






MITRE 2022 ATT&CK EVALUATION RESULTS

Wizard Spider and Sandworm Edition

The MITRE ATT&CK Evaluation is performed annually by MITRE Engenuity to test endpoint protection solutions against a simulated attack sequence based on real-life approaches taken by well-known advanced persistent threat (APT) groups. The 2022 MITRE ATT&CK Evaluation included 30 vendor solutions using attack sequences based on the Wizard Spider and Sandworm threat groups.

MITRE does not rank or score vendor results. Instead, the raw test data is published along with some basic online comparison tools. Solution buyers can use the data to evaluate the vendors as they see fit based on their organization's unique priorities and needs.

The following summary table presents all vendor MITRE ATT&CK test results for Overall Detection, Overall Prevention, and a Total Rating. Overall Detection is the total number of attack steps detected across all 109 sub-steps. Overall Prevention measures how early in the attack sequence the threat was detected so that subsequent steps could not execute. Total Rating is the average of these two key scores.

		Linux Covered	Prevention Rate	Detection Rate			Linux Covered	Prevention Rate	Detection Rate
1	 cybereason	Yes	87.16%	100%	16	 Symantec	Yes	47.71%	84.40%
2	 SentinelOne	Yes	89.91%	99.08%	17	 Uptycs	Yes	3.67%	84.40%
3	 paloalto NETWORKS	Yes	88.99%	98.17%	18	 eset	Yes	33.94%	83.33%
4	 Cynet	Yes	88.07%	98.17%	19	 CISCO	Yes	67.89%	82.57%
5	 McAfee	Yes	59.63%	98.17%	20	 vmware Carbon Black	Yes	50.46%	82.57%
6	 Bitdefender	Yes	N/A	97.25%	21	 CYLANCE	Yes	75.23%	81.65%
7	 FORTINET	No	73.33%	96.67%	22	 FIREEYE	Yes	55.05%	81.65%
8	 CROWDSTRIKE	Yes	84.40%	96.33%	23	 SOPHOS	Yes	44.95%	80.73%
9	 TREND MICRO	Yes	71.56%	96.33%	24	 REAQTA	No	N/A	78.89%
10	 CHECK POINT	Yes	55.96%	94.50%	25	 F-Secure	Yes	N/A	76.15%
11	 Malwarebytes	No	82.22%	92.22%	26		No	N/A	75.56%
12	 AhnLab	No	74.44%	92.22%	27	 Qualys	No	N/A	73.33%
13	 elastic	Yes	N/A	89.91%	28	 CYCRAFT	Yes	39.45%	70.64%
14	 Microsoft	Yes	85.32%	89.91%	29	 deep instinct	No	46.79%	70.00%
15	 Fidelis Cybersecurity	Yes	N/A	86.24%	30	 RAPID7	Yes	N/A	56.88%

Cynet analysis of 2022 MITRE ATT&CK results

* N/A - The vendor did not participate in the Protection test

Cynet MITRE 2022 Results

Cynet performed strongly in this year's MITRE ATT&CK evaluation, outperforming the majority of vendors in several key areas. Here are the top takeaways:

- Cynet achieved 100% visibility and detection across each of the 19 MITRE ATT&CK steps evaluated.
- Cynet achieved 100% protection rate across 9 tests conducted by MITRE.
- Cynet is #3 vendor in number of prevented attacks and in speed of prevention in total
- Cynet is #3 vendor in detection coverage (visibility=98.2%) across all sub-steps (107 of 109 sub-steps) conducted in the MITRE ATT&CK® Evaluation
- Cynet detected 98.5% of the techniques presented (65 of 66 unique techniques) in the MITRE ATT&CK® Evaluation, demonstrating the platform's ability to provide visibility and protection across the entire ATT&CK® Kill Chain.