# Reimagining Cybersecurity with AI

## Balancing Automation, Expertise, and Resilience

ESET Cybersecurity
Progress. Protected.

Artificial intelligence (AI) is increasingly becoming a tool that can help organizations work more efficiently. It helps with automating repetitive tasks and improve decision-making. Yet the same technology is also enabling adversaries to scale attacks and make cybercrime more accessible.

# AI is not the enemy

The challenge and real risk for organizations lies in adopting AI without adequate security controls, governance, and visibility needed to manage it safely. As AI becomes embedded in everyday business operations, cybersecurity teams must learn to manage it as a new operational layer of security.

AI is both an attack amplifier and a defense accelerator. Organizations that understand this balance will be far better equipped to strengthen resilience and capitalize on AI's benefits without introducing unnecessary risk.

# 1. The AI-powered cybersecurity reality

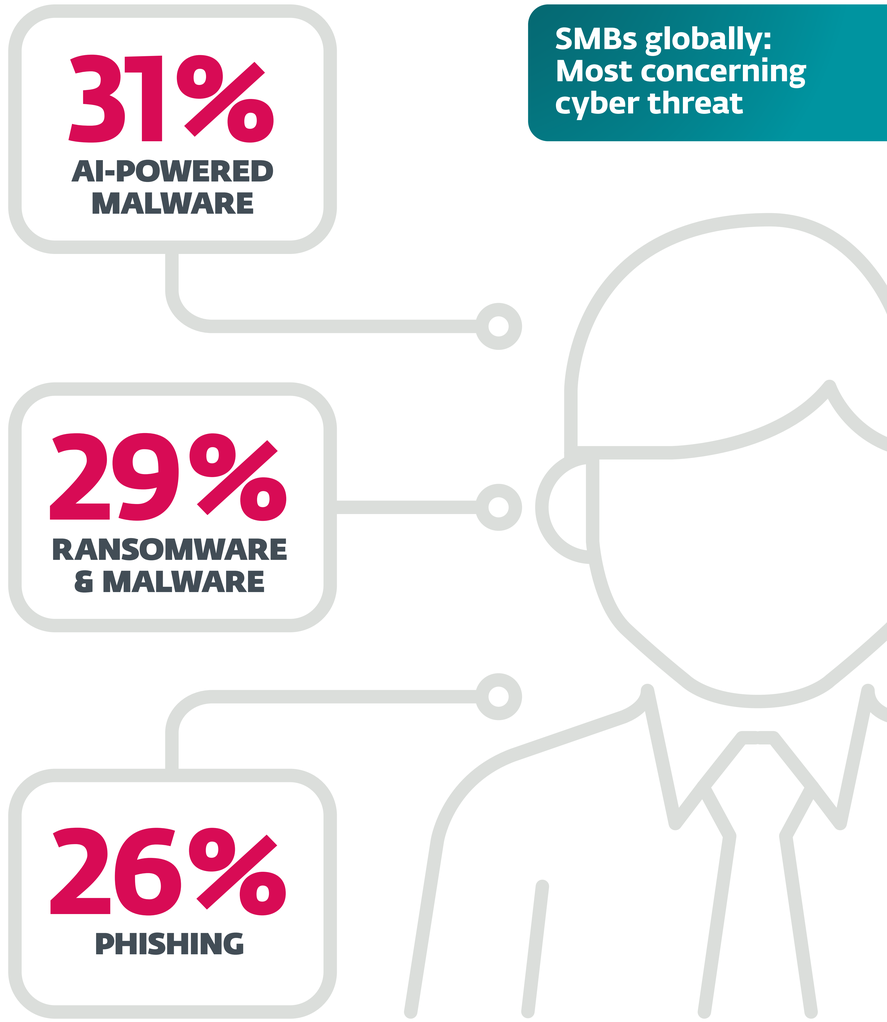
## What has changed?

AI has fundamentally altered the economics of cybercrime. Activities that once required specialist skills can now be performed faster, at lower cost, and at greater scale. ESET research shows that AI more often automates reconnaissance, creates convincing phishing messages, or generates deepfake content. It also accelerates malware development and boosts the effectiveness of social engineering campaigns that can severely compromise cybersecurity.

The most significant impact of AI today is the automation and acceleration of existing attack techniques, particularly social engineering and phishing campaigns, which is well documented in ESET SMB Cyber Readiness Index 2026.

This shift is already shaping business concerns. Our data highlights that **AI-powered malware is regarded as the most concerning cyber threat by 31%** of SMBs globally, ahead of **ransomware, malware (both 29%)**, and **phishing (26%)**.

At the same time, AI is becoming an important defensive capability. Our data also show that organizations increasingly want to leverage AI to **anticipate threats before they occur (32%)**, **identify attacks faster (24%)**, and accelerate incident mitigation. AI-powered automation, threat intelligence, and security analytics can help defenders process massive volumes of data and focus attention on the incidents that matter most.



## What has not changed?

Despite the AI revolution, the fundamentals of cybersecurity remain remarkably consistent.

The Cyber Readiness Index found that **phishing remains the leading cause of cybersecurity incidents at 26%**, followed by **unpatched vulnerabilities at 23%**, **lack of security monitoring reaching 22%**, and **weak passwords hitting 20%**.

ESET telemetry also shows that phishing continues to dominate real-world threat activity and remains the most frequently detected email-based threat category.

The lesson is clear: AI has changed the speed and scale of attacks, but attackers still rely heavily on familiar weaknesses. Human error, poor cyber hygiene, inadequate visibility, and misconfigured systems remain among the most common pathways to compromise.

**26%**
**PHISHING**


**23%**
**UNPATCHED VULNERABILITIES**

**22%**
**LACK OF SECURITY MONITORING**

**20%**
**WEAK PASSWORD**

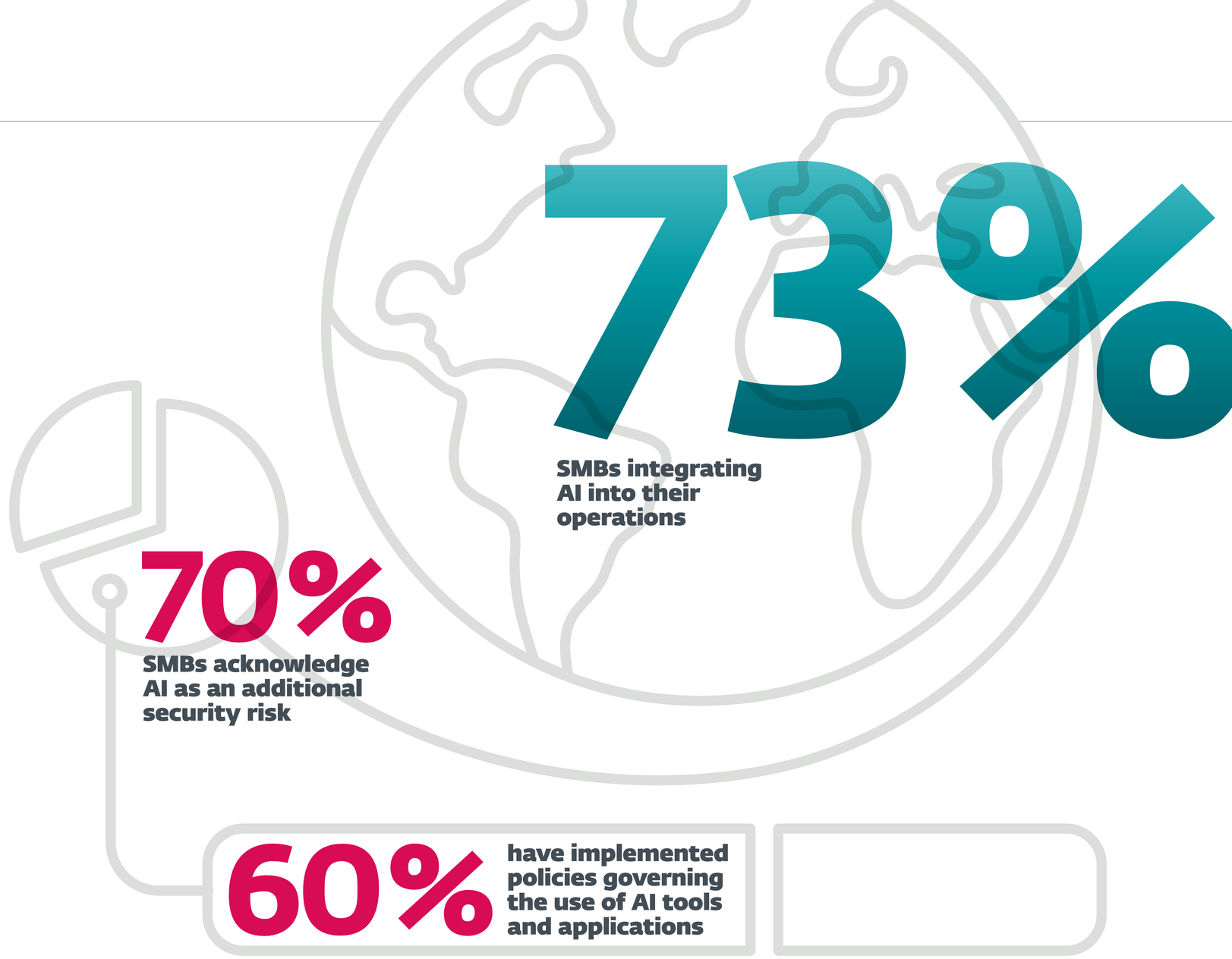
## The AI readiness gap

Organizations are rapidly embracing AI. Globally, **73% of SMBs report integrating AI into their operations**. Yet AI adoption doesn't always translate into AI preparedness.

**While 70% of organizations acknowledged that AI introduces additional security risks, only 60% have implemented policies governing** the use of AI tools and applications.

This disconnect highlights a growing AI readiness gap. Many organizations recognize the risks associated with AI but have yet to establish the governance, oversight, and controls needed to manage them effectively.

As AI becomes further embedded into business processes, closing this gap will become a critical component of cyber resilience.



# 2. How businesses unintentionally increase cyber risk with AI

**MISTAKE 1:**

## Treating AI as an IT project

AI adoption affects the entire organization. Decisions around data sharing, compliance, procurement, and employee behavior all influence cybersecurity outcomes.

Organizations that treat AI solely as a technology initiative often overlook the governance and oversight needed to manage risk effectively.

**MISTAKE 2:**

## Allowing shadow AI to flourish

Employees increasingly use publicly available AI tools to improve productivity. While this can deliver clear business benefits, unmanaged use can expose sensitive information and create unnecessary risk.

Our data show that despite widespread adoption of AI technologies, 40% of SMBs still lack formal AI policies governing which tools can be used and how they should be used.

**MISTAKE 3:**

## Focusing on the wrong threats

Many organizations have become highly concerned about AI-powered malware. Yet ESET research indicates that organizations are **far more likely to experience incidents caused by phishing**, weak passwords, insufficient monitoring, or unpatched vulnerabilities.

Focusing exclusively on emerging AI threats can distract organizations from addressing the attack vectors that continue to drive the majority of real-world incidents.

MISTAKE 4:

## Trusting AI-generated content

Generative AI can produce highly convincing communications, emails, chat messages, and synthetic content. As these capabilities improve, distinguishing authentic content from manipulated content becomes increasingly difficult.

Organizations that assume digital communications can be trusted by default may find themselves vulnerable to sophisticated phishing, impersonation, and fraud.

MISTAKE 5:

## Neglecting employee preparedness

Technology alone can't solve cybersecurity challenges. People continue to play a significant role in cyber incidents, which makes awareness and training just as important as technology.

Encouragingly, 87% of SMBs consider cybersecurity training important or very important, highlighting growing recognition of the role employees play in resilience.

MISTAKE 6:

## Believing AI can replace cybersecurity expertise

Although AI is a powerful force multiplier, it's hardly a substitute for human judgment. ESET's AI strategy explicitly incorporates human expertise into detection, analysis, and response workflows because experienced analysts provide context, validation, and decision-making capabilities that automation alone can't deliver.

Organizations that view AI as a replacement for expertise risk creating dangerous blind spots.

# 3. Building cyber resilience in the age of AI

Cyber resilience is about maintaining business continuity, responding effectively when incidents occur, and recovering quickly without significant disruption. To achieve this, organizations should focus on four core pillars.

## Pillar 1: Visibility

**Organizations can't secure what they're unable to see.**

Visibility begins with understanding which AI tools are being used, where business data flows, who has access to sensitive information, and how systems interact across cloud and on-premises environments.

Comprehensive monitoring and threat intelligence, together with visibility across endpoints, identities, and workloads are **essential for identifying risks before they evolve into incidents**.

## Pillar 2: Protection

**Effective protection starts with fundamentals.**

Organizations should strengthen several foundational controls. The essential ones include endpoint security, identity protection, email security, vulnerability management, and access controls. AI governance must also become part of the protection strategy by establishing clear policies governing approved tools, data handling, and acceptable use.

Well-designed cyber resilience highlights the importance of identity security, exposure reduction, and disciplined cyber hygiene as foundational controls.


## AI is part of the answer, resilience is the goal.

Explore Cyber Resilience by Design for practical guidance on building resilience across people, processes, and technology.

READ THE PAPER

## Pillar 3: Preparedness

### Employee preparedness is a vital part of cyber resilience strategy.

Providing regular training focused on AI-generated phishing, deepfake scams, impersonation attempts, and emerging forms of social engineering is also crucial part of being prepared. Otherwise, organizations are risking being compromised through one of the most significant blind spots out there.

Preparedness also includes conducting tabletop exercises, validating response procedures, and ensuring stakeholders understand their roles and responsibilities during a cyber incident which core competencies necessary for managing any crisis.

## Pillar 4: Response

### Even mature organizations should assume that incidents will occur.

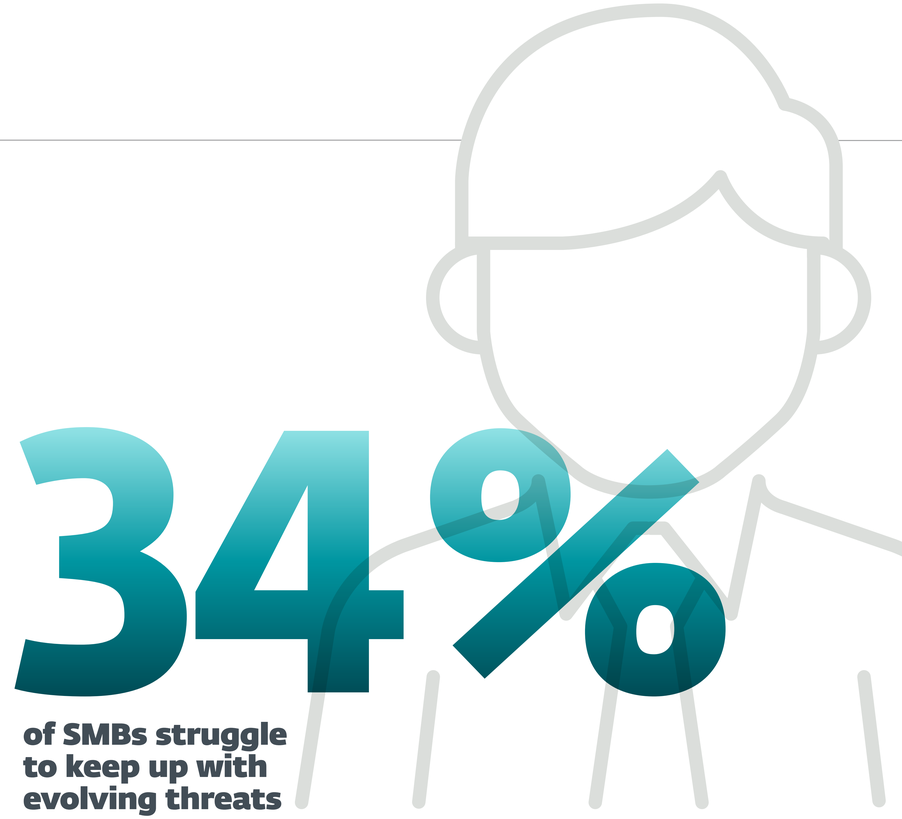
Preparedness is an essential for effective response capabilities, which rely on rapid detection, investigation, containment, and recovery. Being prepared means being able to respond seamlessly and effectively.

ESET SMB Cyber Readiness Index found that keeping up with evolving threats and emerging technology **remains among the biggest cybersecurity challenges** facing SMBs today.

This is where AI can serve as a meaningful force multiplier by helping teams analyze events faster, reduce alert fatigue, and prioritize response activities. Most importantly, the future of cybersecurity is human expertise amplified by AI. That's one of the key takeaways one should focus on when building cyber resilience in the age of AI.

# 4. ESET as a force multiplier for cyber resilience

Turning the principle of human expertise amplified by AI into reality requires a balanced approach, one that combines the speed of AI with the experience and judgment of human experts. That can help addressing various challenges and internal struggles.




## The challenge

Expanding attack surfaces combined with growing complexity, limited resources, skills shortages, and rapidly evolving AI-driven threats are all crucial aspects of today's cyber security world.

Keeping pace with this environment can be difficult, particularly for SMBs that may not have large security teams or **dedicated security operations centers** (SOCs).

## Why internal teams struggle

The reality is that many organizations can't maintain 24/7 monitoring, continuous threat hunting, and rapid incident response capabilities internally.

ESET research shows that **34% of SMBs struggle to keep up with evolving threats**, while 32% cite keeping pace with emerging technologies such as AI as a key challenge. Budget constraints (24%), complexity and integration challenges (21%), and cybersecurity skills shortages (20%) further compound the problem.

At the same time, organizations are being asked to improve in many areas. Strengthening governance and improving cyber resilience are among the top. Integrating AI safely into daily operations is another pressing challenge, often complicated by both real and perceived barriers.

# The ESET approach

ESET approaches cybersecurity as a continuous process. This effortless and fully supervised approach brings together the speed and scale of AI with the judgment and experience of human experts, helping make advanced cybersecurity more accessible to organizations of all sizes.

ESET's AI strategy is built upon proprietary security-focused AI models, a layered AI security architecture, and continuous innovation designed specifically for cybersecurity use cases.

Through our ongoing AI security research, we've analyzed roughly 1.1 million AI skills and identified thousands that warranted further investigation, including many considered suspicious or malicious. To help organizations assess these emerging risks, ESET offers AI Skill Checker, **a free tool that analyzes AI agent skills and plugin URLs** in real time to detect hidden malicious activity, unsafe payloads, and excessive permissions before installation.

At the same time, ESET continues to expand the role of AI wherever it can reduce complexity, improve decision-making, and help security teams respond faster.

By combining AI innovation with expert oversight, ESET aims to make enterprise-grade cybersecurity capabilities easier to access. This also means better management with more benefits, regardless of an organization's size or security maturity.

# Why MDR matters

Cyber resilience depends on more than technology alone. It requires continuous monitoring accompanied with expert analysis and followed by rapid response. Together, this creates the ability to act before threats cause business disruption.

ESET Managed Detection and Response (MDR) combines **AI-powered automation, global threat intelligence, expert-led threat hunting, continuous monitoring, and immediate response** capabilities into a 24/7 service designed to help organizations detect, investigate, contain, and remediate threats quickly.

By combining machine-scale analysis with human expertise, ESET MDR helps organizations bridge skills gaps and improve visibility. It also strengthens detection capabilities and supports cyber resilience without requiring large internal security teams.

The goal is simple: to make expert-led, AI-enhanced security available to more organizations, enabling them to achieve stronger cyber resilience with less operational burden.

As cyber threats and AI capabilities evolve in tandem, resilience must become a business imperative. The future belongs to organizations that proactively adapt to this shifting landscape.

With an effortless supervised approach that unites intelligent automation and expert oversight, cyber resilience becomes more attainable for everyone. Ultimately, this balance turns complex security challenges into a manageable reality, ensuring your organization remains secure, adaptable, and prepared for whatever comes next.

# This is ESET

ESET® protects organizations, critical infrastructure, and individuals, empowering them to be digitally resilient and confident in a world increasingly shaped by AI. Headquartered in the European Union and privately owned, ESET develops proprietary AI-driven cybersecurity technologies and independent AI models engineered to protect both digital infrastructure and the broader AI technology stack.

Every solution ESET builds is shaped by more than 35 years of cybersecurity expertise, over 25 years of AI innovation, and reflects the real-world experience, expert judgment, and human values that guide our decisions. We take a preemptive approach, securing against both conventional and AI-driven cyber threats. Grounded in scientific rigor and powered by 11 global R&D centers, ESET continuously advances research and drives innovation to deliver effortless cybersecurity with expert human oversight. Our technologies are consistently validated by leading independent analyst houses and testing labs.

ESET safeguards millions of users and organizations across 178 countries. Committed to responsible AI and customer trust, we protect the progress that technology enables.

For more information, visit www.eset.com
or follow our social media, podcasts, and blogs.



Cybersecurity
**Progress. Protected.**