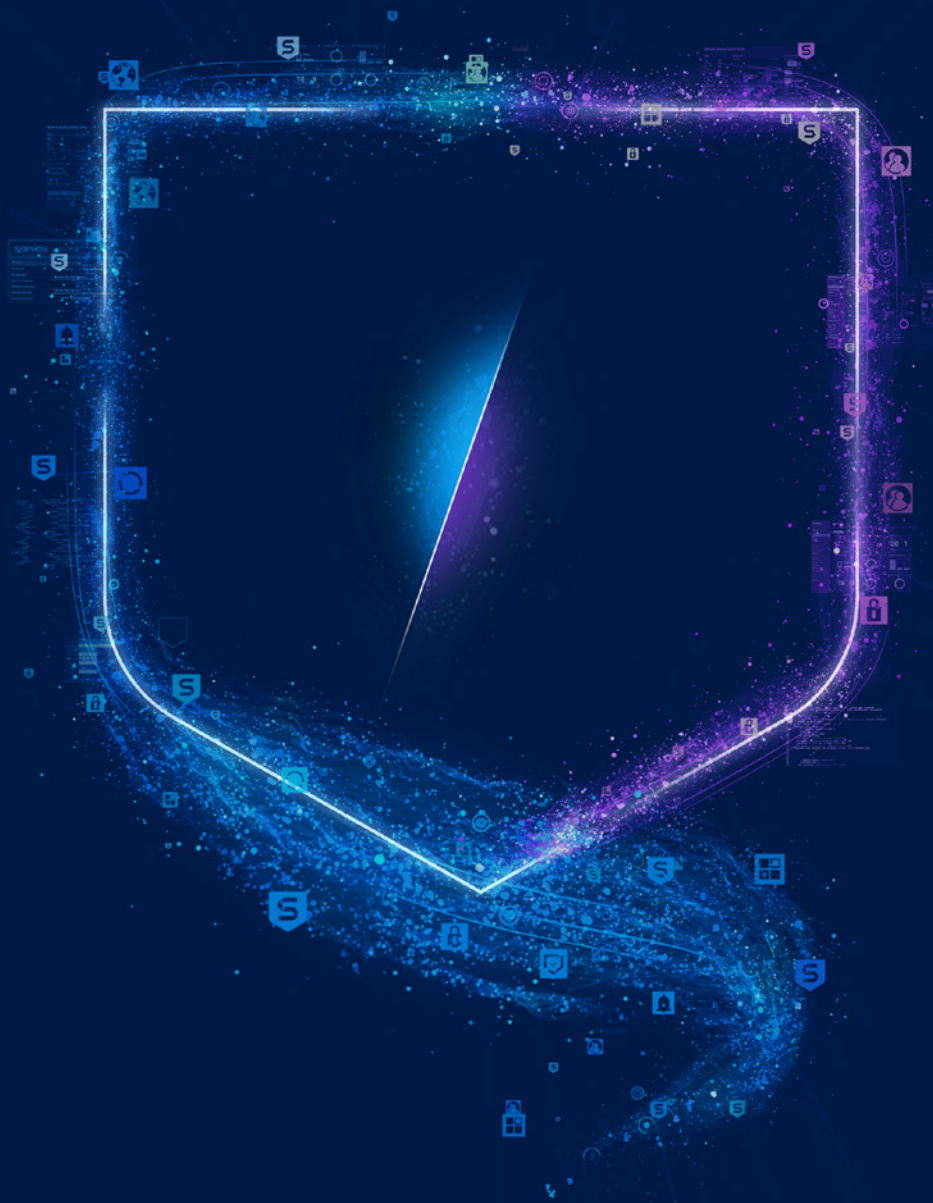
SOPHOS

Sophos AI-powered Cyber Defenses

Robust, battle-proven products and services that combine AI technologies and human expertise expertise, delivered through Sophos' adaptive AI-native platform.



SOPHOS

Sophos has been pushing the boundaries of AI for cybersecurity since 2017, bringing together AI technologies and human cybersecurity expertise to stop the broadest range of threats, wherever they run. Security analysts are empowered to make smart decisions faster while organizations can operate with confidence knowing our robust, battle-proven AI solutions have their back.

Deep learning and generative AI capabilities that solve the most critical problems for our customers are embedded in our solutions and delivered through the largest AI-native platform in the industry. Training on data from attacks in more than 600,000 diverse customer environments, our adaptive AI-native platform delivers unrivalled defenses for our customers and enhances the power of defenders.

AI level set

AI is a short acronym that covers a broad range of technologies of varying size and purpose. While generative AI models such as Microsoft Copilot and Google Gemini are often front of mind with AI, they are just a part of the story.
At Sophos, we use an extensive range of AI models to accelerate cybersecurity, matching the model to the security goal.

Type

Deep Learning AI (APPLY)

Uses artificial neural networks to recognize patterns and make decisions in a way that mimics the human brain. It applies learnings to perform tasks.

EXAMPLE:

Sophos URL Security Model
Detects malicious URLs, phishing websites, and other web-based threats.

Deployed In:
Sophos Endpoint, Sophos Firewall, Sophos Email, Sophos Mobile

Generative AI (CREATE)

Creates (generates) brand new content based on the structure and pattern of existing data.

EXAMPLE:

Sophos AI Case Summary tool
Provides an easy-to-understand summary of threat activity and recommends next steps.

Deployed In:
Sophos XDR, Sophos MDR

Size

Massive AI Models

Assists users in performing a wide range of tasks.

EXAMPLE:

Microsoft Copilot, Google Gemini
These large language models (LLMs) can help users with a very broad range of tasks. They are trained on vast quantities of data that are publicly available.

Small AI Models

Designed, trained and built for a specific, focused use case.

EXAMPLE:

Sophos Android DL model
Trained on Sophos' proprietary Android data to detect Android-specific malware.

Deployed In:
Sophos Mobile

AI at every point in your defenses

More than 50 (and growing) deep learning and GenAI models in Sophos solutions deliver fast, effective protection against cyberthreats, whenever and wherever they run. Our AI-powered cybersecurity reduces exposure, stops threats automatically, and empowers security analysts to make smart decisions faster.

Examples of AI use in Sophos products and services

Mitigate Risk of Threats
Reduce exposure to attack

SOPHOS MANAGED RISK
Uses the Tenable Vulnerability Priority Rating (VPR) AI model to predict the likelihood of CVE exploitation within 28 days

Automatically Stop Threats
Prevent attacks from executing

SOPHOS ENDPOINT
Multiple deep learning models secure against known and never-before-seen attacks, including threats in Microsoft Office solutions, PDFs and rich text format (RTF) files

SOPHOS FIREWALL
AI-powered zero-day threat intelligence is delivered through SophosLabs Intelix

SOPHOS ENDPOINT & FIREWALL
Web protection models detect malicious URLs, phishing websites, and other web-based threats

SOPHOS EMAIL
Deep Learning-powered Natural Language Processing (NLP) identifies impersonation attempts

SOPHOS MOBILE
Android DL model is trained on proprietary Android data to detect Android-specific malware

Hunt, Investigate, and Respond
Identify and neutralize threats

SOPHOS XDR, SOPHOS MDR
AI-generated threat scores for detections help analysts prioritize their time and effort

SOPHOS XDR, SOPHOS MDR
AI Case Summary provides a clear overview of detections and recommended next step

SOPHOS MDR
AI-powered case triage accelerates investigation and eliminates duplicate cases

SOPHOS XDR, SOPHOS MDR
AI Command Analysis provides insights into attacker behavior by examining commands that create detections

SOPHOS XDR, SOPHOS MDR
AI Search enables analysts to use natural language to search for data, speeding up investigations

Delivered through Sophos' adaptive AI-native platform

Sophos Central is the adaptive AI-native platform that delivers unrivalled protection and enhances the power of defenders. Dynamic defenses, battle-proven AI, and an open, integration-rich ecosystem come together in the largest AI-native platform in the industry.

Sophos Central

Dynamic

- Protection is constantly updated based on threat intelligence from attacks in more than 600,000 diverse customer environments across the globe.
- Adaptive defenses automatically respond to threats.
- AI models are continually enhanced using real-time inputs from 300 human security operations specialists.

Open

- Works with Sophos products, other vendors' products, or any combination of the two—across multiple OS environments.
- Centralized data and integrated workflows optimize security tasks and enhance human productivity to accelerate security outcomes.

Largest

- Breadth: Leverages telemetry from attacks on 600,000+ customers of diverse size and industries across the globe.
- Depth: Uses data from across the IT environment, from Sophos and non-Sophos technologies, and devices running Windows, iOS, and Linux OS.

Win-win: Human expertise plus AI technologies

Our people are at the heart of our AI-powered cybersecurity solutions, bringing their expertise to every aspect of the development process.

- Sophos X-Ops, our cross-functional cybersecurity task force, has deep knowledge of **threats and adversary behaviors**, helping identify how and when AI can have the greatest impact.
- The Sophos AI team applies extensive **AI expertise** to design, build, and maintain 50+ AI models specific to cybersecurity.
- 30+ years of **cybersecurity engineering expertise** ensure successful integration of AI models into Sophos products and services and safe feature rollouts.

Learnings from AI deployments advance our human expertise, enabling us to continually refine models, identify new applications, and advance our technology.

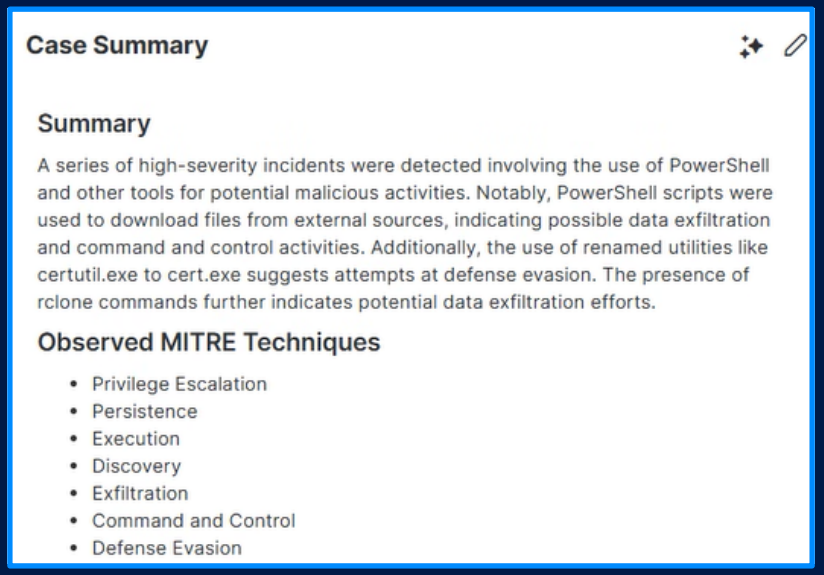
Sophos AI use cases

Accelerate security operations with genAI

Extensive GenAI capabilities in Sophos Extended Detection and Response (XDR) empower your security analysts to neutralize adversaries faster, increasing both analyst and business confidence.

- **AI Case Summary** provides an easy-to-understand overview of detections and recommended next steps, helping analysts make smart decisions fast.
- **AI Command Analysis** delivers insights into attacker behavior by examining commands that create detections.
- **AI Search** uses natural language search to accelerate day-to-day tasks and lower the technology barrier to security operations.
- **AI Case Assistant** provides support and advice for analysts as they work a case, helping seasoned and less experienced analysts alike neutralize adversaries faster (Q1 2025).

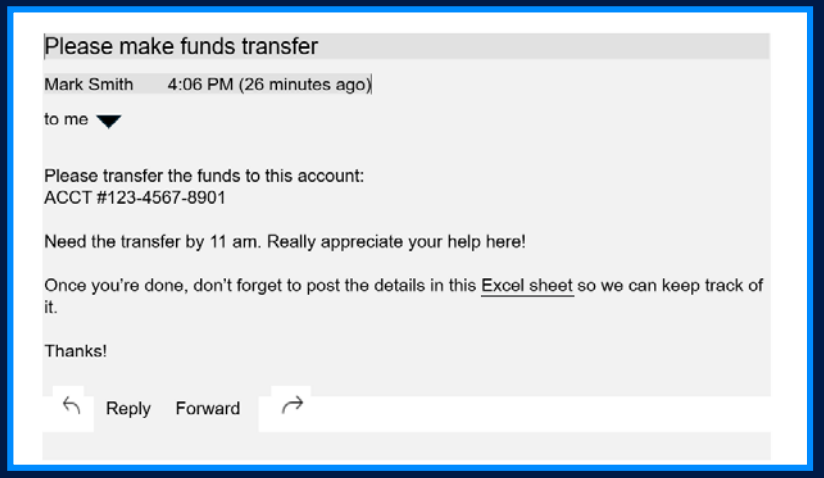
Sophos GenAI features are available on an opt-in basis, giving you full control.



Stopping Business Email Compromise with deep learning

Deep learning-powered Natural Language Processing (NLP) in Sophos Email identifies impersonation attempts trying to trick users into believing a scam or phishing email is legitimate.

Sophos Email uses AI to analyze subject lines and content for both tone and wording to identify suspicious conversations. Impersonation attempts are automatically blocked, preventing the attack, and the administrator is notified.



Experience you can count on

We've been using AI successfully to accelerate cybersecurity since 2017. With Sophos, you can focus on your business, confident that AI is delivering reward, not risk, for your organization.

Risk	Sophos Approach
Organizations don't see the promised benefits from their AI investments.	**Outcome-focused AI** With years of AI expertise, we know how to deliver real-world impact.
Poorly developed, trained, and deployed AI solutions can cause real damage.	**Security-first processes** Our robust development processes allow customers to use Sophos AI with confidence.
Vendors focus on the AI, not the benefits it delivers.	**Real-world benefits** Our robust, battle-proven AI-powered solutions make a material difference by neutralizing threats faster and empowering analysts to make smart decisions.

The Sophos AI team

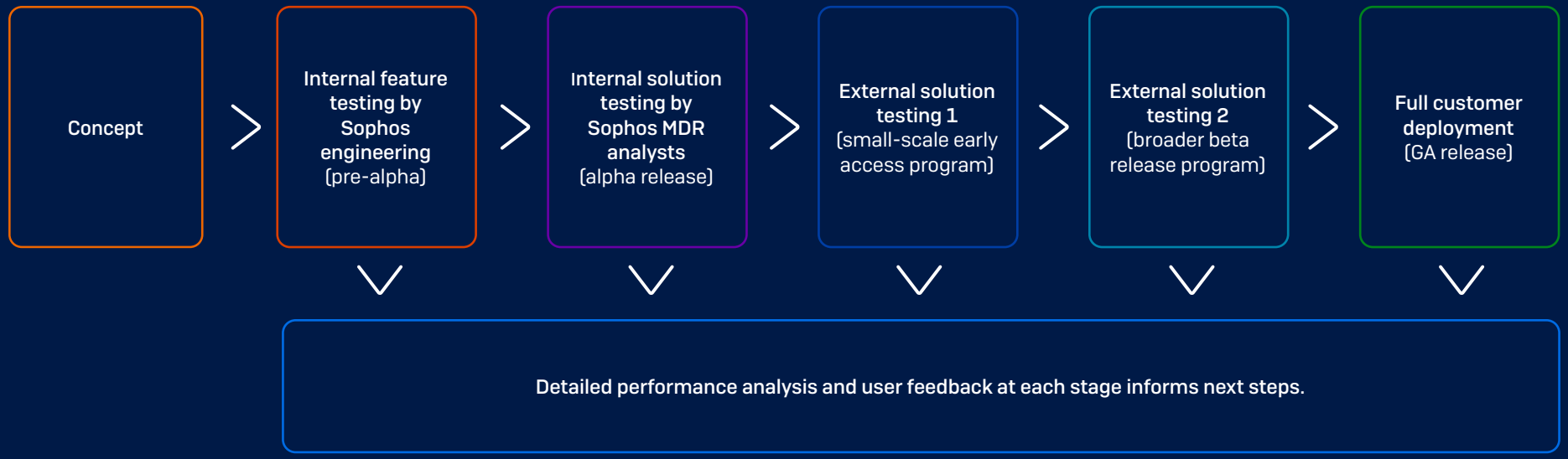
The Sophos AI team comprises experts who know how to use AI to accelerate positive cybersecurity outcomes. This dedicated global group focuses on two main areas:

- Developing and applying AI in Sophos solutions
- Novel research that advances AI for cybersecurity

The Sophos AI team shares its research findings through public reports and events. Check out its latest publications on the **Sophos AI blog site.**

Robust generative AI development process

The benefits of GenAI for cybersecurity are matched by their potential danger. Sophos deploys rigorous processes for all GenAI tools, from concept to full deployment. Detailed performance analysis and user feedback at each stage informs the next step in the development process.



Securely navigate the AI hype with Sophos

To find out more about Sophos' AI-powered cybersecurity solutions and how they can help you achieve your goals, visit **www.sophos.com** or speak with your Sophos Partner or representative.

SOPHOS

2025-01-17 SG-EN [DD]