Reducing Cyber Complexity

A Critical Approach for Prevention-First Cybersecurity

ESET®

Digital Security
Progress. Protected.

Table of Contents

Introduction

Software ate the world many years ago, and it will continue digesting it due to more novel developments such as the rise of AI. Sadly, software advancements will keep introducing critical business risks that organizations are already struggling to manage, with security teams finding their job much harder than it needs to be. The culprit? **Cybersecurity complexity**.

Even smaller businesses with nominally smaller IT footprints are not spared from the complexity conundrum. For example, widespread skills challenges make managing complex tools even harder. All the while remote working — commonplace among most businesses — can expand the attack surface and IT complexity in unpredictable ways through employee-owned devices and insecure home networks.

It's critical that IT and security teams find more effective and cohesive ways to cut through this complexity and manage the fast-moving, multi-vector threats facing them.

To address the issue, ESET compiled this white paper, offering essential insight into the top challenges organizations face as they battle cybersecurity complexity. And, most importantly, relaying some practical strategies and guidance for success.

Among other things, you will learn how the following can help **reduce cyber complexity**:

- AI and automation, which help upskill security teams and **reduce manual effort**, while increasing productivity
- Holistic, **multi-layered protection** delivered from a single platform to proactively tackle threats while expanding visibility into your environment
- **Outsourcing** some security operations (SecOps) to an expert third-party Managed Detection and Response (**MDR**) provider
- A **zero-trust approach** which can mitigate remote working and data access risks

80%

of companies

acknowledge that the use of multiple point solutions hampers their team's efficiency in detecting, responding to, and recovering from incidents.

Source: *2024 CISCO Cybersecurity Readiness Index, 2024.*

Tackling cyber complexity is one of the first stages of implementing a prevention-first approach to cybersecurity, designed to minimize cyber risk by dealing with ineffectively designed security processes, solutions, or even services.

The goal is to **create an effective security operation**, building up cyber resilience without ompromise.

Understanding Cybersecurity Complexity

What exactly does complexity mean in the cybersecurity context? There are various aspects to this. It could mean:

1. **Number and type of security tools** that IT teams must manage and the processes they need to work through to keep an organization safe.

2. Likewise, it could relate to the **distributed, heterogeneous IT systems** that they must defend — from mobile phones, through computers, to entire cloud networks stretched wide by remote working.

3. And of course, it can mean the **rapidly evolving threat landscape**, which many in-house security teams struggle to keep pace with.

In fact, one of the greatest challenges these often overstretched and under-resourced IT security professionals must face is the sheer speed at which new threat actor tactics, techniques, and procedures (TTPs) emerge.

What's more, their job is made much harder by having to work with **siloed data**, **difficult-to-use tools**, and **constrained budgets**, while facing an extensive and expanding attack surface.

What Does Cybersecurity Look Like?

All in all, complexity is a great enemy of cybersecurity. Hence understanding how it can impact a typical business is the first step towards defeating it. It can be mostly encountered in:

MULTIPLE TOOLS AND SOLUTIONS

Cybersecurity is often treated as an afterthought by business leaders. That's unfortunate because reactive spending following an incident or a breach is usually piecemeal and leads to investment in point solutions which only have a single use case.

So rather than **solve the underlying cause of a breach**, these solutions may focus only on one aspect of the security stack, making the IT team's day-to-day tasks harder. This pushes security teams to operate "swivel-chair" environments, having to constantly flit between different screens and management portals.

Medium businesses with 1-5 thousand seats have on average

51

solutions

in use across their organization.

Source: *Pentera: The State of Pentesting Survey 2024*.

Large businesses with 10 thousand seats have on average

58

solutions

in use across their organization.

Source: *Pentera: Tje State of Pentesting Survey 2024*.

Be that as it may, threats invariably hide in the interoperability and visibility gaps that these tools create. Plus, much of IT's time is spent learning new tools rather than solving important problems. The average business reportedly runs dozens of security solutions, with most planning to increase the number of vendors in their stack over the coming years.

SECURITY TOOL COMPLEXITY

There aren't just too many security tools. Often, the tools that businesses do have in place are too complex, with unintuitive interfaces or poor workflows. This can **erode the productivity** of already understaffed teams and mean that IT practitioners are **unable to optimize all the features** at their disposal.

In some other cases, enterprise-grade solutions like SIEM are purchased but left largely untouched because the company can't devote the required resources to configuring and managing them on an ongoing basis.

REMOTE WORK AND BYOD (BRING YOUR OWN DEVICE)

Complexity extends beyond an organization's security tooling. Today, more businesses than ever benefit from the flexibility that remote working affords their employees. In the US, around a third of employees in professional, managerial, and related occupations work from home.

This usually means happier, more productive staff and potentially even lower building/office costs. But it also exposes these same organizations to extra cyber risk.

Remote working means employees could be logging in from unprotected or unpatched devices and laptops, potentially from insecure home or public networks. This could **imperil corporate passwords and provide an unguarded attack path** for threat actors to reach company networks and data.

73%

of VP & C-suite IT leaders

believe remote workers pose a greater risk than onsite employees.

Source: *OpenVPN: OpenVPN Quick Poll Remote Workforce Cybersecurity, 2024*.

Protecting this distributed computing environment may add extra management overheads and headaches, especially when considering the number of different internal and external devices a company has to monitor at once.

A RAPIDLY EVOLVING THREAT LANDSCAPE

The threat landscape is in constant flux. As network defenders and security vendors continue to build protections, their adversaries work out new ways to bypass them in a never-ending arms race. Threat actors have the advantage of surprise and need only be lucky once to penetrate a corporate network or data store.

They have plenty of avenues to do so, thanks to ongoing investments in cloud infrastructure and software, APIs, and other digital technologies, opening new avenues for an attack.

The number of **newly discovered** common vulnerabilities and exposures (**CVEs**) has hit record highs over the past several years, while new AI-powered TTPs are predicted to increase the volume and impact of attacks like ransomware. Complex supply chains introduce extra opportunity for adversaries to reach their targets, and stolen passwords remain an Achilles heel. The use of stolen credentials has featured in almost a third (31%) of breaches over the past decade, all of which can be a challenge for even well-resourced enterprises to manage.

93%

of companies

have suffered a cybersecurity breach because of weaknesses in their supply chain / third party vendors in 2023.

Source: *WSJ Pro Cybersecurity Research: Third-Party Cyber Risk Management Primer*.

The number of unique exploit

detections increased by

68%

over the past five years, indicating a diversification of attack methods.

Source: *Fortinet: Global Threat Landscape Report, 2023*.

CYBERSECURITY SKILLS SHORTAGES AND GAPS

Another problem for small and mid-market businesses is that they rarely have sufficient numbers in their IT team dedicated to cybersecurity. The global cybersecurity workforce gap now stands at nearly five million, up 19% annually. Smaller organizations unable to match the salaries of their larger peers often miss out on talent.

These skills shortages are exacerbated by budget constraints which can hit SMBs harder than large enterprises, and labor-intensive security tooling and processes which eat away at productivity. **Overburdened staff** are also more likely to make mistakes. Skills gaps are another problem.

Just a quarter (26%) of hirers surveyed by ISACA believe at least half of their applicants are well qualified, with cloud computing (47%) and security controls (35%) two of the top three areas for skills gaps.

As technology continues to advance and become more complex, the danger is that **IT security skills will not keep pace**, giving threat actors a further advantage.

DATA OVERLOAD

From a SecOps perspective, the **large number of point solutions** many organizations run **can spit out data and alerts** at an overwhelming rate, submerging analysts to the point where they're unable to prioritize with any accuracy.

This can lead some teams to waste time on false positives while allowing false negatives to sneak through and cause damage. It can also lead to stress and burnout, turning the heat up further on those remaining colleagues. Half of cybersecurity professionals claim to have experienced burnout and 65% have considered leaving their jobs due to stress.

47%

of digital workers

struggled to find the information they need to effectively perform their jobs due to increasing number of applications used in the workplace in 2023.

Source: *Gartner Press Release, Gartner Survey Reveals 47% of Digital Workers Struggle to Find the Information Needed to Effectively Perform Their Jobs, 2023*.

46%

of respondents

with cybersecurity job responsibilities described the current staffing of their organization's cybersecurity team as 'somewhat understaffed' in 2023.

Source: *ISACA's Global Cybersecurity State Report 2023*.

Prioritizing Prevention to Beat Complexity

Tackling this kind of complexity isn't easy. But with a **prevention-first approach** as a guiding principle, it's within the reach of any business. Why does prevention make most sense?

Because by focusing on building resilience into systems through **better cyber-hygiene**, **blocking threats outright**, and **rapidly detecting and containing** any that sneak through, organizations stand the best chance of mitigating risk before it escalates. It's about enhancing the first line of defense, because prevention is always better (and cheaper) than a cure.

However, prevention requires robust but simple-to-operate security which is heavily automated, out-of-the-box ready, maintenance-free, and designed with SMBs in mind — with a price tag to match. In short, it should favor **simplicity over complexity**. With this in mind, here's how to tackle the complexity challenges cited above:

TOOL CONSOLIDATION A simple answer to tool bloat is to consolidate prevention-first security onto a single platform from a trusted provider. This is what the **ESET PROTECT** platform offers, for example. From a single pane of glass, it protects the entire IT environment, from endpoints and servers to mobile devices, cloud applications, and email.

It's about delivering prevention, detection, and proactive threat hunting from one location — closing security gaps and reducing the workload for under-pressure IT teams. There are also seamless integrations with third-party products that further expand the value of the platform, reducing the need to operate "swivel-chair" environments.

Additionally, multilayered technologies including HIPS, Advanced Memory Scanner, UEFI Scanner, Deep Behavioral Inspection, Botnet Protection, and DNA Detections work together as **ESET LiveSense**. They perform a wide range of functions from a single platform: blocking malware, flagging suspicious behavior, and protecting against botnets and UEFI firmware threats, among other things.

SIMPLIFIED USER INTERFACE Cybersecurity tools aren't all complex to use. **ESET PROTECT** prioritizes user-friendly design and a consistent look-and-feel across a huge sweep of its capabilities. Deployment is child's play thanks to its cloud-based design, the admin console can be accessed from any device, anywhere, and dashboards and

reports can be customized to any organization's requirements. A high degree of built-in automation further streamlines the user experience, while AI features like **Incident Creator** or the **ESET AI Advisor** streamline the work of SecOps analysts.

ZERO TRUST APPROACH When it comes to distributed, cloud, and mobile-based IT environments, **Zero Trust** is the best approach to mitigate risk. It's an idea based on one thing – don't trust anyone by default. This approach involves frequent verification of all users and devices, implementing least privilege access policies, network segmentation, continuous monitoring, strong encryption, and more.

Zero Trust works to maintain strict access controls, as it's designed to reduce the chances of bad actors reaching corporate networks and cloud resources, minimizing their ability to perform malicious actions if they do get in.

ESET PROTECT offers multiple capabilities to support Zero Trust, from Integrated Security Management and Endpoint Protection to Full Disk Encryption, Cloud Sandbox, Cloud App Protection, and more. **ESET Secure Authentication** is another key component; supporting seamless multifactor authentication (MFA).

MANAGED DETECTION & RESPONSE (MDR) Cyber-skills shortages are difficult to plug without wholesale and long-term action from governments and educators. However, one thing organizations can do to mitigate the challenge is to outsource aspects of their operations where there are high-value but cost-effective alternatives.

ESET PROTECT MDR offers just such an option. It removes the need for expensive investment in SecOps technology and outlays on staffing and ongoing training. Even better, it ensures expert ESET analysts well-versed in the latest ESET research and threat intelligence are always watching customer environments, 24/7/365, with continuous threat hunting and monitoring, while internal IT personnel can focus on other important priorities.

What's more, it can bring down threat detection times from the usual 277 days (or 16 hours for a professional SOC) to just below 30 minutes – massively lowering the chances of a data breach and its long-term complications.

PROACTIVE DEFENSE Threat actors might seem to hold all the cards. But by deploying AI in the cloud, on the endpoint, and across the network, organizations can trawl through vast volumes of data — proactively spotting suspicious behavior and containing threats before they have a chance to make an impact.

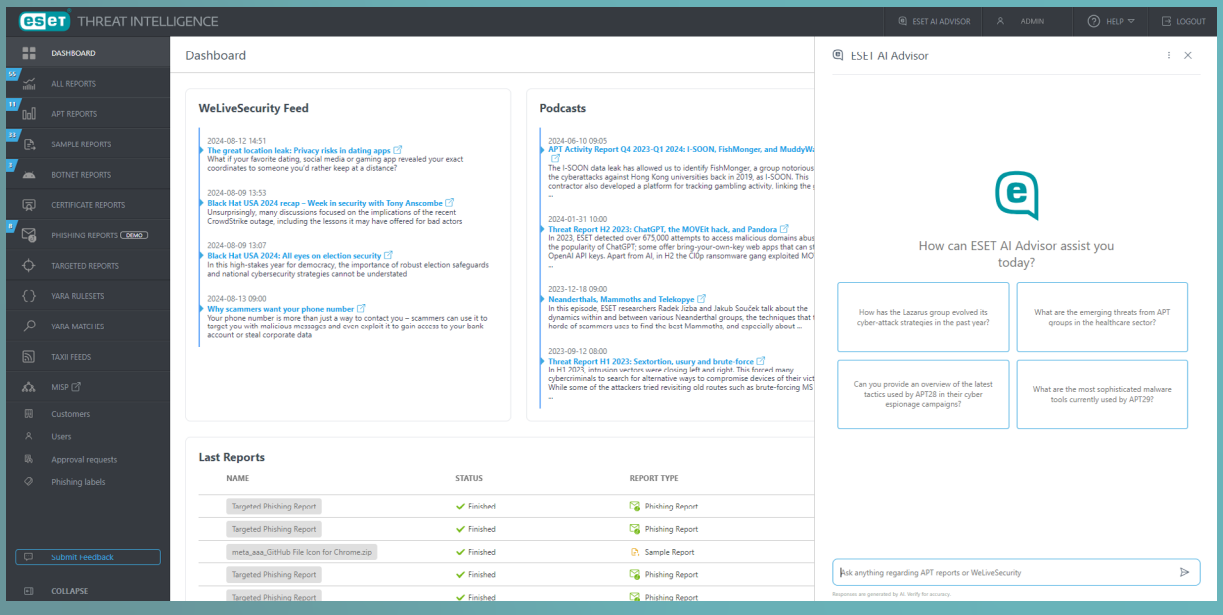
This is what **ESET PROTECT** achieves by combining the customer's telemetry with the

ESET Threat Intelligence from the company's world-renowned experts, delivering unique global insights on all endpoints in the network.

AUTOMATION & AI In fact, AI and machine learning (ML) can play an outsized role in minimizing cybersecurity complexity for businesses. When it comes to the data and alert overload impacting many SecOps analysts, Generative AI (GenAI) assistants can deliver intuitive insights from large volumes of data, enabling better prioritization of alerts and informed decision-making.

That's what **ESET AI Advisor** does—integrating seamlessly into day-to-day workflows to help SecOps teams optimize their use of **XDR** and threat intelligence. In so doing, it also helps to close potential skills gaps in the function by interacting with analysts in natural language.

Intelligent automation, often driven by AI, can also reduce workload for security teams by taking care of manual, toilsome tasks like patching and incident remediation. **ESET PROTECT** is packed with automated workflows to reduce human error, improve security outcomes, and focus limited staff resources on the jobs that matter — all while minimizing cyber complexity. It can reduce the need to even log into the platform for many IT administrators.



Picture 1: *Integration of ESET AI Advisor in the ESET Threat Intelligence console.*

Conclusion: Simplicity Drives Results

Most ambitious businesses are laser-focused on sustainable growth, but that can only be achieved if they build on secure and solid foundations. The sophistication of modern threats and the complexity of companies' own IT systems and security infrastructure make this more challenging. Skills shortages and security gaps further compound the problem.

This represents a potentially significant threat to their business. A PwC report claims that cyber complexity could lead to data breach-related financial losses, an inability to innovate, and diminished operational resilience.

Simplification should therefore be a priority for IT leaders. Fortunately, there's plenty of low-hanging fruit to go after. By consolidating prevention, detection, and proactive threat hunting onto a single, intuitive, and highly automated platform like **ESET PROTECT**, IT teams can strip away complexity and optimize in-house resources.

They can also turn to a managed service like **ESET MDR**, and reduce the complexity of their security operations even further. By getting on the front foot in this way, they'll be able to block most threats outright, and quickly catch and contain the rest.

ESET PROTECT is your one-stop shop for this type of prevention-first approach. It not only decreases the complexity of management, but also delivers rock-solid support — offering all you need for today, and a secure platform for outsourcing XDR and building Zero Trust initiatives for tomorrow. In short, it's a streamlined roadmap for a simpler, more secure future.

Explore the benefits of MDR services from ESET that combines AI and human expertise to achieve unmatched threat detection and rapid incident response, and removes the need to maintain in-house security specialists.

LEARN MORE

This is ESET

Proactive defense. Our business is to minimize the attack surface.

Stay one step ahead of known and emerging cyber threats with our **prevention-first approach**, **powered by AI and human expertise**.

Experience best-in-class protection thanks to our in-house global **cyber threat intelligence**, compiled and examined for over 30 years, which drives our extensive R&D network led by **industry-acclaimed researchers**. ESET protects your business so it can unlock the full potential of technology.

Multilayered, prevention-first

Cutting-edge AI meets human expertise

World-renowned threat intelligence

Hyperlocal, personalized support

eset
Digital Security
Progress. Protected.