cynet

MITRE ENGENUITY

2024 MITRE ATT&CK Evaluations: Enterprise

2024

ENTERPRISE

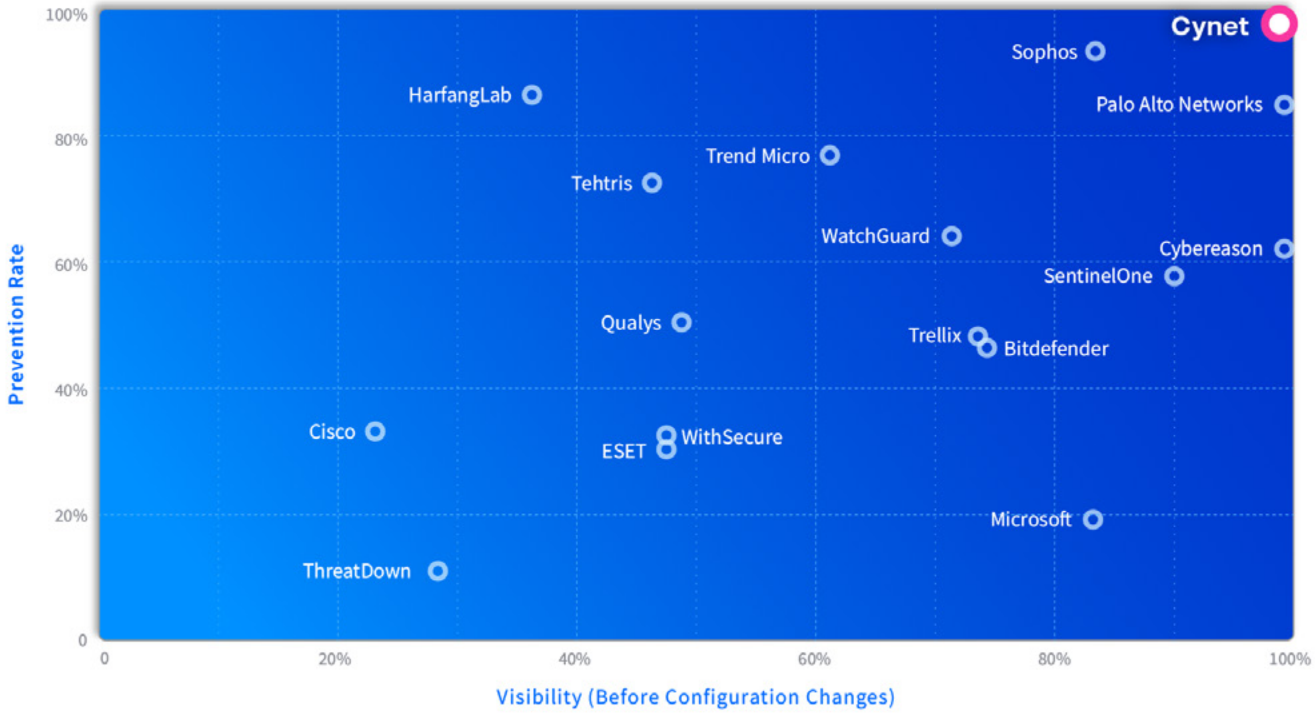
ATT&CK Evaluations

ONLY Cynet Delivers 100% Protection and Detection Visibility in the 2024 MITRE ATT&CK Evaluations: Enterprise

Cynet stands out as the only provider to deliver both 100% protection and 100% detection visibility with zero configuration changes and zero delayed detections.

The results of the sixth round of the MITRE ATT&CK Evaluations: Enterprise are now available. Only Cynet detected 100% of the threats tested in the Detection Phase and blocked 100% of the attacks simulated in the Protection Phase of the Evaluation. While every vendor will spin their results and claim 100% of anything and everything, we created this guide to help you interpret the raw data.

Cynet's results prove that small to medium sized businesses, including MSPs and MSSPs, can now obtain highly effective cybersecurity without breaking the bank.



Visibility vs. Prevention Rate - 2024 MITRE ATT&CK Enterprise Evaluations

Charting Visibility with Prevention illustrates how well a solution does in detecting threats and blocking malicious attacks. Visibility is the percentage of all threats detected in the Detection Phase. Prevention is the percentage of all threats blocked in the Protection Phase. These two metrics are clear indicators of a solution's ability to protect against dangerous attacks across the MITRE ATT&CK framework.

Cynet is the only vendor that delivered BOTH 100% Visibility, 100% Protection and 100% Prevention with no configuration changes! We couldn't be prouder of this performance milestone.

These measurements and all results are discussed in detail in the following sections.

SMEs and MSPs Struggle with Cybersecurity

Most small to medium sized enterprises (SMEs) and the managed service providers (MSPs) that serve this market spend untold billions on very expensive, highly complex security solutions that were built for very large enterprises with very large cybersecurity teams. As expected, these solutions overwhelmed the smaller companies while barely improving their security posture.

SMEs and MSPs need highly accurate threat detection solutions that don't drown their staff with a deluge of false positive alerts. Luckily, the 2024 MITRE ATT&CK Evaluations — the most widely trusted resource to track which solutions are effective — is now available.

The Proof is in the Pudding?

One of the most reliable methods for evaluating the effectiveness of cybersecurity solutions is unbiased, 3rd party testing. In the most trusted technical test of endpoint security solutions – the MITRE ATT&CK Evaluation - Cynet absolutely crushed it. **Cynet DETECTED every single threat and PROTECTED against every attack sequence tested.** While some vendors detected threats after reconfiguring their solution and retesting, or with the aid of a cybersecurity expert review – Cynet automatically and instantly detected and blocked every single threat presented. **Every. Single. One.**

And that's not all! Not only did Cynet detect every single threat, but it was able to provide the most detailed information possible about all detected threats (what MITRE calls Technique-level information). And if that's not enough, **Cynet generated no false positive alerts**.

You might be asking, "how can Cynet outperform the largest security companies in the world"? Well, we're happy you asked that question! You see, at Cynet we spend the vast majority of our budget on research and development to continuously improve and expand our capabilities. We also employ the most highly skilled, battle tested cybersecurity experts in the world. While many larger vendors focus on marketing, we focus singularly on protection.

At Cynet, we do one thing and do it very well – provide extensive, effective, intuitive cyber-protections for MSPs and SMEs. Below you will find an overview of the 2024 MITRE Engenuity ATT&CK® Evaluations: Enterprise. We also provide advice and considerations for using the MITRE ATT&CK results to help determine which security vendor best aligns with your specific needs. To be clear, MITRE does not rank vendors or declare winners or losers. The analysis herein is Cynet's assessment of the latest round of MITRE testing.

MITRE ATT&CK® Evaluations Approach

MITRE uses simulated attacks in a controlled lab environment to evaluate how vendor solutions behave against a set of threats introduced in the exact same manner. Vendor solutions are tested consistently, without external, extraneous factors influencing the results as is the case in a real-world deployment.

This approach helps evaluate how effectively a solution can detect an abundance of discrete steps that might be used by an adversary to carry out an attack. Because MITRE uses the techniques of real threat groups, each technique presented represents what is likely to happen in a real-world scenario.

The evaluation allows vendors to demonstrate whether their solution detects the threats presented as well as the information provided with each detection.

An Important MITRE Evaluation Caveat

It's always important to reiterate that MITRE does not include any type of scoring or ranking of results. Instead, the raw test data is published along with some basic online comparison tools. Buyers can use the data to evaluate the vendors as they see fit based on their organization's unique priorities and needs.

For buyers, this means all vendor claims must be taken with a grain of salt. Buyers should read through all results to determine which measures best suit their particular needs and weigh these results alongside other factors necessary to vendor evaluation.

How MITRE Evaluated Endpoint Protection Solutions

This year's evaluation consisted of two major phases: Detection and Protection. The Detection phase evaluates each solution's ability to detect a variety of commonly used threats. The Protection phase evaluates each solution's ability to block a sequence of threat techniques commonly used in an attack scenario.

Detection Phase

Detections represent the heart of the MITRE ATT&CK Evaluations. The ability to detect threats is the fundamental measure of an endpoint protection solution. Missing threats can allow an attack to expand and ultimately lead to a breach or other catastrophic outcome.

This year, the Detection portion of the MITRE ATT&CK Evaluations focused on a general set of attacks targeting macOS and ransomware attacks targeting Windows and Linux. For the first time, MITRE also executed legitimate actions to help evaluate each solution's false positive rate.

A total of 80 malicious and 21 legitimate actions (sub-steps) were executed across 16 major steps in the Detection phase. To emulate these attacks, MITRE replicated techniques used by well-known ATP groups across three separate scenarios.

- **Democratic People's Republic of Korea (DPRK)** - These emulations featured adversary behavior inspired by the DPRK's targeting of macOS via multi-staged and modular malware that involved privilege escalation, persistence, credential access and exfiltration.

  The DPRK attack sequence featured attack 24 techniques (sub-steps) spread over 4 attack steps (Command and Control, Persistence, Defense Evasion, Collection)

- **CL0P** - These emulations featured common behaviors employed by CL0P, a Russian-speaking ransomware gang, targeting Windows machines. Known for its multilevel ransomware attack techniques, the emulation included installing an in-memory RAT payload, executing ransomware, performing several evasion techniques, and exfiltrating files.

- **LockBit** - These emulations showcased attacks used by LockBit, a notorious ransomware as a service (RaaS) group, targeting both Windows and Linux operating systems. This emulation included access to a Windows machine via compromised credentials, persistence, discovery, defense and a transition to a Linux server and ultimately exfiltrating encrypted files and detonating ransomware.

For every threat tested, MITRE collected the following information to help evaluate each solution's effectiveness.

Detected

This measures how many of the 80 malicious sub-steps were detected by the solution. While this may seem straightforward, each detection is accompanied by three additional important pieces of information discussed further below.

Important – Each vendor may or may not share the following information depending on their testing performance. It's important, however, to evaluate each vendor's performance considering the following factors.

Analytic Coverage

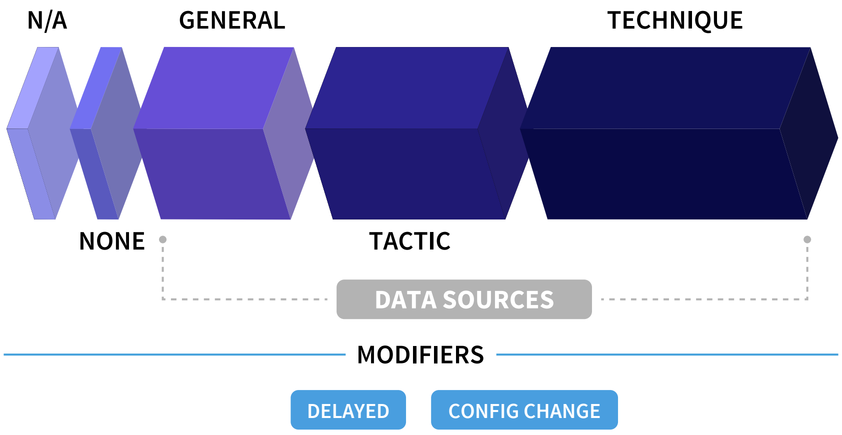
Each successful detection was categorized based on detection quality – the level of context provided to for each detection. Identifying the specific MITRE ATT&CK Technique is best detection quality outcome as it provides the richest information about the detected threat for security analysts.

Analytic detections are critical for security analysts to investigate and respond to alerts. The three levels of analytic alerts in order of increasing value are:

- **General** – informs that a malicious activity occurred, where it occurred, when it happened, and who performed the action

- **Tactic** - adds information about why an activity may have occurred

- **Technique** – adds information about the specific action the attacker used. Technique level alerts provide analysts with the richest information possible to act on a detected threat.



MITRE ATT&CK Evaluation Detection Categories

Detection Modifiers

Each successful detection can potentially include two modifiers indicating that a detection was not accomplished automatically, without human intervention the first time it was presented. Ideally, every detection should be accomplished with no modifiers.

- **Configuration Changes**

  MITRE allows vendors to reconfigure their systems to attempt to detect threats that they missed. The Configuration Change modifier indicates that the threat was originally missed, then on the final day of testing the vendor was allowed to reconfigured their system and given a second chance to detect the threat that was missed on the first day of testing.

  In the real world there are no do-overs or second chances.

  The more realistic measure of a vendor's threat detection effectiveness is detections without the configuration change modifier. As you review MITRE ATT&CK Evaluation outcomes, make sure that the vendor's detections were not accomplished only after they were allowed to make configuration changes.

- **Delayed Detections**

  MITRE explains "If human action or intervention is required to augment an autonomously generated event in order to meet the documented Detection Criteria, then the Delayed modifier will be applied."

  A multi-stage cyberattack can lead to stolen data or ransomware detonation in a matter of minutes. Speed matters. Relying on human intervention means you're dependent on an individual being instantly available to perform a manual intervention, which results in highly variable outcomes.

False Positives

This year MITRE stepped up its game by executing benign activities intermixed with malicious activities. If a tool incorrectly alerte on or blocked benign activity as malicious or suspicious (via a detection or automated protection), it was marked as a false positive alert. Benign activities included actions such file-sharing activities between authorized users or legitimate systems maintenance tasks.

Protection Phase

The Protection phase was executed using a different evaluation plan than the Detection phase (unlike previous years where both Protections and Detections shared the same emulation plan).

The Protection phase consisted of 21 sub-steps organized into 10 major steps. For each step, the sub-steps were executed in order until one was detected, and the step was considered to be blocked. Once a sub-step in a step was blocked, all subsequent sub-steps in that step were considered to be blocked. If any sub-step in a step was blocked, the step was marked as Protected.

Ideally, a solution would block the first sub-step in each of the 10 steps to achieve 100% Prevention. That is, because every step was blocked in the first sub-step, all sub-steps were prevented from executing.

Like the Detection phase, MITRE also executed legitimate actions to help evaluate each solution's false positive rate. If a tool incorrectly generated an alert for a benign activity, it was considered a false positive.

Delayed Modifier

As with the Detection Phase, Protections could also receive the Delayed modifier, meaning that human intervention was required to block the behavior being tested. And again, delays are always undesirable and subject to human error, so Protections without delays are ideal.

Cynet Results

Cynet's 2024 ATT&CK Evaluations results are exceptional by any measure. Cynet excels in every category, in line with our strong ATT&CK Evaluation results from previous rounds. Our results demonstrate the unmatched effectiveness of the Cynet All-in-One platform for protecting your organization with an effective, yet highly intuitive, cost-effective solution.

MITRE ATT&CK 2024 EVALUATIONS RESULTS
CYNET PERFORMANCE HIGHLIGHTS

100%
Detection Visibility

77 of 77 Attack Sub-Steps with NO CONFIGURATION CHANGES

100%
Protection

21 of 21 Malicious Sub-Steps Blocked

100%
Technique Coverage

77 of 77 Technique level Detections with NO CONFIGURATION CHANGES

0 False
Positive Detections

0 of 20 Legitimate Sub-Steps Flagged as Malicious

cynet

Cynet delivered 100% detection visibility - perfectly detecting every attack action *using no configuration changes and no delays*

The ability to detect threats is the fundamental measure of an endpoint protection solution. Detecting attack steps across the MITRE ATT&CK sequence is critical for protecting the organization. Missing any step can allow the attack to expand and ultimately lead to a breach or other catastrophic outcomes.

This year, the attack sequence was executed over 16 steps, which were broken out into 80 malicious sub-steps. During Cynet's testing, 3 of the sub-steps were not executed due to technical reasons and are considered N/A (not counted) which resulted in 77 total sub-step executed. **Cynet detected every single one of the 77 sub-steps.** Cynet had ZERO misses in this year's MITRE testing and detected 100% of attacks over **Windows** and **MacOS** devices as well as **Linux** servers.

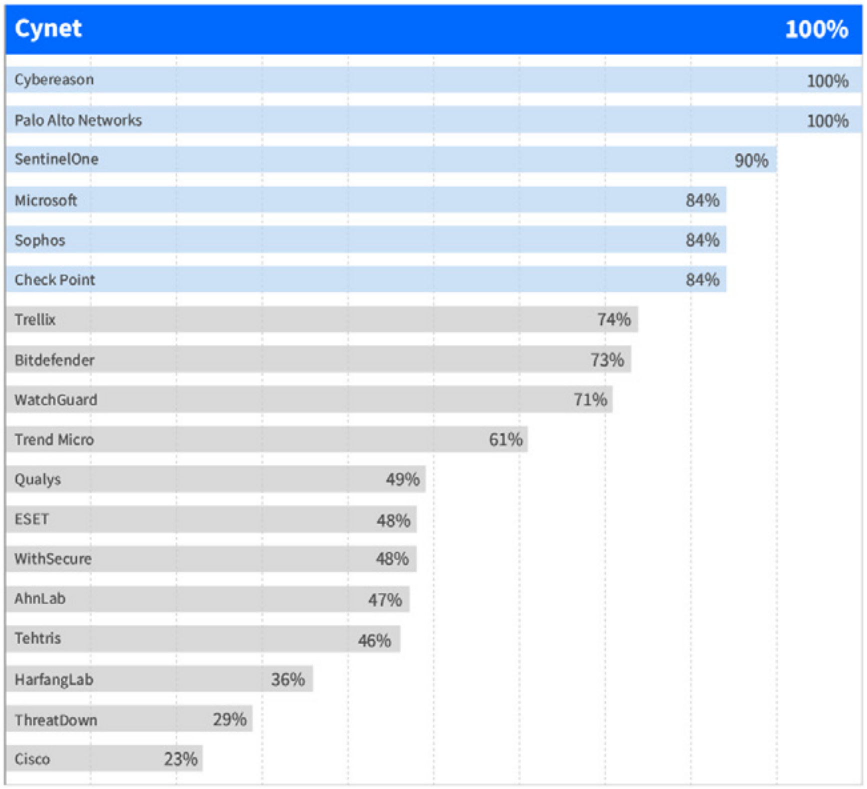
As importantly, every one of the 77 detections was done without the need for configuration changes. As you review MITRE ATT&CK Evaluations reports, we believe the measurement that more reflects real-world performance is detections before configuration changes.

> Another important note when reviewing other vendor claims: Some vendors will define Visibility or Detection as detecting any one of the sub-steps within each step. A vendor could only detect one sub-step in each of the 16 steps and declare 100% success. Don't be fooled by vendor headlines and definition manipulation – look at the data to assess each vendor for yourself and make sure Visibility or Detections refer to total sub-step detections.

MITRE ENGENUITY

2024 MITRE ATT&CK EVALUATIONS VISIBILITY

(Before Configuration Changes)



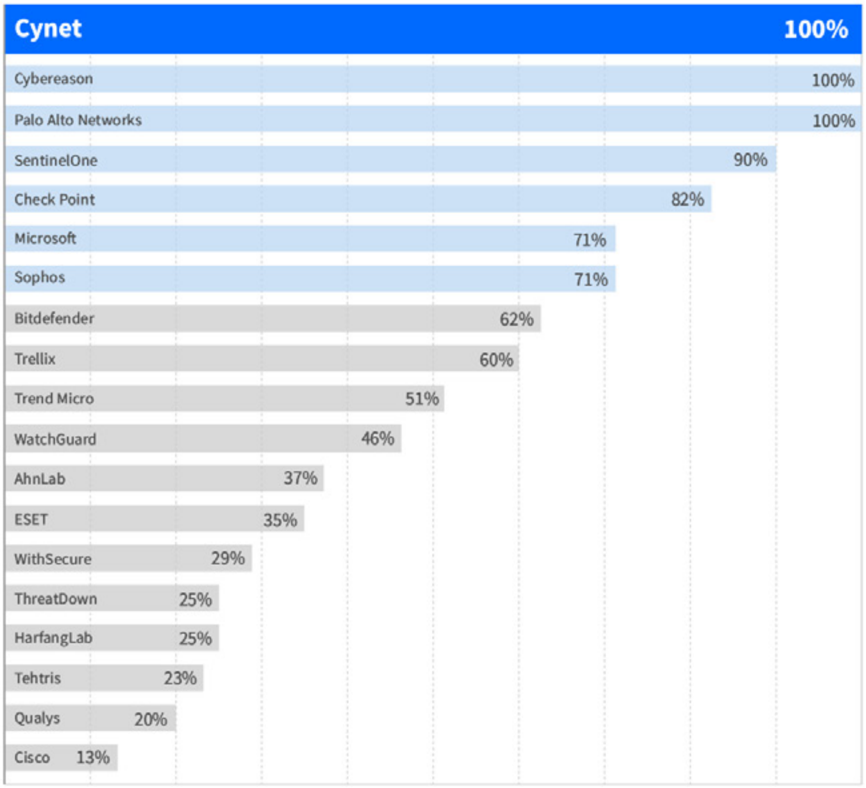
Cynet provided the highest quality (Technique -level) analytic coverage for 100% of the attack steps *using no configuration changes*

Cynet provided Technique-level information for every one of the 77 steps detected in the attack sequence, which is the highest-level quality detection achievable in the evaluation. Again, it's important to note that vendors were allowed to reconfigure their systems to improve their analytic coverage results for each step. All Cynet analytic information was provided without the need for any configuration changes.

MITRE ENGENUITY

2024 MITRE ATT&CK EVALUATIONS TECHNIQUE LEVEL COVERAGE

(Before Configuration Changes)



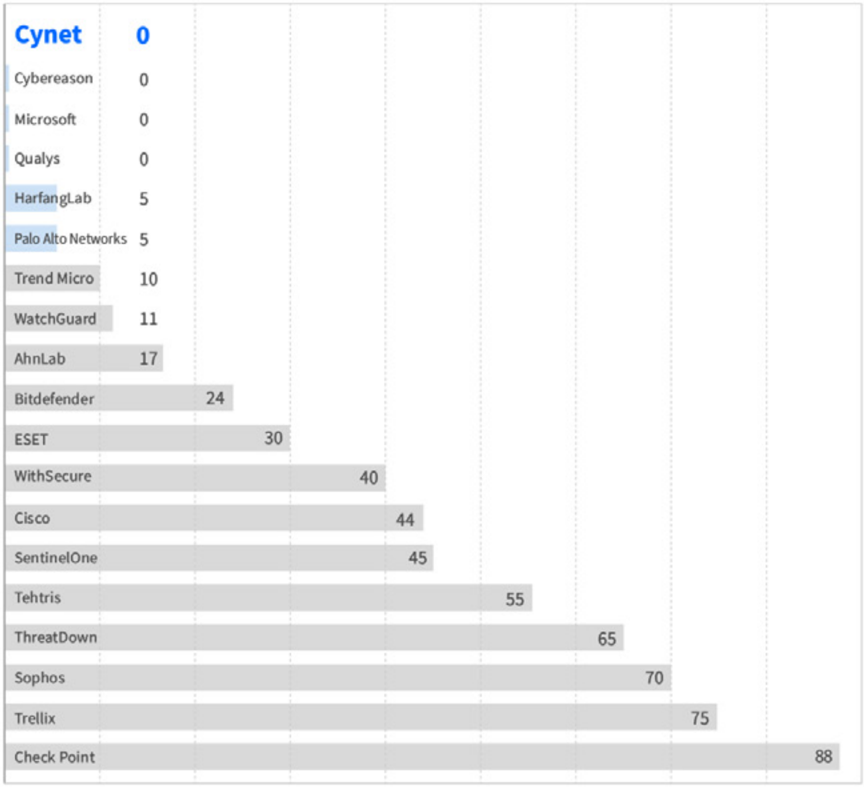
Cynet reported no false-positive Detection alerts

During the Detection phase, MITRE introduced up to 20 legitimate actions to determine whether it would be mistakenly reported as malicious – a false positive alert. Because some vendors did not execute all sub-steps due to technical reasons, the number of legitimate actions tested may be less than 20. **Cynet generated no false positive detections, generating no alerts for the 20 benign actions tested.** Minimizing false positives means security analysts don't waste their time chasing false alerts, focusing only on the dangerous threats that really matter.

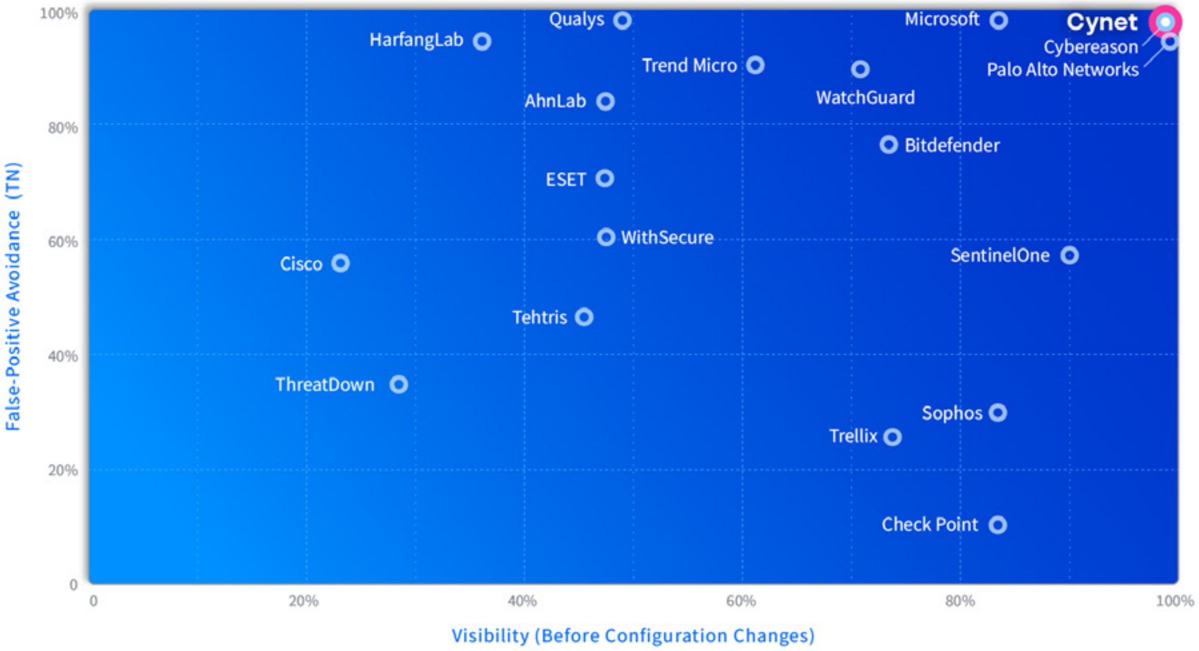
MITRE ENGENUITY

2024 MITRE ATT&CK EVALUATIONS DETECTIONS FALSE-POSITIVE RATE

(Before Configuration Changes)



Another interesting measure is comparing Visibility to False Positive Rate. In the real world, protection solutions struggle to balance detection accuracy with the number of false positive alerts generated. Some solutions generate alerts for almost anything, creating the well-known problem of alert overload. Ideally, a solution will detect all actual threats and not mistakenly alert on benign activities. Comparing Visibility (the ability to alert on real threats) with False-Positive Avoidance (to the percent of time the solution did not generate false positive alerts) during the Detection Phase is a great indicator of detection accuracy. **Cynet achieved both 100% Visibility and 100% False-Positive Avoidance (0 false positives).**



Visibility (before Configuration Changes) vs. False Positive Avoidance for Detection Phase - 2024 MITRE ATT&CK Enterprise Evaluation

Cynet delivered 100% Protection – blocking every attack step attempted

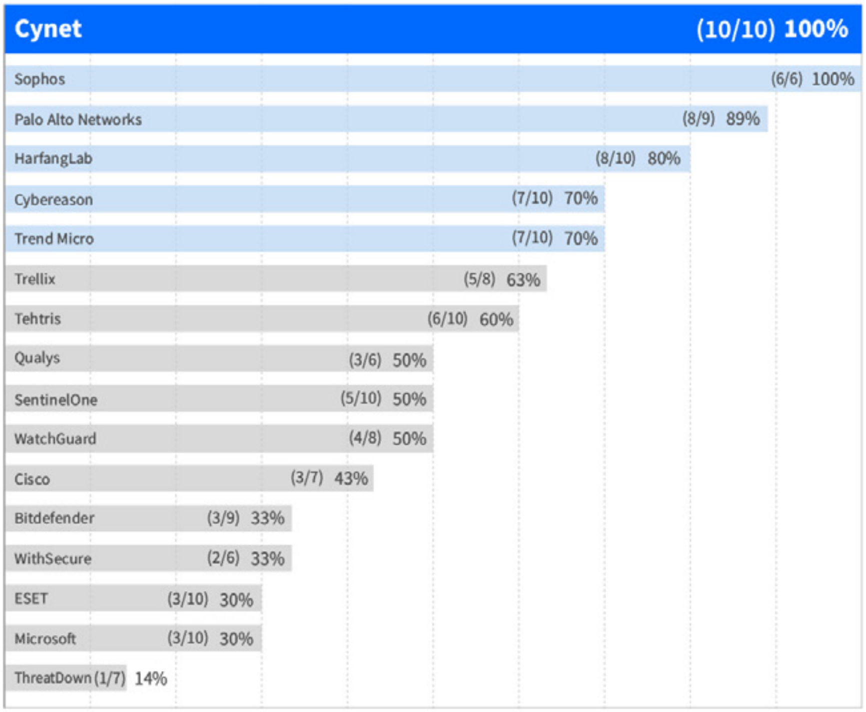
The 2024 MITRE Evaluation experienced a number of technical issues which led to the inability to execute all tests for all vendors. This was especially true in the Protection tests where roughly half of the participants were not able to complete all 10 attack steps in the plan. MITRE was able to execute all 10 attack steps for Cynet. **Cynet blocked every one of the 10 attacks steps - allowing no malicious activity to execute!**

Note: Around half of the participating vendors were not able to test all Protection steps due to technical issues. So, the number of Protection steps tested varied between vendors.

The following chart shows each participant's Protection rate along with the number of steps blocked and number of steps tested (steps blocked/steps tested).

MITRE ENGENUITY

2024 MITRE ATT&CK EVALUATIONS PROTECTION RATE



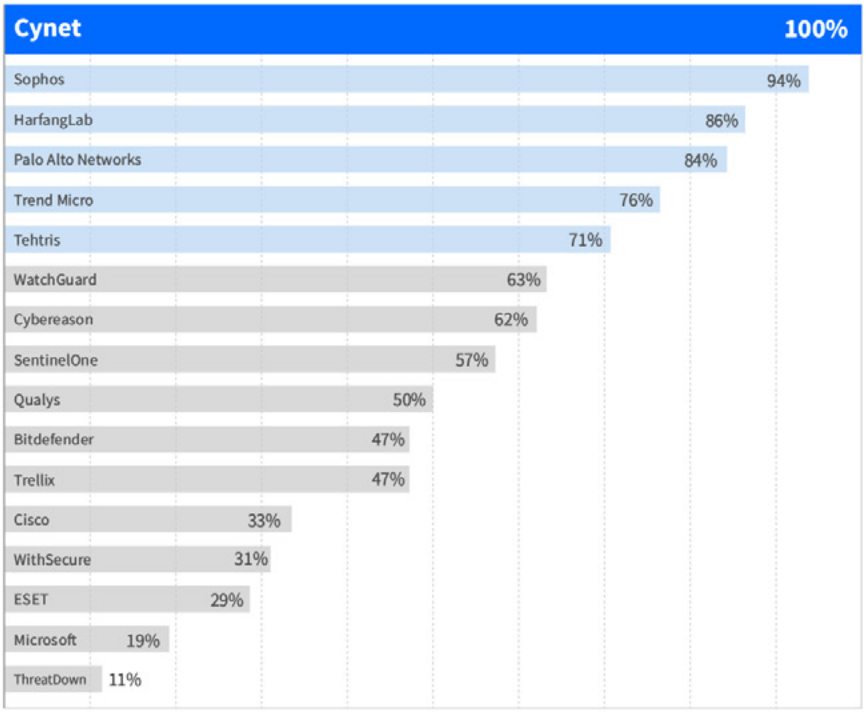
Cynet delivered 100% Prevention – blocking every attack in the first step attempted

Protection measures whether any sub-step in a Protection step was blocked. For example, if a step consisted of 5 sub-steps, a vendor could miss the first four, block the fifth and consider the entire step blocked. Cynet defines Prevention as how quickly (early) in each of the 10 attack steps the threat was prevented.

Prevention measures the percentage of sub-steps that were blocked from executing. Ideally a vendor would block the first sub-step in every step tested so that every subsequent sub-step in the step was considered to be blocked. Using this measure, **Cynet is the only vendor to achieve 100% Prevention - blocking every one of the 21 Protection sub-steps from executing.**

MITRE ENGENUITY

2024 MITRE ATT&CK EVALUATIONS PREVENTION RATE



Cynet required zero Configuration Changes to achieve 100% Detection Visibility, 100% Technique-Level Coverage, 100% Protection and 100% Prevention

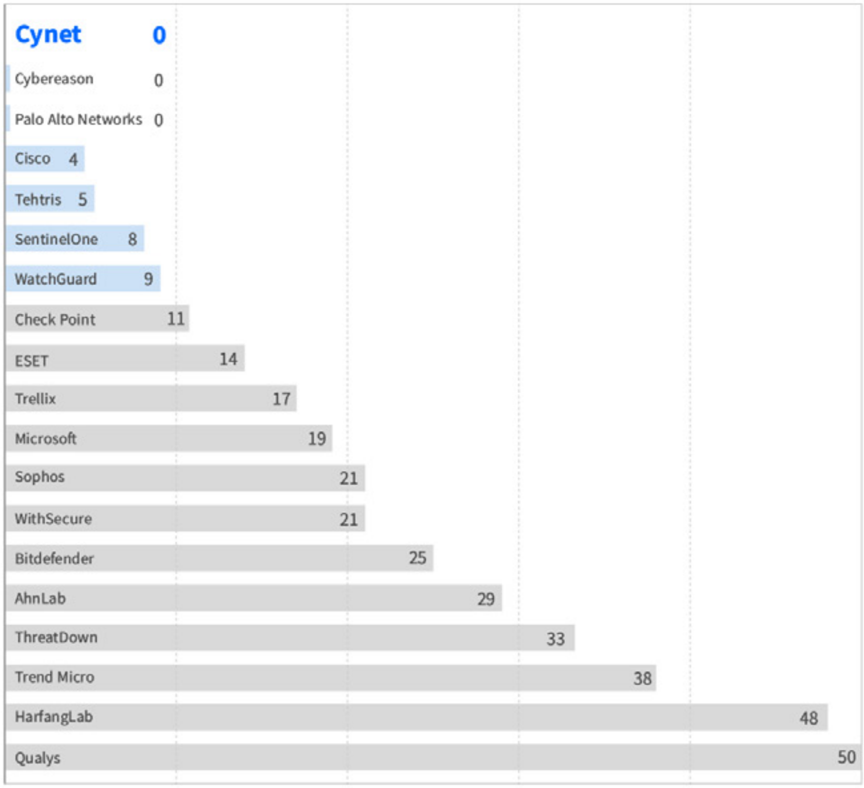
After the Detection tests are complete, MITRE allows vendors to make changes to their systems and retest the entire attack sequence. That is, after the vendor knows they missed detections or provided limited analytic coverage, it could change their configuration to include new data source, change detection logic or modify the data accessed and again attempt to detect the known missed threats.

This year, some vendors made a significant number of configuration changes before retesting. When reviewing any vendor claims regarding MITRE ATT&CK Evaluations results, it's important to know whether the results occurred with or without configuration changes. Many vendors report results without divulging the results only occurred after they implemented configuration changes.

All Cynet results reported in this guide were achieved with no configuration changes.

MITRE ENGENUITY

2024 MITRE ATT&CK EVALUATIONS NUMBER OF CONFIGURATION CHANGES



Key MITRE Evaluation Metrics

With so many metrics generated from the MITRE testing, the following table helps summarize vendor performance across several key measures. All measures shown are before Configuration Changes – the more realistic measure of each vendor's performance. Note that the definitions below were created by Cynet based on test results data.

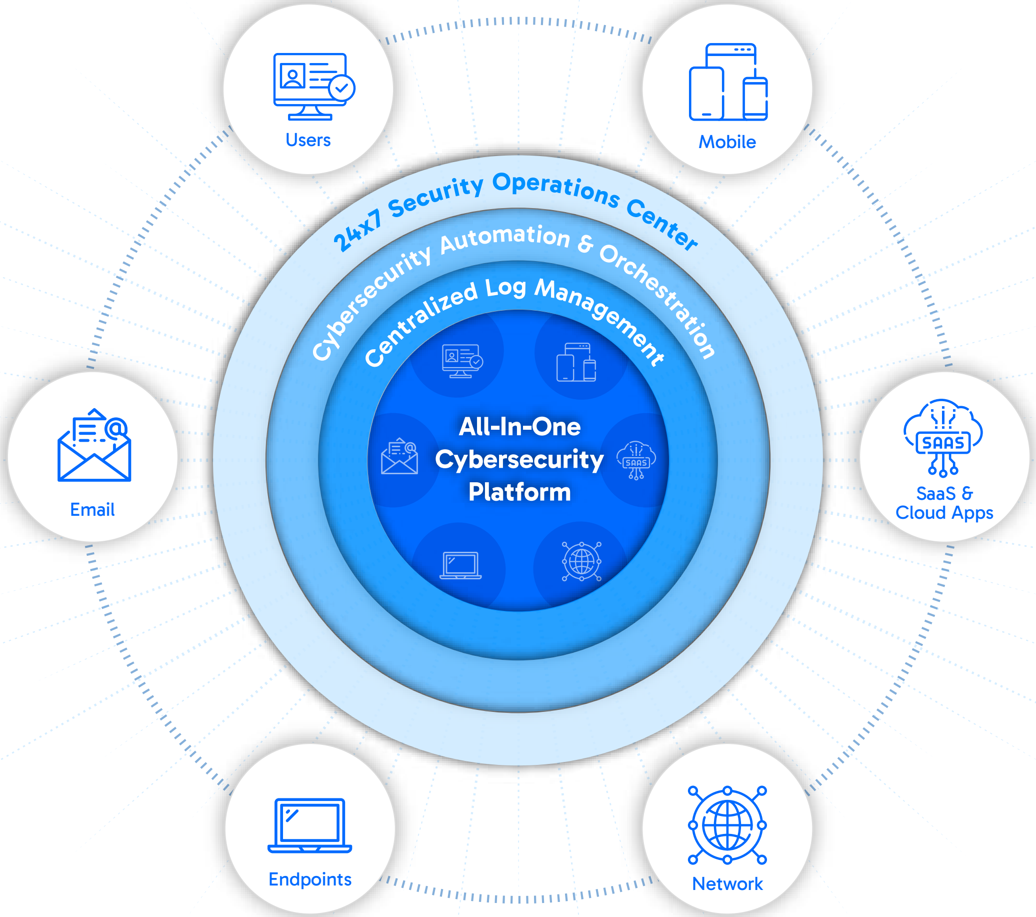
- **Visibility** - the number of threats detected out of the total number of malicious threats actions
- **Visibility %** - the ratio of detected threats vs. total malicious threats
- **Detection False Positive** – the number of false positive alerts generated out of the total number of benign actions presented
- **Detection False Positive %** - the ratio of false positive alerts vs. total benign actions
- **Protection** – the total number of steps where a vendor had at least one sub-step blocked out of the total number of protection steps for that vendor (not including steps that were N/A)
- **Protection %** - the ratio of steps with at least one blocked sub-step to total protection steps tested
- **Prevention** – the total number of sub-steps considered to be blocked in the protection tests
- **Prevention %** - the ratio of blocked sub-steps to the total number sub-steps executed for that vendor
- **Protection False Positive** – the number of false positive alerts generated out of the total number of benign actions presented
- **Protection False Positive %** - the ratio of false positive alerts to the total number of benign actions presented.

Vendor	Visibility	Visibility %	Detection False-Positive	Detection False-Positive %	Protection	Protection %	Prevention	Prevention %	Protections False-Positive	Protections False-Positive %
Cynet	**77/77**	**100.00%**	**0/20**	**0.00%**	**10/10**	**100.00%**	**21/21**	**100.00%**	**3/28**	**10.71%**
Palo Alto	80/80	100.00%	1/20	5.00%	8/9	88.89%	16/19	84.21%	1/10	10.00%
Cybereason	79/79	100.00%	0/20	0.00%	7/10	70.00%	13/21	61.90%	6/23	26.09%
SentinelOne	72/80	90.00%	9/20	45.00%	5/10	50.00%	12/21	57.14%	7/26	26.92%
Sophos	67/80	83.75%	14/20	70.00%	6/6	100.00%	15/16	93.75%	0/24	0.00%
Microsoft	67/80	83.75%	0/20	0.00%	3/10	30.00%	4/21	19.05%	0/27	0.00%
Check Point	46/55	83.64%	15/17	88.24%	N/A	N/A	N/A	N/A	N/A	N/A
Trellix	54/73	73.97%	15/20	75.00%	5/8	62.50%	8/17	47.06%	9/28	32.14%
Bitdefender	58/79	73.42%	4/17	23.53%	3/9	33.33%	9/19	47.37%	2/23	8.70%
WatchGuard	40/56	71.43%	2/18	11.11%	4/8	50.00%	12/19	63.16%	6/25	24.00%
Trend Micro	49/80	61.25%	2/20	10.00%	7/10	70.00%	16/21	76.19%	3/10	30.00%
Qualys	22/45	48.89%	0/7	0.00%	3/6	50.00%	7/14	50.00%	2/19	10.53%
WithSecure	38/80	47.50%	8/20	40.00%	2/6	33.33%	5/16	31.25%	0/19	0.00%
ESET	38/80	47.50%	6/20	30.00%	3/10	30.00%	6/21	28.57%	1/28	3.57%
AhnLab	28/59	47.46%	3/18	16.67%	N/A	N/A	N/A	N/A	N/A	N/A
Tehtris	37/80	46.25%	11/20	55.00%	6/10	60.00%	15/21	71.43%	6/16	37.50%
HarfangLab	29/80	36.25%	1/20	5.00%	8/10	80.00%	18/21	85.71%	1/27	3.70%
ThreatDown	17/59	28.81%	11/17	64.71%	1/7	14.29%	2/18	11.11%	1/26	3.85%
Cisco	13/56	23.21%	8/18	44.44%	3/7	42.86%	6/18	33.33%	6/26	23.08%

About Cynet

Cynet's end-to-end, natively automated All-in-One platform, backed by 24/7 security experts, was purpose-built to enable lean IT security teams to achieve comprehensive and effective protection regardless of their resources, team size or skills.

Cynet All-in-One includes the essential security technologies you need to protect your organization – including your endpoints, users, email, network, SaaS and Cloud apps - in one automated, simplified platform that delivers enterprise-grade protections with less manual effort and lower cost.


Users
Mobile
Email
SaaS & Cloud Apps
Endpoints
Network
24x7 Security Operations Center
Cybersecurity Automation & Orchestration
Centralized Log Management
All-In-One Cybersecurity Platform

To learn more about Cynet visit
https://www.cynet.com/