

Tougher than ever.

Unmatched results in the most challenging evaluation yet.

Cortex XDR® delivered a historic 100% technique-level detections and the highest prevention rate in the 2024 MITRE ATT&CK® Enterprise Evaluations.

SEE HOW WE DID IT



Want the strongest protection? Look at the strongest performers.

The MITRE ATT&CK® Enterprise Evaluations are the industry's most rigorous test of endpoint security. These simulations measure how well a solution defends against advanced, real-world threat actors.

WATCH THE WEBINAR

In 2024, MITRE brought the heat with its toughest scenarios yet.

THE SIMULATIONS



Ransomware as a Service: Attacks by CLOP and LockBit targeting Windows and Linux systems.



North Korea: Attacks on macOS that mimicked DPRK's multi-staged modular malware.

THE STEP UP IN DIFFICULTY



Expanded platform testing with increased coverage for Linux and added macOS for the first time.



The introduction of false-positive testing assessed accuracy in distinguishing genuine threats from legitimate business activity.

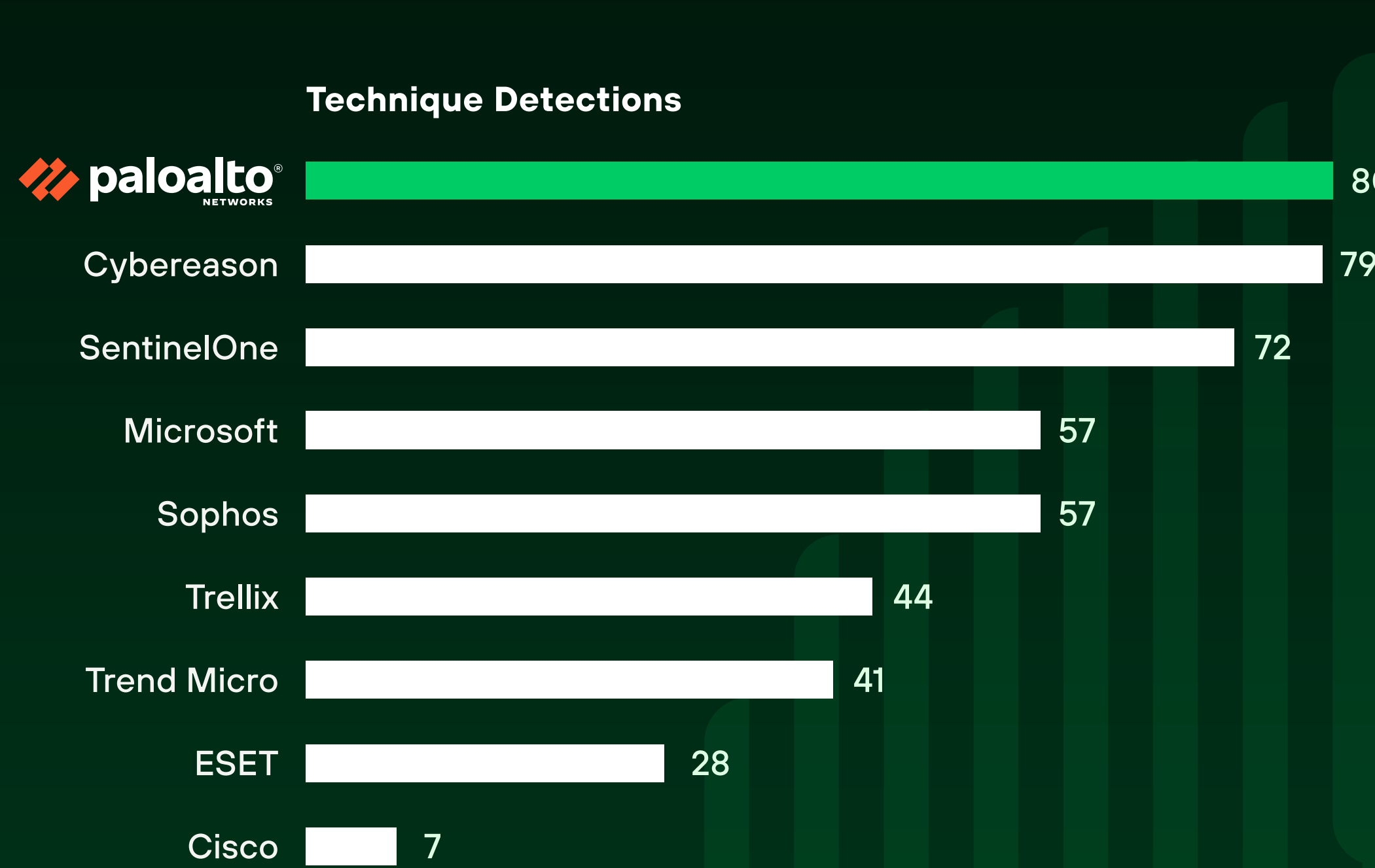
Once again, Cortex excelled.

Palo Alto Networks rose to the challenge, delivering outstanding results.

Detection



Palo Alto Networks is the first-ever vendor to achieve **100% technique-level detection coverage** with no delays or configuration changes.

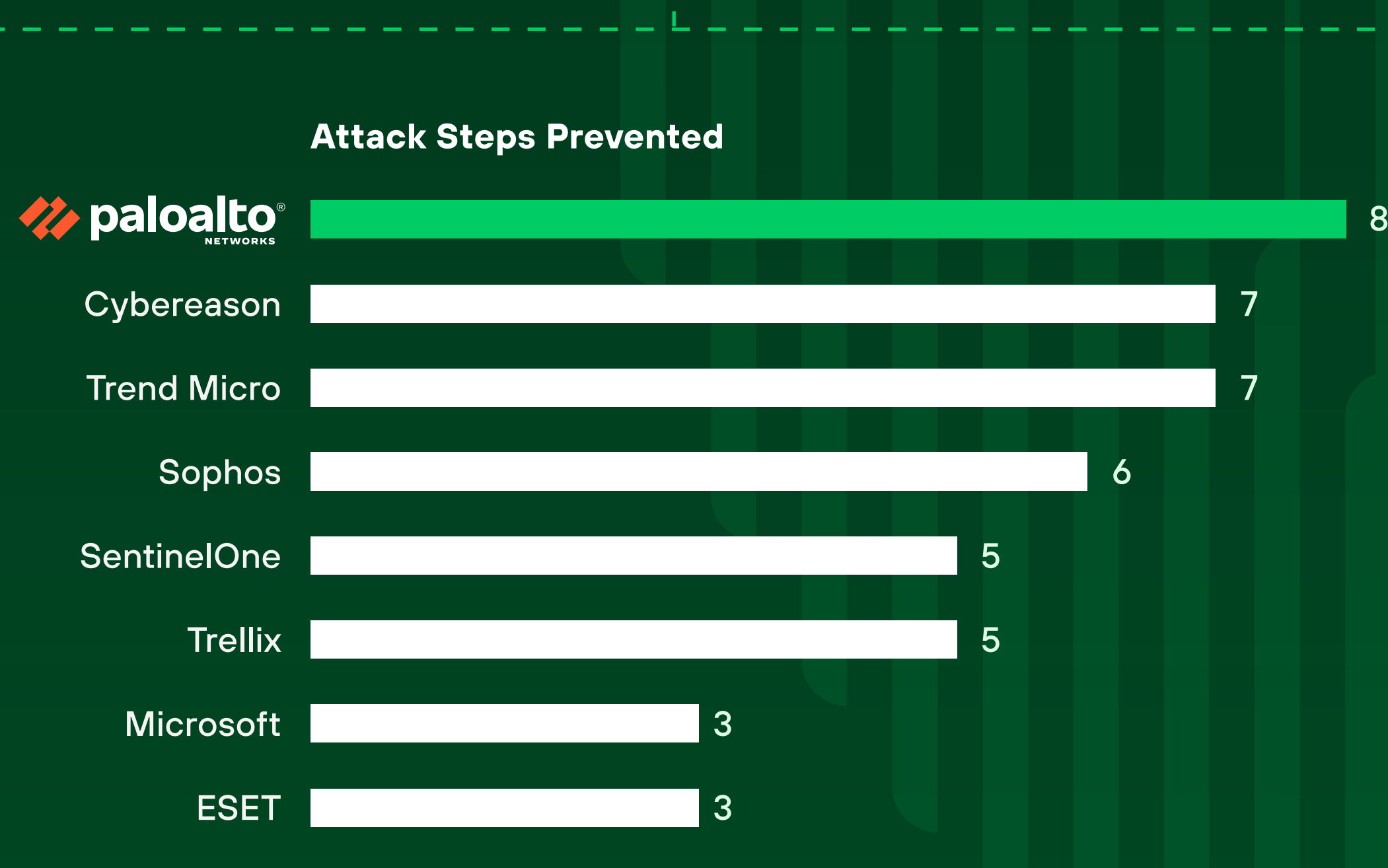


In a real attack, there are no do-overs. Other vendors may claim 100%, but those results often include detections resulting from configuration changes and a re-test to improve their scores.

Prevention



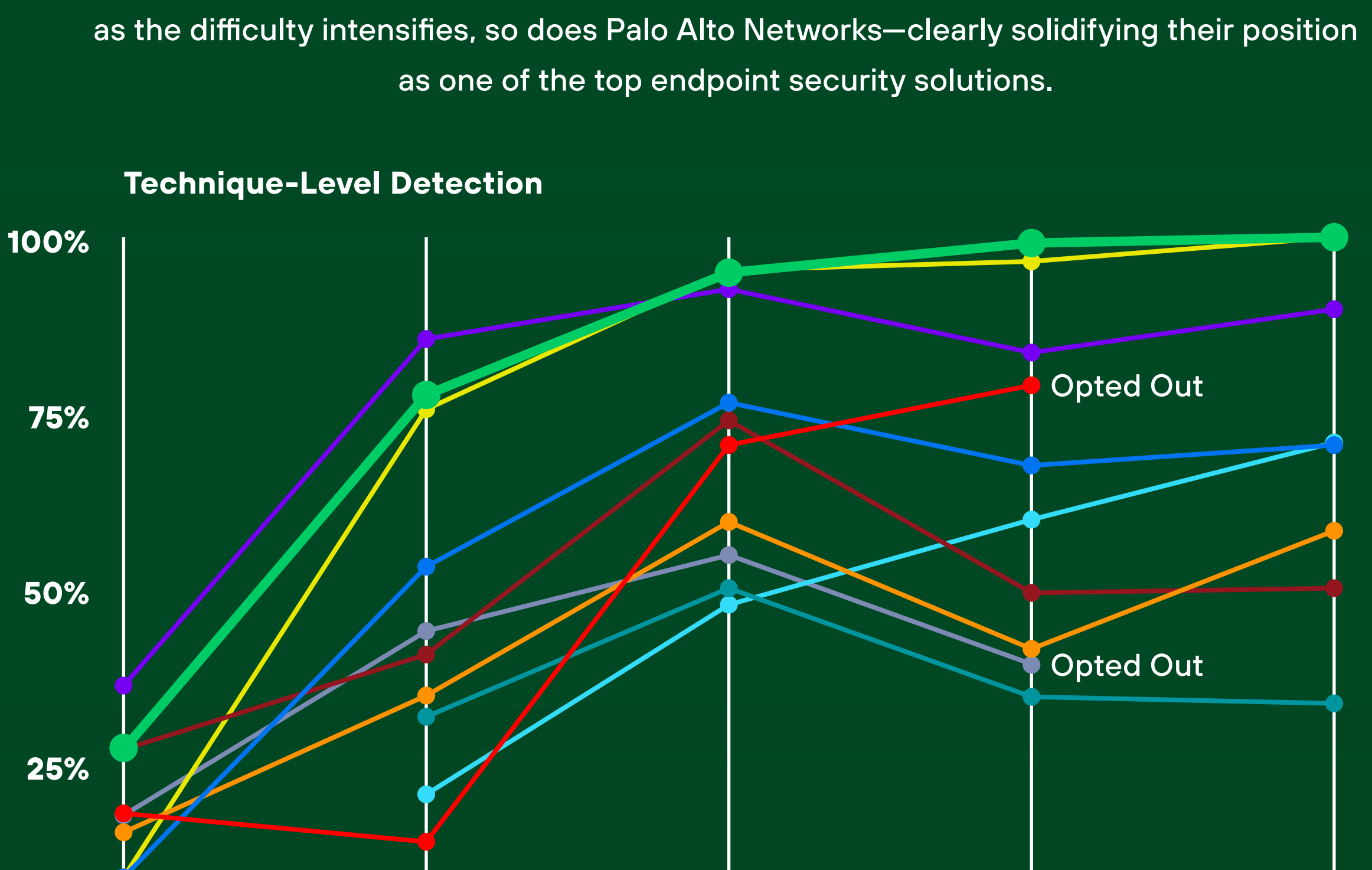
Cortex XDR achieved the highest prevention rate among all vendors with **zero false positives**—a critical distinction for endpoint security.



Unmatched accuracy plus zero disruptions make Cortex the ideal endpoint solution for the world's most demanding organizations.

Five years of excellence.

This wasn't the first year that Cortex achieved outstanding results. Year after year, as the difficulty intensifies, so does Palo Alto Networks—clearly solidifying their position as one of the top endpoint security solutions.



Top Market Share Vendors:

- Palo Alto Networks Cortex XDR
- SentinelOne
- Trellix
- Sophos
- CrowdStrike
- ESET
- Cybereason
- Microsoft
- Trend Micro
- Broadcom

DIG INTO THIS YEAR'S RESULTS

Cortex XDR sets the bar.

You can count on Palo Alto Networks to show up and stand up—in MITRE and in real-world attacks. Cortex XDR delivers industry-leading endpoint security for stopping the most sophisticated attacks.

- Detect more attacks with real-time AI on stitched data
- Prevent endpoint threats with industry-leading accuracy
- Quickly pivot to the root cause to minimize investigation time
- Respond faster than the adversary to stop a breach
- Stop cyberattacks in the cloud with the same investigation workflow

REQUEST A DEMO