EVALUATION BRIEF

MITRE ATT&CK® Enterprise 2025 Evaluation

SOPHOS

Sophos achieves 100% detection in the MITRE ATT&CK® Enterprise 2025 Evaluation

MITRE ATT&CK® Evaluations measure how effectively security solutions like Sophos XDR detect, analyze, and communicate sophisticated multi-stage threats. In the Enterprise 2025 evaluation:

- Sophos successfully detected all 16 attack steps and 90 sub-steps, proving the power of our open AI-native XDR platform.
- **100% detection:** Sophos detected and provided actionable threat detections for all adversary activities — zero misses.
- **Highest possible scores:** Sophos generated full Technique-level detections for 86 of the 90 adversary activities evaluated.

MITRE ATT&CK® Evaluations: Enterprise 2025

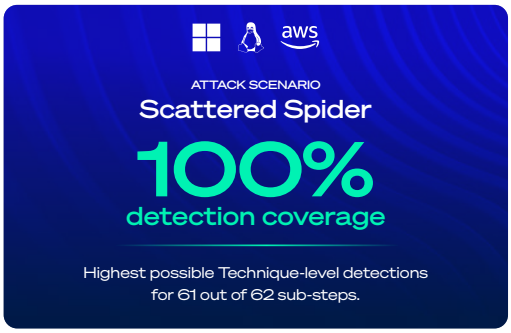
MITRE ATT&CK® Evaluations are among the world's most rigorous independent security tests. They emulate the tactics, techniques, and procedures (TTPs) leveraged by real-world adversarial groups and evaluate each participating vendor's ability to detect, analyze, and describe threats, with output aligned to the language and structure of the MITRE ATT&CK® Framework.

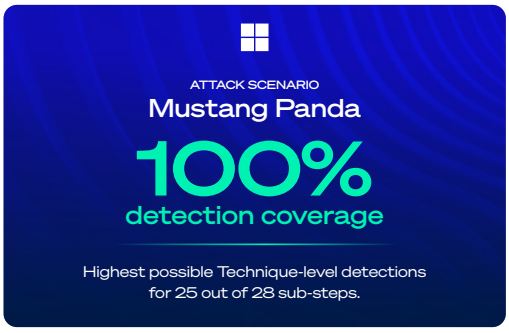
The Enterprise 2025 evaluation included MITRE's first-ever cloud adversary emulation and addressed the sophisticated, multi-platform threats organizations face from both financially motivated cyber criminals and state-sponsored espionage groups:

- **Scattered Spider: A financially motivated cybercriminal syndicate**
  Known for their expertise in social engineering, this threat group persistently targets victims' cloud resources to establish footholds, conduct reconnaissance, and access sensitive systems and data.
- **Mustang Panda: A People's Republic of China [PRC) espionage group**
  An active PRC state-sponsored cyber espionage group that employs living-off-the-land techniques, custom malware, and cloud-hosted infrastructure.

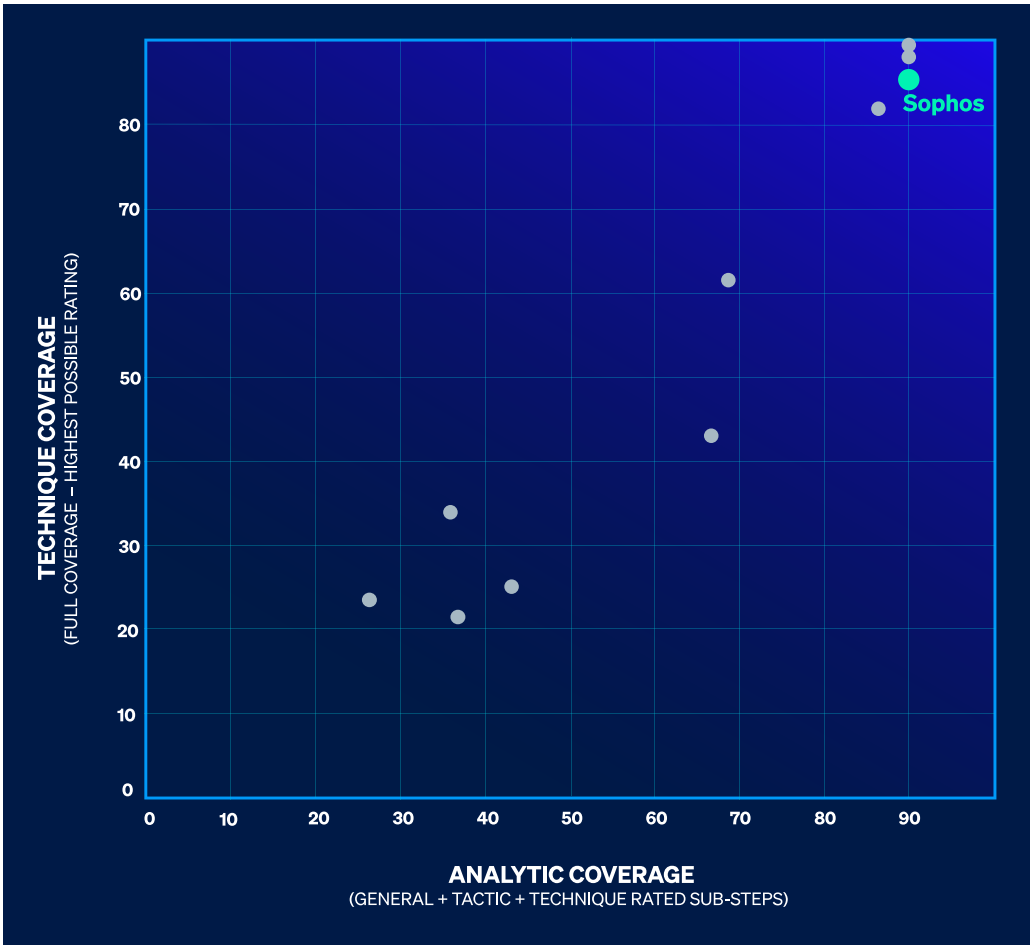
Evaluation results

Sophos successfully detected and provided actionable threat detections for all adversary activities (sub-steps) across two comprehensive attack scenarios.





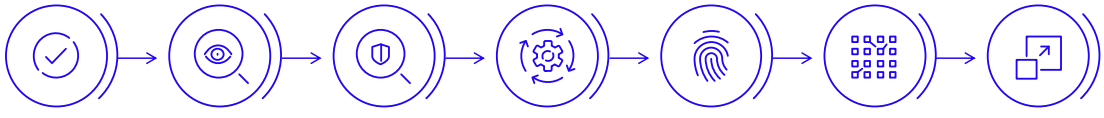
Detection quality is critical for providing security analysts with the information to investigate and respond quickly and efficiently. The chart below compares the number of sub-steps that generated a detection providing rich detail on the adversarial behaviors (analytic coverage) and the number of sub-steps that achieved full 'technique' level coverage, for each participating vendor.



MITRE does not rank or rate participants of ATT&CK Evaluations.

Evaluation attack scenarios

Attack scenario 1: Scattered Spider [Windows, Linux, and AWS]



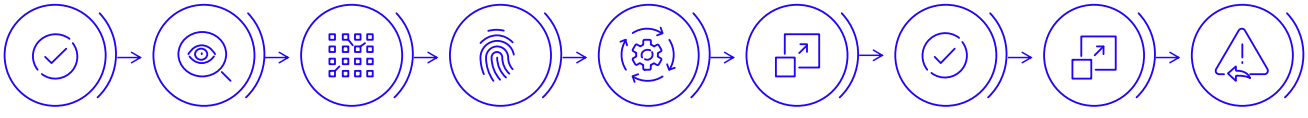
Step 1: **Initial access via unmanaged device**
Step 2: **Discovery**
Step 3: **AWS discovery and defense evasion**
Step 4: **AWS persistence and defense evasion**
Step 5: **Credential access**
Step 6: **Lateral movement**
Step 7: **Collection and exfiltration**

A sophisticated hybrid-environment intrusion combining social engineering, cloud exploitation, identity abuse, and living-off-the-land techniques. The adversary spear phishes for credentials, gains remote access, conducts discovery, evades defenses, and exploits the company's AWS environment using native tools.

This scenario comprised 7 attack steps with 62 sub-steps across Windows, Linux, and AWS.

- **100% of sub-steps detected. Zero misses.**
- Actionable threat detections generated for every sub-step.
- Highest possible Technique-level ratings achieved for 61 out of 62 sub-steps.

Attack scenario 2: Mustang Panda [Windows]



Step 1: **Initial access**
Step 2: **Discovery**
Step 3: **Lateral movement**
Step 4: **Credential access**
Step 5: **Persistence**
Step 6: **Collection and exfiltration**
Step 7: **Initial access**
Step 8: **Collection and exfiltration**
Step 9: **Indicator removal**

An evasive intrusion showcasing the adversary's skilled use of social engineering, legitimate application abuse, persistence mechanisms, and custom malware. The attack begins with a phishing email granting access to the victim's Windows workstation. The adversary discovers key assets — including a file server, domain controller, and other workstations — exfiltrates data and removes their tools to cover their tracks.

This scenario comprised 9 attack steps with 28 sub-steps targeting Windows devices.

- **100% of sub-steps detected. Zero misses.**
- Actionable threat detections generated for every sub-step.
- Highest possible Technique-level ratings achieved for 25 out of 28 sub-steps.

Why we participate in MITRE ATT&CK® Evaluations

MITRE ATT&CK® Evaluations are among the world's most rigorous independent security tests. Sophos is committed to participating in these evaluations alongside some of the best security vendors in the industry. As a community, we are united against a common enemy. These evaluations help make us better, individually and collectively, for the benefit of the organizations we defend.

11 EDR/XDR security vendors participated in the Enterprise 2025 evaluation:

Check out the full results on the MITRE website: https://evals.mitre.org/enterprise/er7

A market leader in detection and response solutions

Gartner Peer Insights Customers' Choice 2025

Sophos is a 2025 Gartner Peer Insights "Customers' Choice" vendor for Extended Detection and Response (XDR).

Gartner

Sophos is a Leader in the 2025 Gartner Magic Quadrant for Endpoint Protection Platforms for the 16th consecutive time.

Sophos is named a Leader for both EDR and XDR in G2's Fall 2025 Overall Grid® reports.

SE Labs

Sophos consistently achieves strong protection results in independent tests.

MITRE | ATT&CK® Evaluations

Sophos is a strong performer in MITRE ATT&CK Evaluations.

IDC

Sophos is a Leader in the IDC MarketScape: Worldwide Extended Detection and Response (XDR) Software 2025.

SOPHOS

Get started with Sophos XDR

See how Sophos can streamline your detection and response and drive superior outcomes for your organization. Learn more at Sophos.com/XDR

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2025-12-05 EN (DD)