BRILYANT

Modern security operations with unified platform - Enterprise

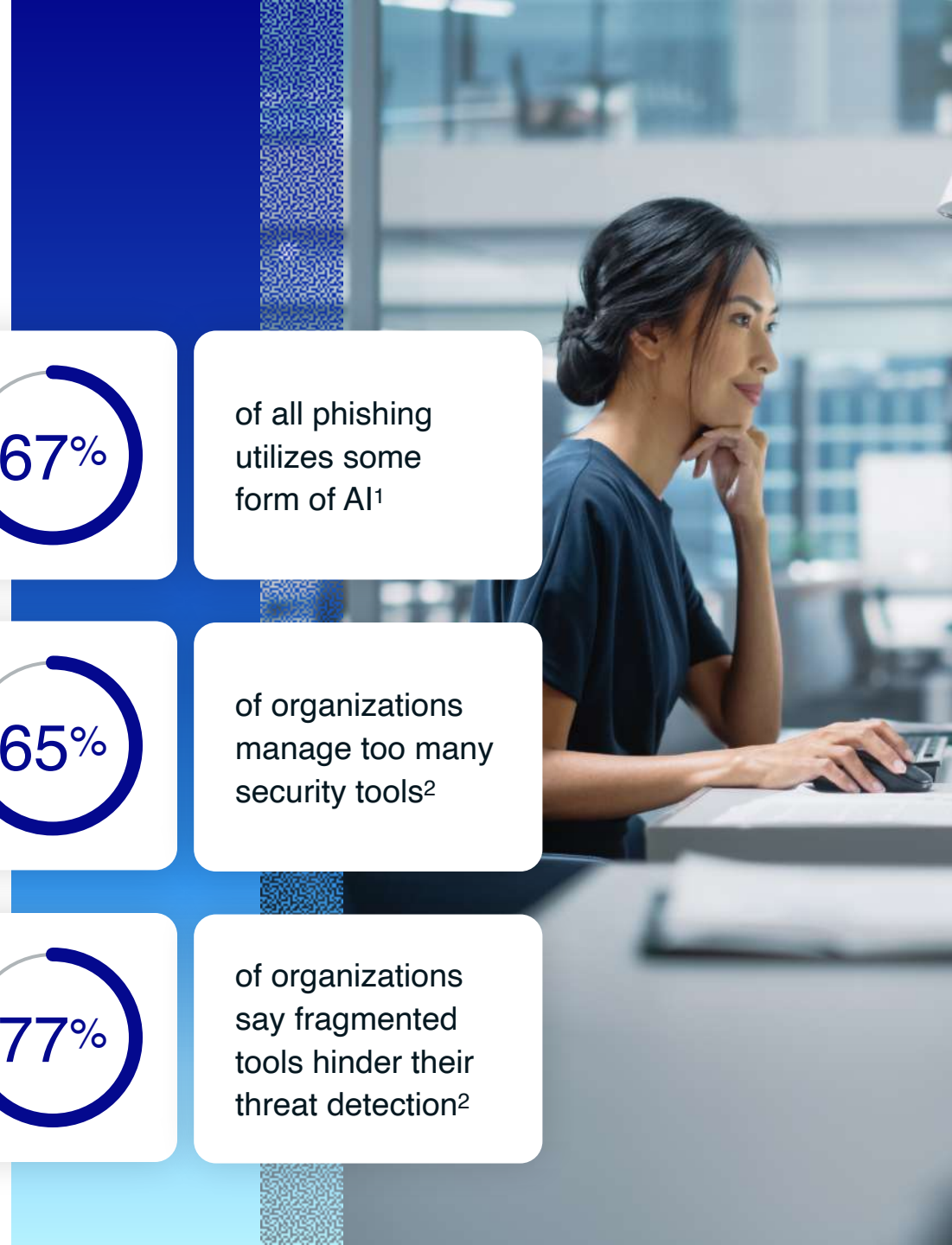
Simplifying security with an AI-powered threat defense

Microsoft

Complexity, fatigue, and rising threats

Today's security operations centers (SOCs) face unprecedented pressure as cyberattacks grow in scale, sophistication, and speed. Overwhelmed by false positives, fragmented tools, and siloed data, analysts find themselves missing or slowly responding to threats.

Generative AI changes the equation by correlating alerts, enriching investigations, and surfacing prioritized insights in seconds. Guided responses, automated threat hunting, and real-time attack path analysis help security teams quickly turn overwhelming data into actionable intelligence. It also enables SOCs to move from reactive to proactive protection by anticipating, disrupting, and containing threats before they escalate.



67% of all phishing utilizes some form of AI[1]

65% of organizations manage too many security tools[2]

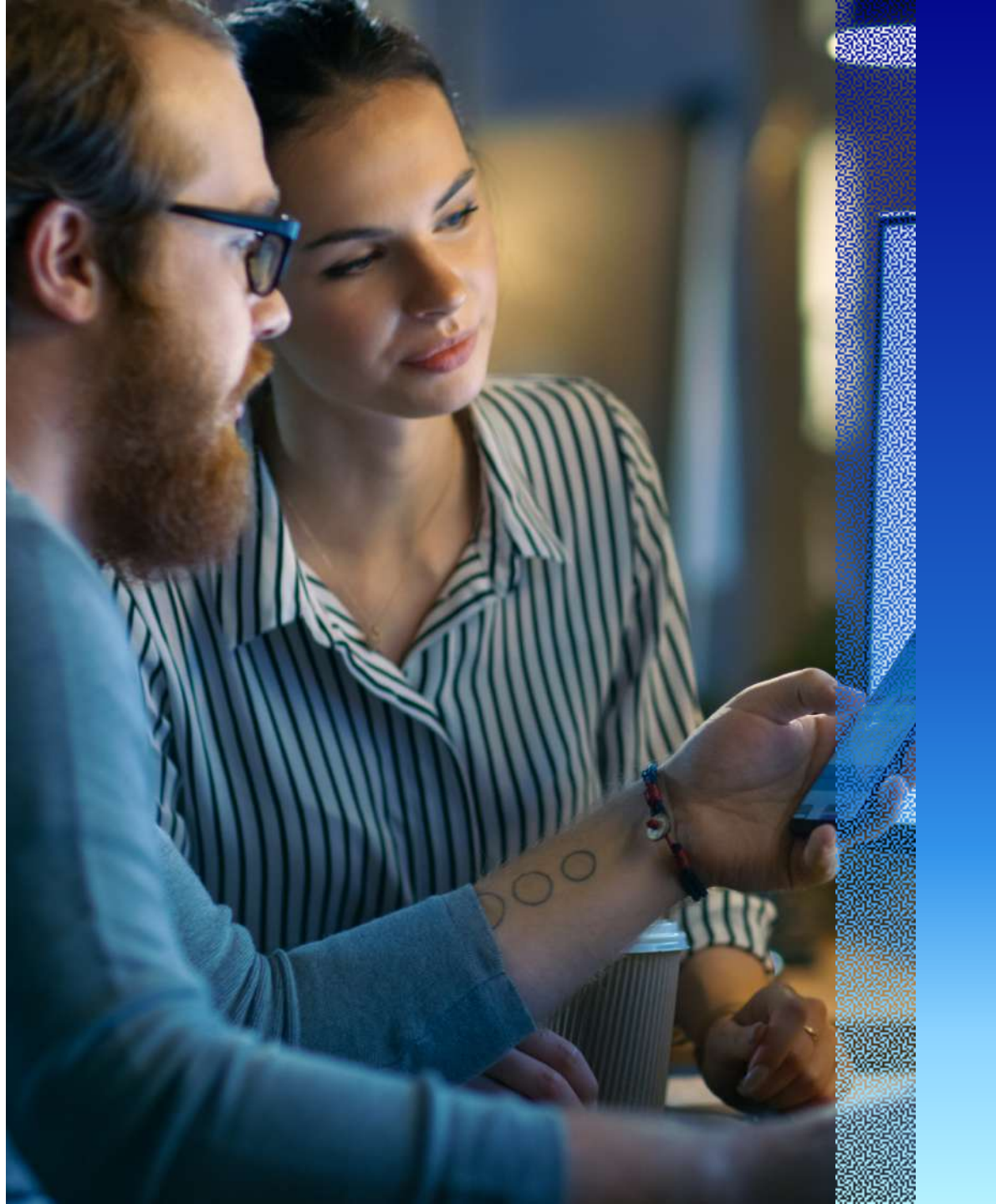
77% of organizations say fragmented tools hinder their threat detection[2]

1. https://cybelangel.com/rise-ai-phishing
2. Travers, T. (2025, June 2). New global business research shows how security sprawl increases risk. Barracuda Networks Blog. Barracuda Networks.

One platform for full coverage and fast response

The rapid expansion of the digital estate and sophistication of data attacks have exposed the limits of fragmented security environments. Many enterprises now run more than a dozen tools, creating complexity and visibility gaps. As a result, they're prioritizing the unification of their SecOps platform by integrating security information and event management (SIEM), extended detection and response (XDR), identity and access management (IAM), and AI for end-to-end coverage.

A single platform with a shared data foundation improves cross-team collaboration, simplifies infrastructure, and accelerates detection and response across hybrid and multicloud environments. With built-in AI-driven automation and threat intelligence, security teams can connect events across domains and correlate alerts into incidents, disrupting attacks quickly while strengthening protection.



Transform your SOC with AI-powered tools

Optimize, predict, detect, and remediate threats

Modern security operations with unified platform helps security teams do more with deep integration across cybersecurity, compliance, identity, and management. Agentic AI capabilities and Security Copilot amplify analyst productivity, boost scalability, accelerate threat hunting, and reduce mean time to respond (MTTR). AI-powered automation with Security Copilot enables proactive defense at scale, identifying and stopping threats before they affect your organization.

With Modern security operations with unified platform, security teams can:

- Optimize SOC operations.
- Detect emerging threats across data.
- Predict attack paths and prevent breaches.
- Rapidly remediate threats with AI.

Optimize SOC operations

Save your security staff time and energy by consolidating operations and automating processes.

With Modern security operations with unified platform, you optimize
detection coverage and data efficiency with full-spectrum visibility for detection.

Enhanced threat detection closes detection gaps and gives recommendations through AI-powered tools. You also gain long-term retention, advanced analytics, and AI-driven insights without the high overhead of existing infrastructure and manual work. Most important, your teams work more effectively across the full lifecycle of threats.

30%

decrease in the time to investigate and remediate threats[3]

3. The Total Economic Impact™ Of Microsoft Defender For Cloud, A commissioned study conducted by Forrester Consulting, January 2025

Predict attack paths

Identify and close critical gaps and blind spots using advanced exposure management.

Modern security operations with unified platform empowers your security team to understand, measure, manage, and improve your security posture across devices, identity, applications, data, and multicloud infrastructure.

Prioritize prevention efforts across your estate. Access threat-intel-driven insights. Monitor security controls and model potential attack paths. Modern security operations with unified platform helps you connect the dots between isolated security incidents to predict attacks and limit your vulnerability to them.

50%

decrease in number of false positives[3]

3. The Total Economic Impact™ Of Microsoft Defender For Cloud, A commissioned study conducted by Forrester Consulting, January 2025.

Detect emerging threats

Maximize visibility and automatically hunt for threats.

With Modern security operations with unified platform, you can stop active threats like ransomware, business email compromise, and adversary-in-the-middle attacks in as little as three minutes!

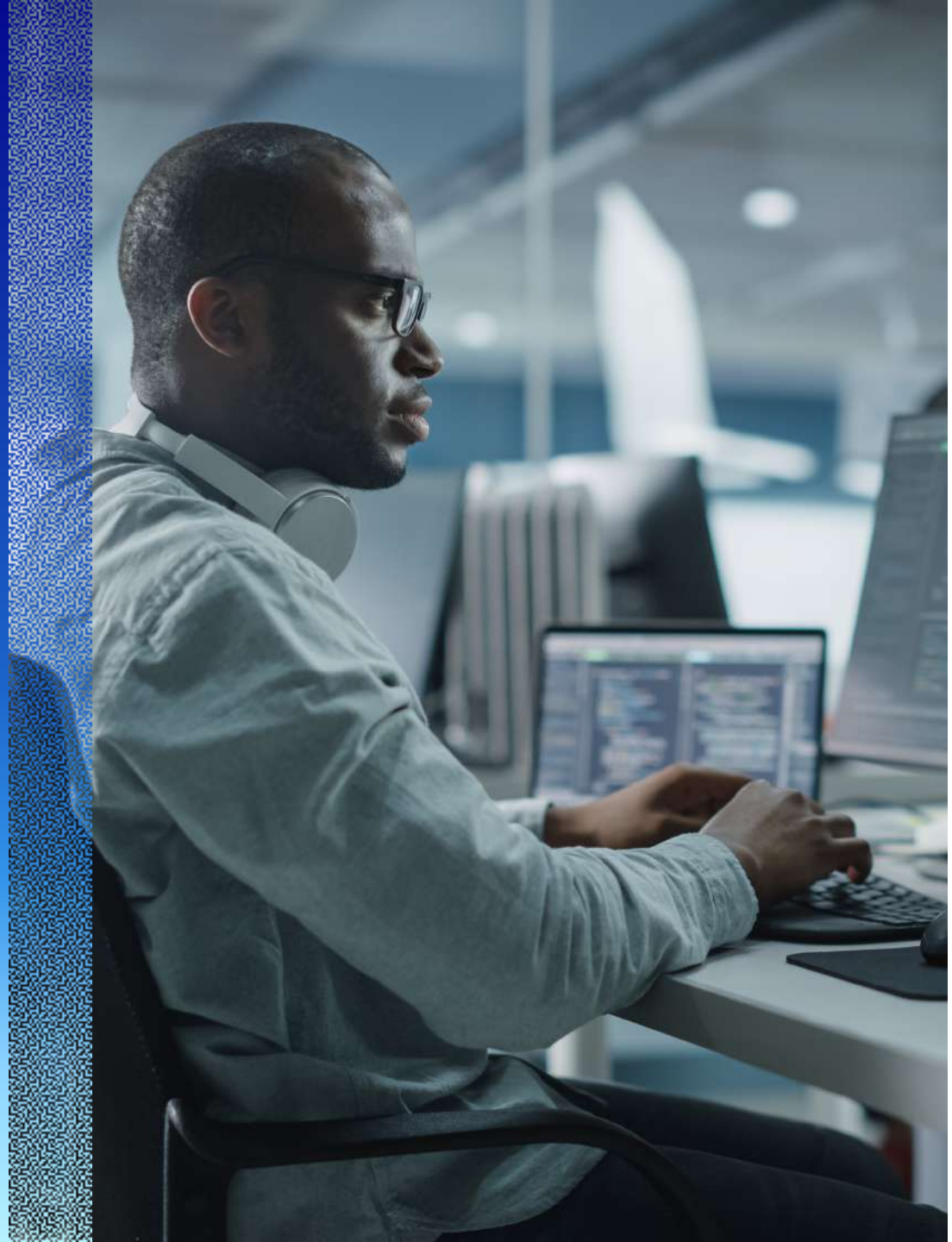
The platform helps prevent targeted attacks with proactive, intelligence-driven defense that automatically triggers detections. A unified generative AI-powered analyst experience enriches investigations and minimizes context switching for faster resolution.

To disrupt threats, the platform coordinates defense and detects attacks across identities, endpoints, cloud workloads, email, network, and more with complete visibility into the kill chain.

54%

reduction in time to resolve device policy conflicts[4]

4. Security Copilot randomized controlled trial (RCT) with experienced security analysts conducted by Microsoft Office of the Chief Economist, January 2024.



Rapidly remediate with AI

Disrupt attacks before they escalate and respond to incidents at the speed of generative AI.

Modern security operations with unified platform helps you improve core SOC metrics like MTTR with agentic assistance, built-in automation, and orchestrated responses.

Security Copilot instantly summarizes incidents the second you open them, helping analysts triage and efficiently begin investigations. In addition, teams gain step-by-step guidance automation that turns complex, multistage incidents into manageable investigations for analysts of every skill level.

30%

faster MTTR with Security Copilot[5]

5. Security Copilot: Evidence of Productivity Gains in Live Operations.

Conclusion

Modern security operations with unified platform offers an integrated solution, powered by AI, automation, and global threat intelligence.

- Anticipate and disrupt attacks.
- Reduce complexity.
- Move from reactive decisions to proactive.
- Automate processes.

Brilyant adds exceptional value in helping organizations capture these benefits at scale. We bring proven expertise in large-scale deployments, seamless integration, and fine-tuning Microsoft security solutions like Microsoft Sentinel and Microsoft Defender.

We offer Envisioning Workshops that enable us to work with leaders to link security priorities to business goals, forecast return on investment, and chart a clear adoption path. Managed and co-managed SOC services provide the ongoing coverage, advanced capabilities, and expert oversight enterprises need to fully take advantage of the platform without placing unsustainable demands on internal teams.