significant consideration when buying security software.

7 tips for reducing complexity

1. Consolidate vendors

Each new vendor increases your regulatory and compliance requirements, such as SOC2 reports. Each security tool typically requires its own management interface, configuration, and maintenance, and each new tool increases the potential for conflicts with other tools.

> ***"If I need to do ten different things and I need ten different tools, I have to know ten different tools. If I can do it in three, great!"***
>
> **Ryan Powell,** Senior Director, Information Technology, Malwarebytes

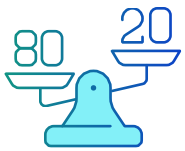
2. Make ease-of-use a requirement

When you're selecting new security tools, take time to understand how easy it is to deploy the tool, how easy it is to train your staff to use it, and how easy it is to operate. Keep in mind that the software is only as capable as features you know how to use, and the true cost of the software is the cost of the time it wastes.

3. Take time to understand and configure tools thoroughly

One cause of overly complex security stacks is buying tools to cover gaps in protection created by incomplete training or misconfiguration of existing tools. This can happen when the tools are first installed, or over time as IT environments change. Crystal Green, Malwarebytes Senior Director, Customer Success says "We see a lot of companies that purchase software but don't deploy or use it. Sometimes it doesn't get deployed at all, other times key features aren't used." The key, Green says, is to manage security tools as an ongoing process rather than a project.

7 tips for reducing complexity (continued)



4. Use the 80/20 rule

Computer networks are complex and ever-changing, so some complexity in security environments is inevitable. You can't eliminate it, but you can decide how much you're prepared to tolerate, and the Pareto principle, or 80/20 rule, is a good guide. Aim to make 80% of the things you do as close to "set it and forget it" as you can, so that you can focus on the 20% where it's impossible or unworkable to reduce complexity.

5. Get rid of legacy tech

Complexity grows when you add new tools that overlap with old tools, and the old tools aren't removed. Make removing legacy technology and paying down technical debt a small part of every project so that it doesn't become overwhelming.

6. Find a way to say "no"

OK, this is easier said than done, but if your life is spent firefighting because of complexity and technical debt, you will not firefight your way out of it. Nothing gets done without people or budget, and simplifying a complex environment can only happen while another project waits.

7. Use automation wisely

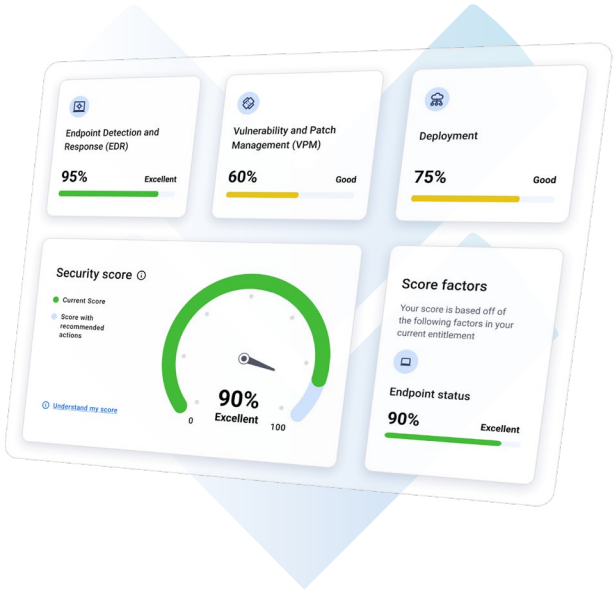
Automation can reduce complexity by simplifying processes and eliminating repetitive or predictable steps. However, be aware that automation often requires more up-front configuration, and that complexity for its own sake can increase complexity.

ThreatDown™ Powered by Malwarebytes

How ThreatDown reduces complexity

ThreatDown, powered by Malwarebytes, was designed to reduce complexity and costs while eliminating poor security outcomes. ThreatDown Bundles consolidate multiple technologies into an integrated bundle with one lightweight agent, managed from a single, intuitive console. By eliminating the time and effort needed to understand, manage, and optimize tools from multiple vendors, IT teams can focus instead on core business activities without blind spots from missed threats. Every ThreatDown Bundle includes Security Advisor, which provides a clear security score and guidance on how to instantly improve your protection levels.

For small or resource-limited organizations without the in-house skills required to effectively monitor, detect, and respond to cybersecurity threats, ThreatDown MDR, provides the always-on technology and expertise you need to maximize your threat protection without the significant investment required to build and maintain these capabilities internally.



ThreatDown Powered by Malwarebytes

How ThreatDown reduces complexity (continued)

We get it - security is hard. Security products shouldn't be.

ThreatDown Bundles bring together the capabilities you need in a single console with an intuitive interface. Every bundle includes Security Advisor with personalized guidance to take immediate actions that improve your security score.

Try ThreatDown Bundles today!

Let us take care of your endpoint security. Deploy the solution that delivers superior defense, easiest to use management, and the best value for your security investment.

Get started

What you get	Core	Advanced	Elite	Ultimate
Security Advisor	✓	✓	✓	✓
Incident response	✓	✓	✓	✓
Next-gen AV	✓	✓	✓	✓
Device control	✓	✓	✓	✓
Application Block	✓	✓	✓	✓
Vulnerability Assessment	✓	✓	✓	✓
Ransomware Rollback		✓	✓	✓
Endpoint Detection & Response		✓	✓	✓
Patch Management		✓	✓	✓
Managed Threat Hunting		✓		
Managed Detection & Response (includes threat hunting)			✓	✓
Website Content Filtering				✓
Add-Ons	✓	✓	✓	✓

What IT professionals say about ThreatDown

Ease-of-use is central to the way ThreatDown products are designed, why IT staff love them, and why users cite ease-of-use so often in their reviews.

"Easy to use product that just works!"

Blake R.,
IT Manager

"Streamlines everything into one place and makes it much easier for our small team to monitor and manage a large number of devices."

Daniel P.

"With an easy to view panel, ThreatDown let us have a clear sight of alerts on managed devices."

Marco C.,
Sys Admin

"MDR was very easy for us to implement ... Most threats are handled without needing to interact with us."

Tammy O.,
Senior Programmer/Analyst

"[ThreatDown] has an easy to use and navigate user interface. It is intuitive and easy to deploy."

Brett E., Small Business
(50 or fewer employees)

"Incredibly responsive and easy to use."

Micheal R.

"So easy to set up"

Tony D.,
Information Technology Specialist

"This product is excellent; easy-to-use: affordable; and most-importantly, effective."

Tech By Trade L.

"An effective product and an easy to use interface."

Brandon S.,
Systems and Applications Technician

Conclusion

IT teams simply don't have the bandwidth or specialist security skills to combat their increasingly sophisticated adversaries by adding more and more tools to their arsenal. Each new tool creates additional complexity and offers diminishing returns, until eventually security outcomes start to get worse, not better, while burning up ever more IT time.

Instead, organizations need to prioritize their IT team's limited time and resources by selecting comprehensive solutions that are easy to understand, simple to use, and tightly integrated. For organizations without the capacity to maintain a 24/7 security operations center (SOC), Managed Detection and Response (MDR) services can provide access to skilled security analysts who specialize in monitoring, investigation, and incident response around-the-clock.

Above all, IT teams should remember that their security stack is there to help them do their job, and needless complexity. With a methodical approach and the right technology choices, complexity can be tamed, costs reduced, and wasted time eliminated.

Talk to an expert

[1] Malwarebytes surveyed its VIP customers.

ThreatDown™ Powered by Malwarebytes | threatdown.com | corporate-sales@malwarebytes.com | 1.800.520.2796