cybereason

MITRE ATT&CK ENTERPRISE EVALUATION 2023

WHO IS MITRE ENGENUITY?

ATT&CK Enterprise Evaluations 2023

- ✓ **Non-profit organization**
  “A Foundation For Public Good”
- ✓ **Transparency and publicly available testing**
- ✓ **Annual evaluations**
- ✓ **Based on MITRE ATT&CK Framework. Built from TTP’s of malicious actors and cybercriminals.**
- ✓ **Unbiased - vendors can’t pay for better results**
- ✓ **Demonstrates expected performance of an endpoint security solution**

WHO IS TURLA?

Enterprise Evaluations 2023

Turla Overview

- Destructive Russian-based threat group that has infected victims in over 45 countries.
- Known to target government agencies, diplomatic missions, military groups, and research and media organizations.
- Executes highly targeted campaigns aimed at exfiltrating sensitive information from Linux and Windows infrastructure.

Linked to several cyber-espionage campaigns

- **Moonlight Maze** - one of the first cyber espionage campaigns that targeted the US, breaching the Navy, Air Force, NASA, & EPA.
- **Agent.btz** - malware was beaconing out from inside classified network of DOD which was supposed to be air-gapped.
- **RUAG Espionage Incident** - Swiss military technology was stolen in a cyber-espionage campaign against Swiss defense company.

cybereason

cybereason

MITRE ATT&CK 2023 TURLA EVALUATION

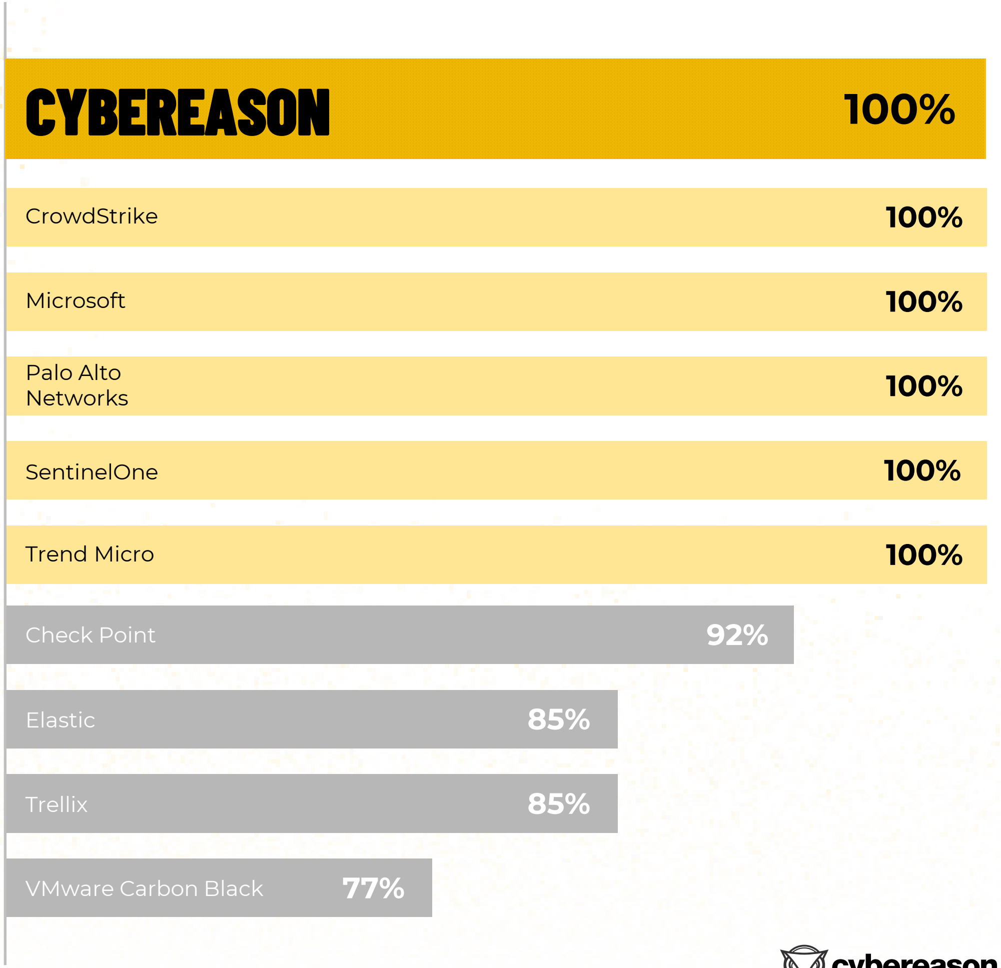
Top Performance in All Categories

100% Protection	Blocked 13/13 Protection Tests
100% Detection	Detected 19/19 Attack Steps
100% Visibility	Revealed 143/143 Attacker Sub-Steps
100% Real Time	No Delayed Attack Detections
100% Out of the Box	No Configuration Changes Needed

MITRE 2023 ATT&CK PROTECTION COVERAGE

% of 13 Protection Scenarios Blocked

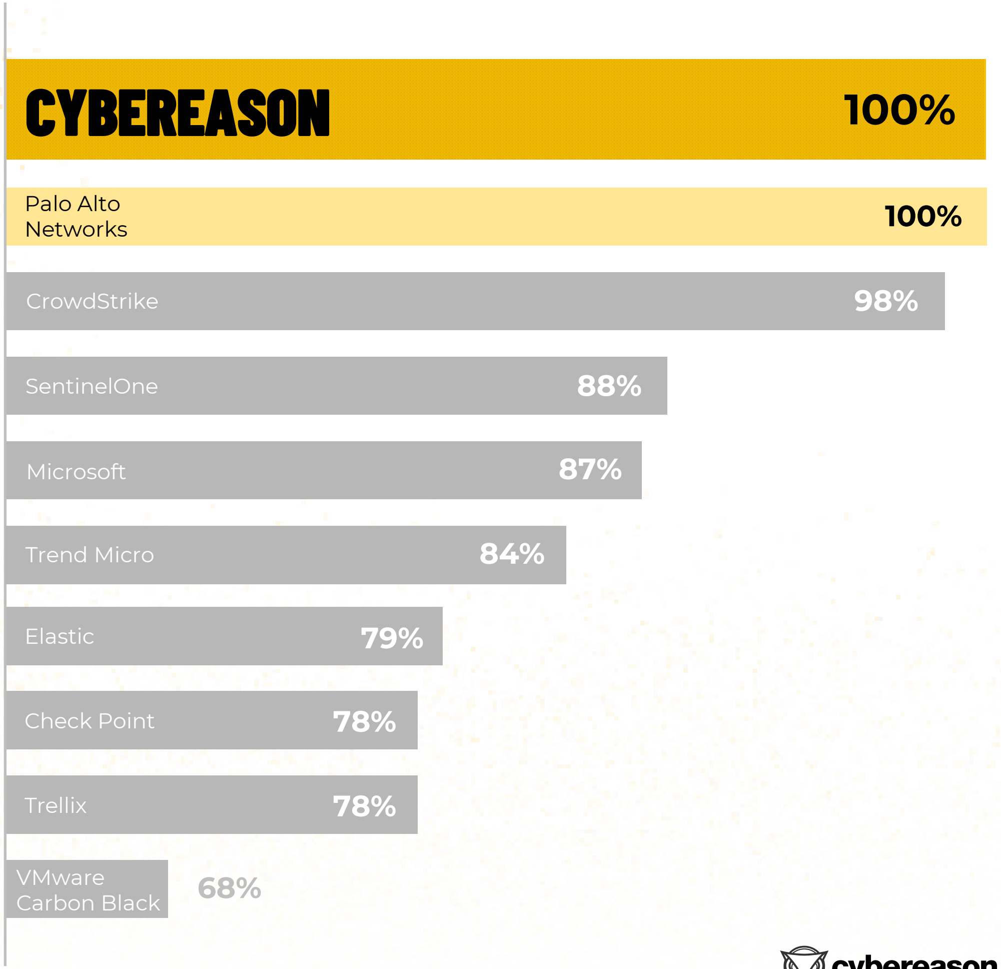
Subset of participating vendors



MITRE 2023 ATT&CK VISIBILITY COVERAGE

% of 143 Sub-steps Detected

Subset of participating vendors

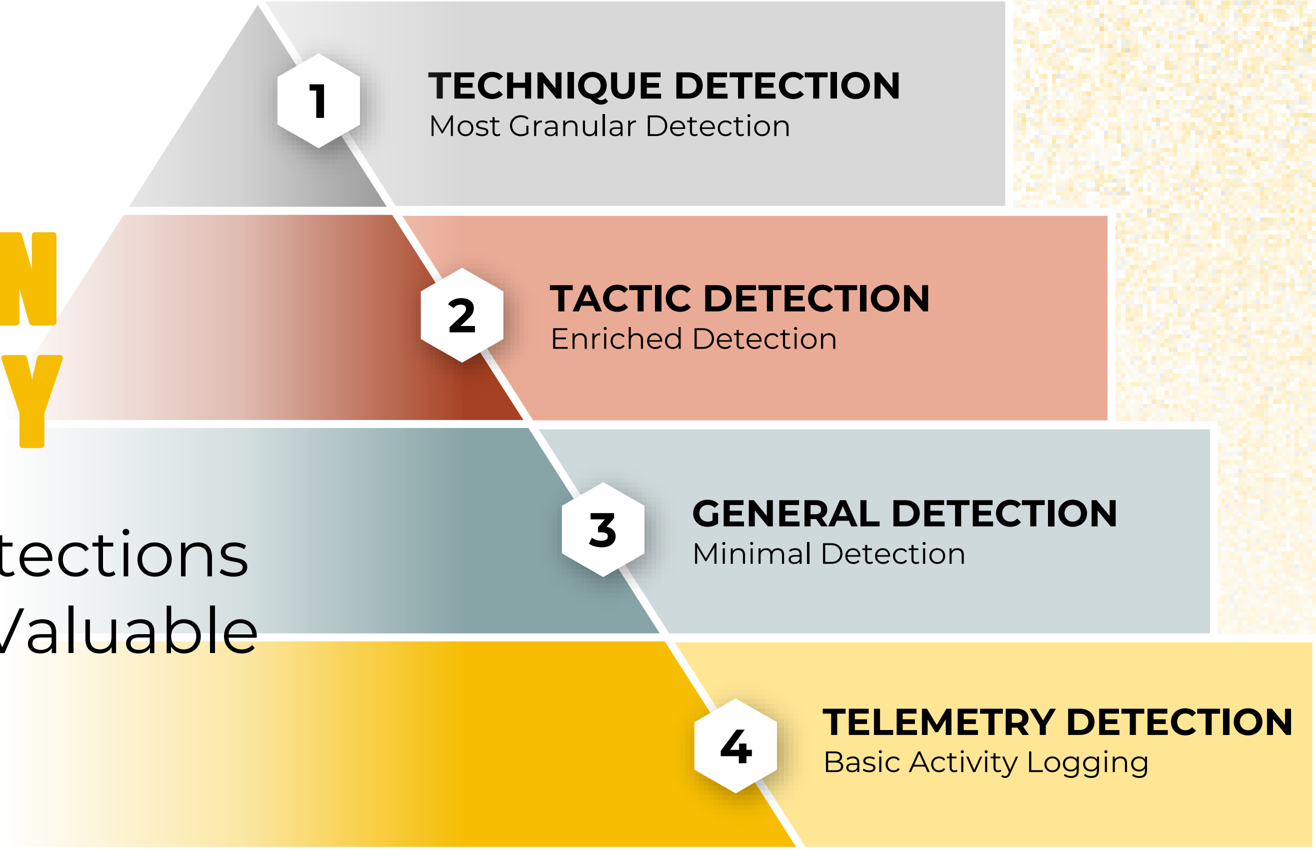


*Delayed detections and detections requiring configuration changes are not included

cybereason

MITRE DETECTION HIERARCHY

Technique Detections Are The Most Valuable

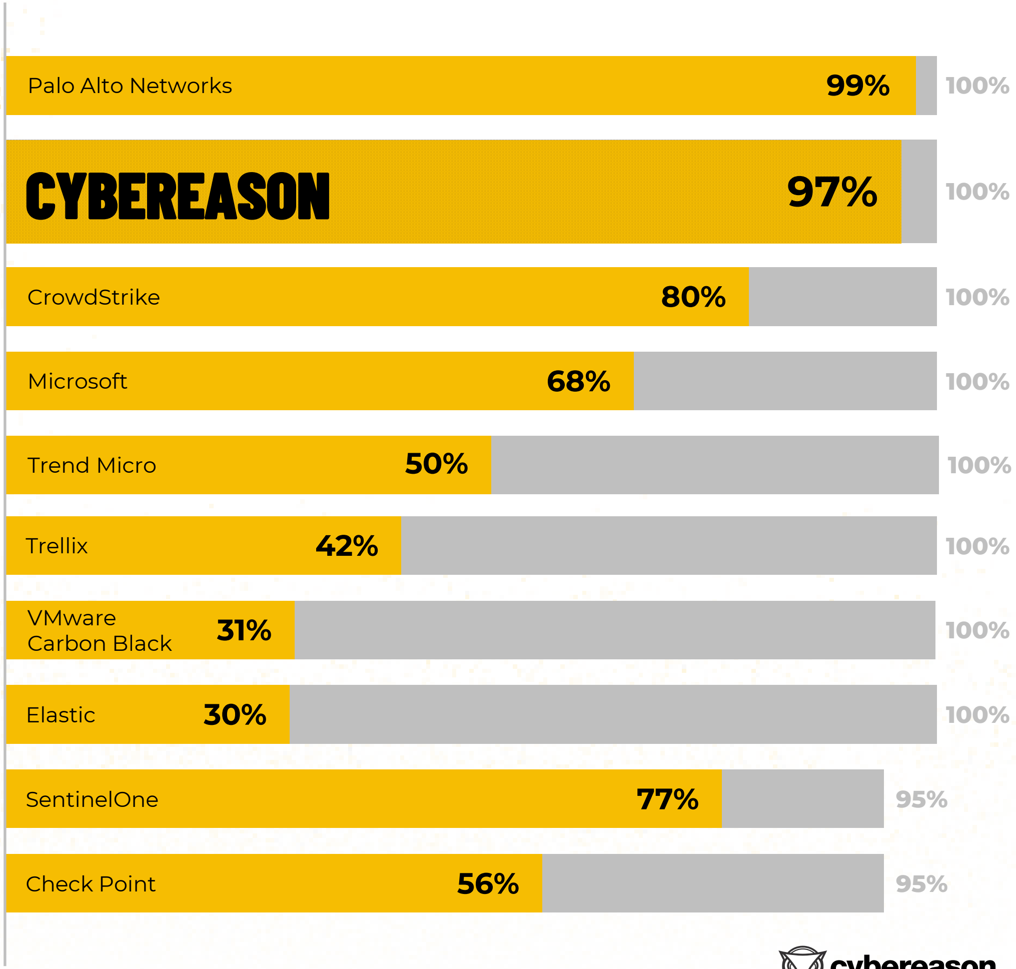


cybereason

MITRE 2023 ATT&CK DETECTION COVERAGE

◼ % of Steps Detected
🟨 % Technique Detections

Subset of participating vendors



*Delayed detections and detections requiring configuration changes are not included

cybereason

WHY WE WIN

MITRE ATT&CK Evaluations
2023

Cybereason NGAV: 9 Layers of Protection

Round 5 of the ATT&CK Evaluations highlights the efficacy of our NGAV with it's 9 layers of unparalleled attack protection. Critical to the 2023 evaluation:

- Variant File Prevention
- Fileless Protection
- Variant Payload Prevention
- Behavioral Execution Protection

The MalOp™

Leveraging an operation-centric approach, the MalOp Detection Engine correlates detections and presents data in an enriched and digestible view.

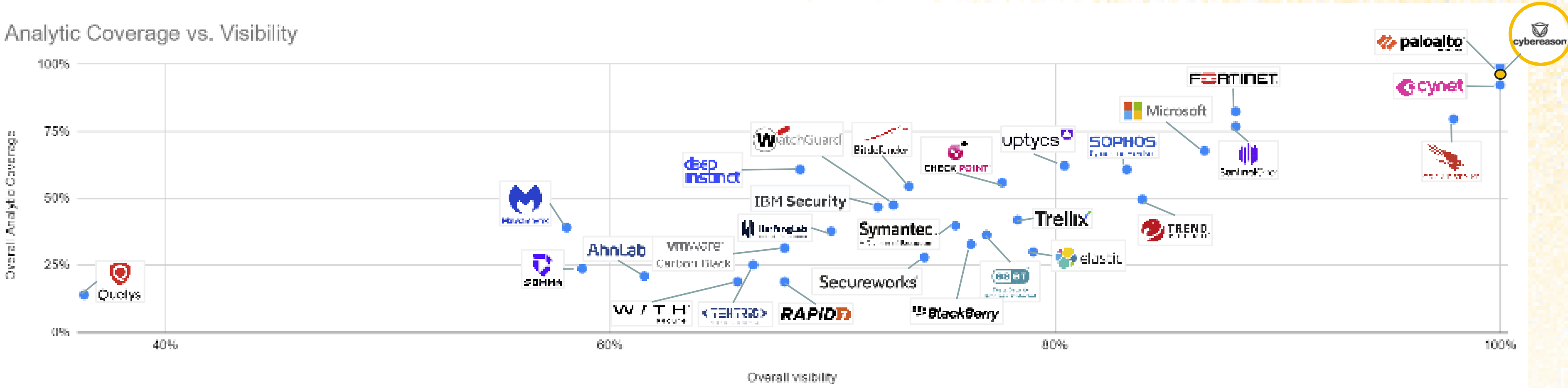
Cybereason EDR: Stop Chasing Alerts

Our market-leading EDR detects sophisticated attack techniques from threat actors right out-of-the-box. Key collection techniques for this test:

- Windows driver-based collections
- Linux eBPF process collections

MITRE 2023 ATT&CK VENDORS

CYBEREASON IS A LEADER AMONG LEADERS



MITRE 2023: Key Metrics to Consider

Vendor	Protection (out of 13 tests)	Detection * (out of 19 steps)	Visibility (out of 143 substeps)	Technique * (out of 143 substeps)	Out of the Box Capability	Real Time Detections
Palo Alto Networks	100%	100%	100%	99%	100%	100%
Cybereason	100%	100%	100%	97%	100%	100%
Cynet	92%	100%	100%	92%	98%	100%
CrowdStrike	100%	100%	98%	80%	97%	91%
SentinelOne	100%	95%	88%	77%	100%	100%
Microsoft	100%	100%	87%	68%	73%	100%
Broadcom Symantec	100%	95%	76%	40%	100%	100%
Trend Micro	100%	100%	84%	50%	78%	91%
Sophos	85%	100%	83%	61%	82%	96%
Elastic	85%	100%	79%	30%	97%	100%
Check Point	92%	95%	78%	56%	76%	100%
Trellix	85%	100%	78%	42%	83%	97%
VMware Carbon Black	77%	100%	68%	31%	100%	99%
Malwarebytes	54%	95%	58%	39%	67%	100%
Rapid7	0%	95%	68%	19%	92%	97%