

Lenovo Work Reborn Research Series 2025

# Reinforcing the modern workplace.

How to confidently assess and combat AI threats as you transform your digital workplace.

**Smarter  
technology  
for all**

**Lenovo**

# Prepare your workplace for anything.

To supercharge employee productivity with AI, IT leaders must transform the digital workplace. But as security threats evolve, they also need to transform their defenses to make sure nothing stops their progress.

In our first Work Reborn report, we lifted the lid on how productivity and employee engagement are among IT leaders' most urgent priorities. By creating a more dynamic, AI-enhanced and personalized working environment, leaders enable employees to focus on what they do best: creative problem solving and human collaboration.

We also revealed that IT leaders understand the need for fundamental digital workplace

transformation to harness AI's productivity promise. Working environments must be reinvented for AI to support individual needs, and IT support must be rethought to deliver seamless, uninterrupted employee experiences.

Now, we investigate another vital pillar of digital workplace transformation for the age of AI: cybersecurity.

The advance of AI has given rise to new threats from both external actors and internal sources. Our latest survey of 600 enterprise IT leaders reveals which of these AI security concerns are keeping them awake—and those they might be underestimating.

We believe that a two-pronged response is necessary for reinforcing the modern workplace. First, companies must escalate their efforts to detect new, adaptive AI-powered threats. Second, they must reinforce their security operations by harnessing AI itself to protect their most valuable assets.

This report outlines the path for IT leaders to evolve their defenses and embed AI in the heart of their cybersecurity architecture, enabling value-driving transformation in today's AI-powered work environment.

Hope you enjoy the report.

Rakshit



**Rakshit Ghura**

Vice President & General Manager  
Lenovo Digital Workplace Solutions



# Transform your workplace without security disruption.

Our research reveals how organizations must evolve their cybersecurity defenses for the age of AI.

Click to jump to section:



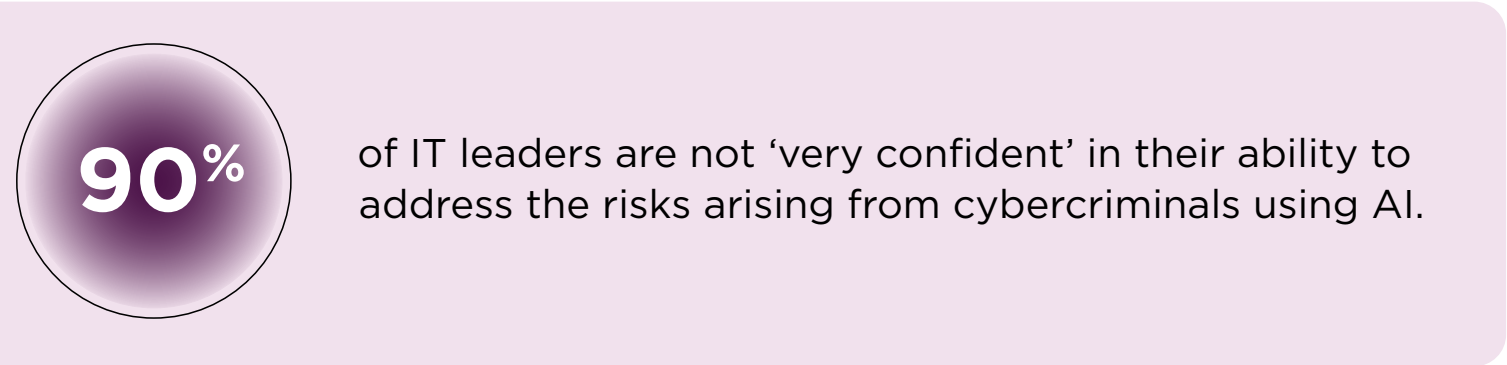
ASSESS

# Identifying new AI threats.

IT leaders are rightly concerned about the risks posed by AI—but they’re not all confident they can defend against them.

## Understanding risks from external threats.

IT leaders are alert to the cybersecurity risks that emerge from AI. They are especially worried about the threat posed by cybercriminals using AI, with over six in 10 acknowledging this as a growing source of cybersecurity risk.

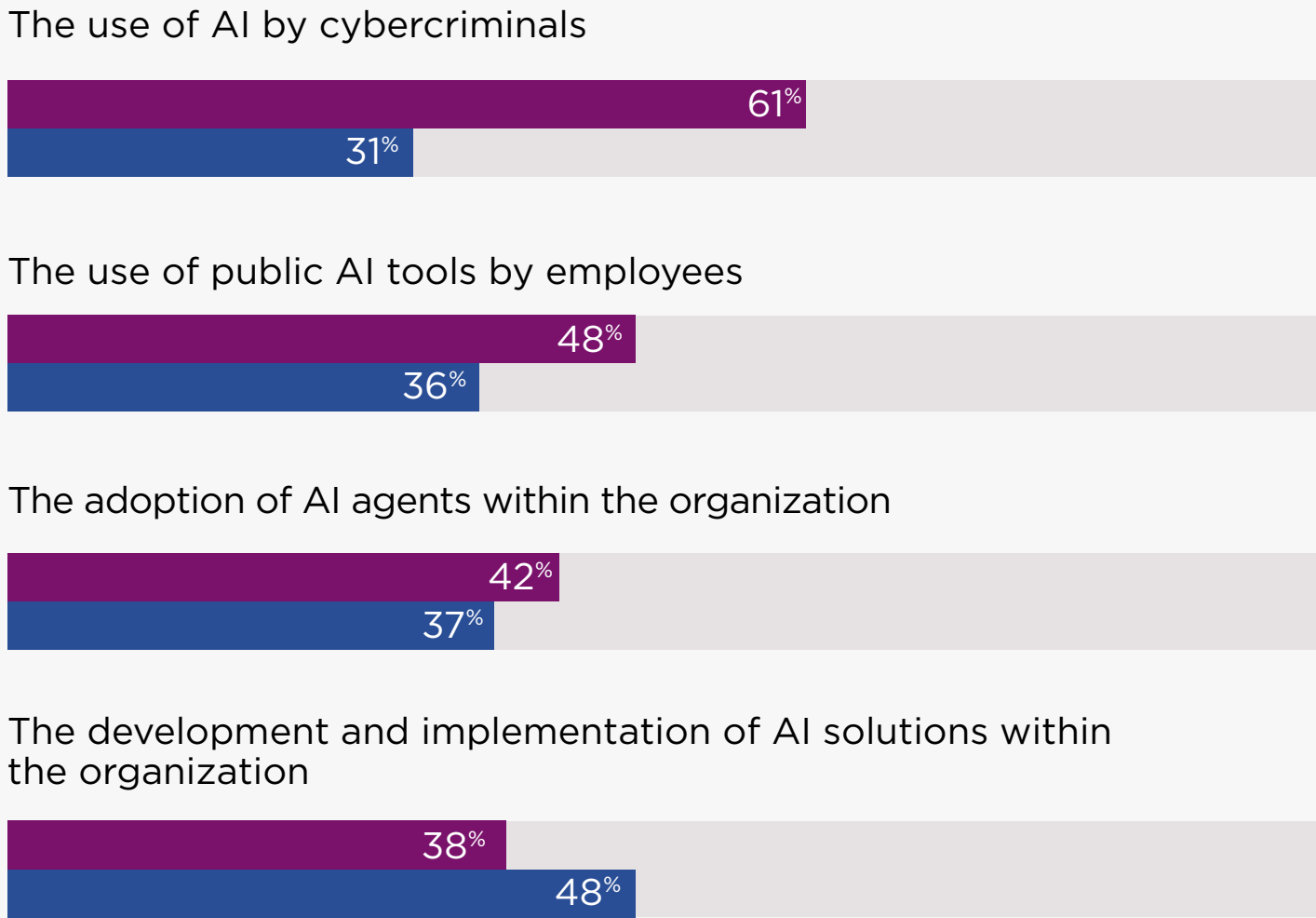


IT leaders are certainly right to be concerned about the use of AI by cybercriminals. Rather than replacing traditional tactics, AI amplifies them—helping attackers bypass detection systems with more accelerated and dynamic methods.

Modern AI-generated attacks can evolve in response to the defense mechanisms they encounter. They can mimic benign behavior, and they can be spread across multiple domains: cloud, devices, applications and more.

## Where cybersecurity risks are growing vs IT leaders’ confidence in addressing them:

- % reporting ‘significant’ or ‘moderate’ increase in cybersecurity risk
- % ‘very’ or ‘somewhat’ confident in their ability to manage risks







## ASSESS

# Addressing internal AI threats.

Identifying AI-powered attacks from external sources is just one dimension of the broader AI security challenge.

### More than six out of 10



IT leaders agree that AI agents pose a new kind of insider threat that they are not fully prepared to face.

### Seven in 10



agree that the misuse of AI by employees is a risk that they must address.

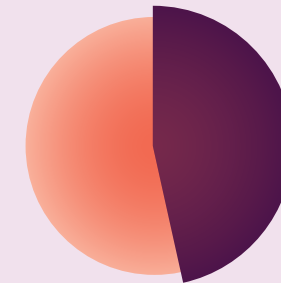
### Less than four in 10



are confident in their ability to manage either of these risks.

AI is evolving rapidly, and the associated cybersecurity implications are only now starting to become clear. This extends to the protection of AI itself—including models, training data and prompts—which is another primary security objective for IT teams.

But while confidence is low when it comes to defending against AI-enabled attacks from external sources, IT leaders feel more assured in their ability to manage risks coming from internal AI initiatives.



### Nearly half (48%)

of IT leaders feel ‘very’ or ‘somewhat’ confident in their ability to manage risks coming from the development and implementation of AI solutions within the organization.

If organizations have adopted the cybersecurity measures required to secure internal AI systems, this confidence may be well-placed. But it could be that some are underestimating the risks.

“IT leaders are focused on the race to implement multiple AI initiatives—but this can cause them to overlook the potential threat vectors arising from their deployment.”



**Tiago Da Costa Silva**

Security Services Director  
Lenovo Digital Workplace Solutions





## ASSESS

# New risks call for new approaches.

Traditional cybersecurity capabilities are not sufficient to address AI-related risks.

IT leaders must ensure that their cybersecurity capabilities are keeping pace with AI-related risks. And in many cases, these risks call for fundamentally new approaches to security.

For example, conventional data protection measures—limiting access to data based on an individual’s role—are no longer sufficient when an AI system is scanning multiple documents to find the answer to an employee’s question.

And traditional approaches to endpoint security—such as antivirus—can only spot threats once they have been identified and defined. AI allows malicious code to be created far faster than ever before. And it makes it easier for attackers to create polymorphic malware, which mutates to avoid detection and blends in with normal activity.

In the face of these new risks, businesses must upgrade their capabilities and step up protection for their most valuable assets.

“Generative AI’s ability to create polymorphic attacks has given adversaries an asymmetric edge, enabling faster, more evasive attacks that blend into normal activity and evade traditional detection mechanisms. Even with Zero Trust in place, defenders must assume, and prepare for, detections to fail.”



**David Majernik**

Senior Offering Design Technologist  
Lenovo

### AI cybersecurity risk factors.

Emerging threats to be aware of:

- Model poisoning/data poisoning
- AI model manipulation
- AI data privacy leakage
- Over-permissioned AI access
- AI adversarial inputs
- AI-driven malware
- Denial of service via AI workload exhaustion
- AI hallucinations and misinformation
- Data leakage via AI applications
- Shadow AI usage
- AI supply chain risks
- Bias and ethical risks leading to regulatory non-compliance
- AI-powered brute-force attacks

ASSESS

# Assessing your defensive abilities.

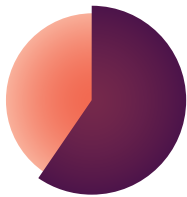
IT leaders understand the importance of data protection and vulnerability management, identifying them as the two most important cybersecurity capabilities to defend against AI-related threats. But they are not all certain that their capabilities are up to the task.

Confidence is lacking.



**Over half (54%)** of IT leaders feel that their data protection tools, processes and staff capabilities are not fully sufficient to address AI-related cybersecurity threats.



Even fewer are confident of their vulnerability and threat analysis capabilities.



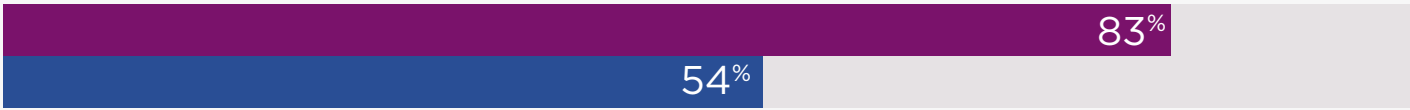
**65%** believe their current capabilities are not fully sufficient to tackle AI threats.

And the majority also believe the same of their abilities across both incident detection and response, and identity and access management.

## Capabilities which IT leaders think are important vs capabilities in which they are confident:

-  % **'critical' or 'high importance' in tackling AI risks**
-  % **current capabilities not fully sufficient to address AI risks**

Data protection



Vulnerability and threat analysis



Incident detection and response



Identity and access management



Endpoint security



Lenovo





## ASSESS

# How to understand and mitigate AI risks.

Recommendations for identifying and mitigating AI-driven risks from both internal and external sources.



### For external threats.

Recognize emerging AI threats from external sources and take proactive steps to secure your systems.

#### Re-evaluate your security systems.

With IT leaders' confidence in their cybersecurity capabilities being low, it's imperative that businesses get clarity on their current defensive abilities in the face of AI threats. That starts with dynamic reviews of your organization's cybersecurity posture and technology to ensure it is at a level of risk the business is comfortable with.

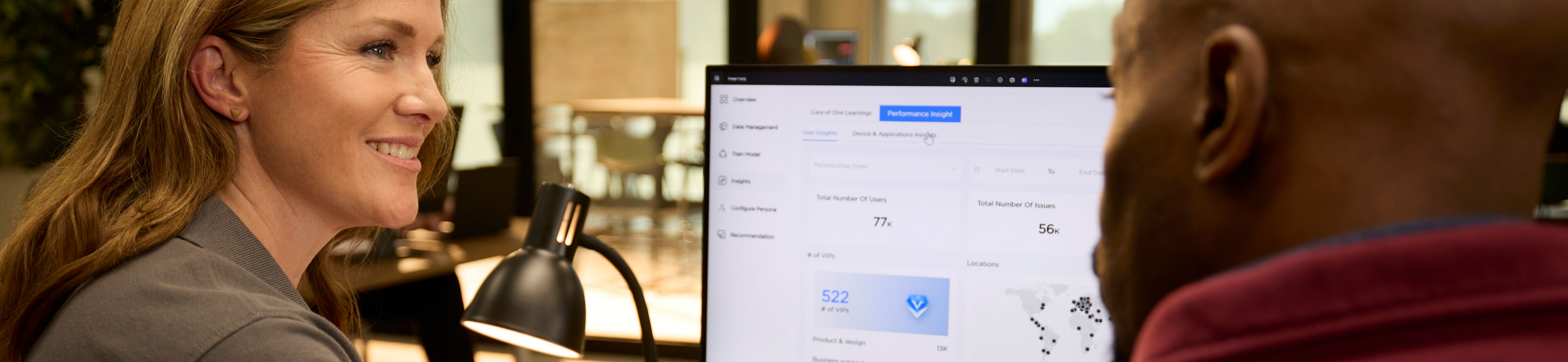
#### Outpace threats.

Attackers now operate at machine speed, taking just moments to gain the upper hand and causing irreversible damage before traditional defenses can respond. Organizations must move beyond isolated monitoring to embrace AI-native sensemaking: the ability to translate real-time, cross-domain signals into intelligent, coordinated responses. By unifying telemetry architecture and consolidating contextual analysis across all layers, organizations can detect, understand and act before threats take hold.

#### Reduce human vulnerabilities.

Identifying AI threats requires moving beyond static awareness programs. For example, advanced attackers can now use AI-powered social engineering like deep fake voice and video impersonation to trick employees into sharing sensitive information or credentials. Just as employees need to be able to spot a likely phishing email, they also need to be trained to identify and mitigate sophisticated AI threats.





## For in-house threats.

Identify weak points that can develop with in-house AI systems and practices—often overlooked by traditional cybersecurity systems.

### Establish clear AI usage policies.

Employees may not be aware that entering sensitive information into a public AI system could make that data available to other users outside the organization. Explicit policies and controls must be established to guide employees away from risky behavior.

### Audit access rights.

Unless agentic AI data access privileges are carefully controlled, AI agents could compromise internal data protection measures or be taken control of by attackers attempting to quickly extract sensitive information. The risk of data leakage means that businesses should heighten their efforts to monitor and ensure that AI systems and employees can only access the data they need.

### Secure your AI development lifecycle.

Building and implementing AI systems within the organization raises new types of risk. For example, if cybercriminals tamper with the training data of a customer-facing AI solution, it could cause considerable reputational and regulatory harm. Organizations should establish internal controls and checks that prevent manipulation of AI systems.





## EVOLVE

# Fighting AI with AI.

To tackle the cybersecurity risks of AI, IT leaders must unlock the potential of AI.

### Enhancing reactivity.

In a security environment where attack speed outpaces the ability of humans to respond, harnessing AI to support and scale up human decision-making is critical.

AI-integrated cybersecurity systems also enable security teams to interact with their tools using a natural language interface, instead of trawling through multiple screens to access the information they need to make an urgent decision.

“From a security perspective, the more holistic your view is of what’s happening, the faster you can spot something going wrong.”



**Mikkel Seiero**

Global Security Services Offering Lead  
Lenovo

### Achieving unified visibility.

In a traditional enterprise cybersecurity architecture, capabilities such as data protection or vulnerability analysis are delivered by separate teams using specialized tools. Gen AI-enabled adversaries can exploit the blind spots between these functions, minimizing the observability of these attacks.

To tackle these attacks, cybersecurity teams need a holistic view of the company’s security posture—one that crosses domains and draws from multiple toolsets. Extracting intelligence, a dynamic security posture score, and automated measures from the aggregated view is only possible by leveraging AI.

“Visibility is the first step to AI security—through complete visibility into all AI modules and applications, their functionalities, and continuous usage monitoring, we safeguard sensitive data, enforce security compliance and defend the organization against emerging AI-driven threats.”



**Kamrul Hasan**

Cybersecurity Architect  
Lenovo



EVOLVE

# The barriers to integrating AI with cybersecurity.

To defend against future threats, IT teams must utilize AI throughout their digital workplace defenses. But getting there isn't straightforward.

Our survey shows that businesses have already made some progress in adopting AI in cybersecurity. For example, nearly half are using AI and automation 'extensively' in endpoint security and identity access management (IAM).

But with less than half confident that their security capabilities are entirely sufficient to address AI risks, there is clearly plenty of room for improvement.

And successfully bolstering cybersecurity measures with AI is not as simple as deploying the right tools. For many organizations, there are substantial barriers that must be overcome.

## Barrier #1: Complex IT environments.



of IT leaders say 'complexity of IT environment' is a top barrier to AI-powered security.

Our survey reveals that the most common barrier is the complexity of the IT environment.

Most enterprise organizations have an IT estate—including their cybersecurity toolkit—that has evolved over many decades. This may well feature some legacy tools that are not supported by new AI-powered platforms.

## Barrier #2: Lack of skilled cybersecurity staff.

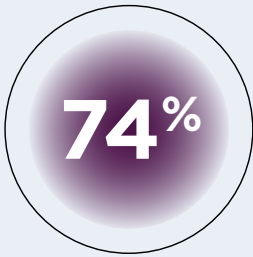


of IT leaders say 'lack of skilled staff within cybersecurity function' is a top barrier to AI-powered security.

The second-most common barrier is a lack of skilled staff within the cybersecurity function. This is not surprising: both AI and cybersecurity skills are in high demand and short supply. Finding employees with experience in both fields is extremely challenging.

This shortage is exacerbated by the mounting burden on security analysts, who operate in a high-stress, cognitively demanding environment as they face increasingly advanced adversaries.

## Barrier #3: Cost of solutions/limited budget.



of IT leaders say 'cost of solutions/limited budget' is a top barrier to AI-powered security.

Advanced tooling, skilled personnel and ongoing investment in AI readiness all require significant resource commitment. For many organizations already under budgetary pressure, allocating funds toward emerging technologies can be difficult to prioritize—especially when existing tools are still functional, even if outdated.



EVOLVE

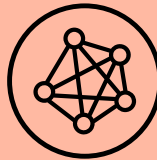
# How to transform your defenses.

Recommendations for practical steps that organizations can take to defend against AI-driven threats.



## Build a holistic view.

With complex IT estates and stretched security teams, fragmented tooling leads to inefficiencies, hidden costs and limited threat visibility. Consolidating telemetry across users, endpoints, applications and cloud infrastructure helps reduce tool sprawl and training costs—while creating the unified view needed to detect and respond to AI-powered threats faster and more effectively.



## Adopt versatile tools.

Large enterprises often have business-critical systems running on legacy platforms that they cannot easily migrate. To tap into AI-driven cybersecurity capabilities, companies need to embed security solutions and tools that support a wide range of operating systems, including those that might otherwise have fallen out of support.



## Boost your security team with experienced partners.

AI threats are moving fast while upskilling in-house teams takes money and time. Expanding your capabilities by working with experienced partners gives you access to the skills you need today, at the scale the challenge requires.



# Welcome to Work Reborn, reinforced.

Protecting the digital workplace in the age of evolving AI requires a complete reinvention of how businesses monitor, understand and respond to cybersecurity threats, and how they defend their digital assets.

**To turn the tables on Gen AI threats, businesses must:**

- **Enhance detection abilities.**

Given the ability of AI-powered threats to escape detection, organizations must redouble their efforts to protect their high-value assets. These include AI systems themselves—the agents, models, training data and prompts that power these AI systems are increasingly valuable targets for malicious actors.

- **Harness AI capabilities.**

Organizations must also adopt a more adaptive security posture, tackling threats in real time where possible. This can only be achieved by harnessing the same capabilities of AI that attackers use, equipping security teams with the insights, context and rapid recommendations they need.

**This two-pronged approach delivers better business outcomes:**

## **Increased productivity.**

Embedding AI into security operations can strengthen the productivity of security workers. Microsoft's Security Copilot, an AI assistant for cybersecurity teams, can boost productivity for SecOps teams by between 23% and 47%, according to an assessment by Forrester Research.<sup>1</sup> And, according to Microsoft's own analysis, device policy conflicts can be resolved 54% faster<sup>2</sup> and incidents resolved 30% quicker<sup>3</sup> by using Security Copilot.

## **Reduced costs.**

Transforming your defenses comes with a variety of benefits to the bottom line. For example, creating a holistic view across your security operations using AI reduces the training costs required to enable security teams to use the underlying tools. It can also minimize maintenance costs by optimizing the number of tools that are used—and provides an opportunity to outsource non-differentiated functions to partners with the scale to deliver cost effectively.

## **Seamless transformation.**

Perhaps most importantly, retooling cybersecurity for the age of fast-moving AI can give you the confidence to fully embrace digital workplace transformation. Our previous survey found that business leader security concerns are among the most common barriers to AI adoption. And as we've seen, these concerns are not unfounded. So, any AI-led transformation of the digital workplace must be accompanied by a cybersecurity upgrade.

<sup>1</sup> [New Technology: The Projected Total Economic Impact™ Of Microsoft Security Copilot, Forrester Research](#), November 2024

<sup>2</sup> [Security Copilot: Evidence of Productivity Gains in Live Operations](#), Microsoft Corporation, March 2025

<sup>3</sup> [Generative AI and Security Operations Center Productivity: Evidence from Live Operations](#), Microsoft Corporation, November 2024



# Ready to securely transform your workplace?

Confidently assess AI threats and ensure you're secure as you modernize your digital workplace.

Start [here](#).

**The vision is yours. Get there with Lenovo.**

---

## Methodology

For this study, Lenovo surveyed 600 IT leaders in April and May 2025. The survey sample included respondents from the US (17%), Canada, UK, France, Germany, India, Japan, Singapore, Brazil, Mexico (8% each), Australia (4%), and New Zealand (4%). Respondents included IT leaders from companies with at least 1,000 employees and from a range of sectors.

**Smarter  
technology  
for all**

**Lenovo**