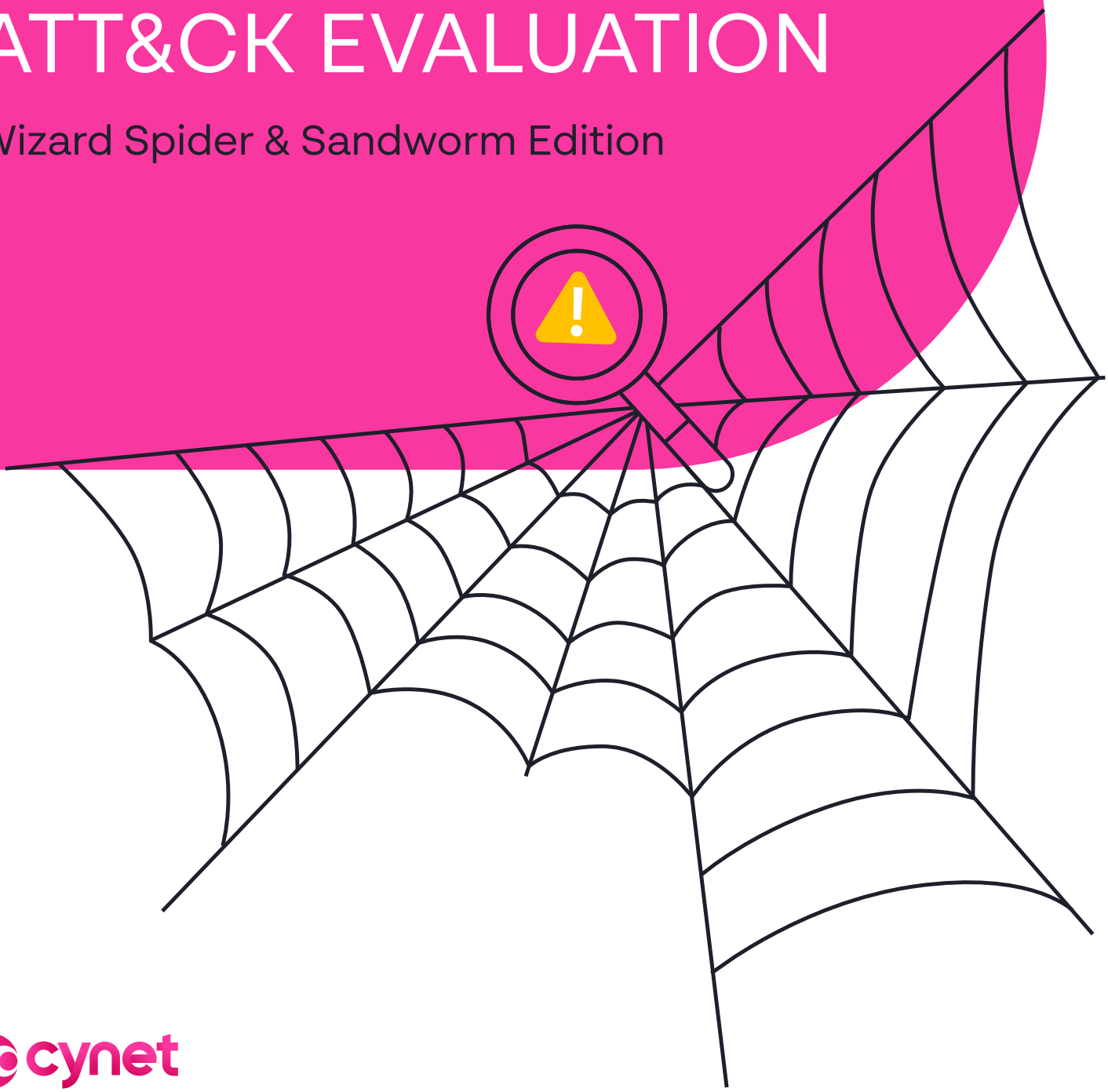
THE PRACTICAL GUIDE TO THE MITRE ATT&CK EVALUATION

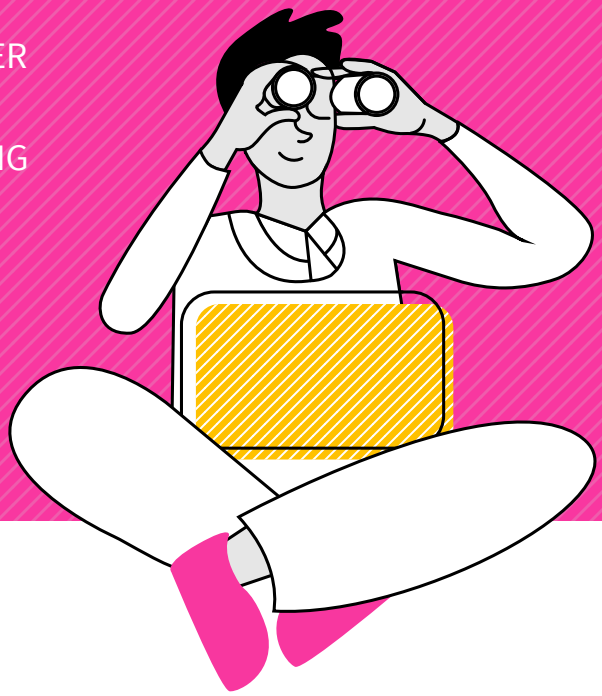
Wizard Spider & Sandworm Edition



cynet

SELECTING THE RIGHT CYBERSECURITY TECHNOLOGY REMAINS AN ARDUOUS TASK.

AS THE VENDOR MARKET EXPANDS AND NEWER TECHNOLOGIES EMERGE, LIKE EXTENDED DETECTION AND RESPONSE (XDR), EVALUATING COMPETING SOLUTIONS IS EXTREMELY TIME CONSUMING AND OVERLY DAUNTING.



Other than running a time- and resource-consuming proof of value (POV) evaluation – a live trial – in your environment and getting trusted client references, evaluating real-world capabilities is difficult.

Fortunately, MITRE's testing methodology objectively evaluates endpoint security solutions, based on the highly regarded MITRE ATT&CK framework.

The evaluation tests the endpoint protection solutions against a simulated attack sequence based on the real-life approaches of well-known Advanced Persistent Threat (APT) groups.

The most recent MITRE ATT&CK evaluation pits 30 vendor solutions against attack sequences based on the Wizard Spider and Sandworm threat groups.

As in the past, MITRE does not rank or score vendor 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 company's unique priorities and needs. But the results are not presented in the familiar four quadrant matrix or ranked using common analyst methodology, making it hard for people to know how to best use the results in their search.

Vendor selection is not a one-size-fits-all methodology. This guide provides advice and considerations for how to use the MITRE ATT&CK results as one component of your selection criteria as you determine which vendor will meet your specific needs.

MITRE ATT&CK EVALUATION – APPROACH

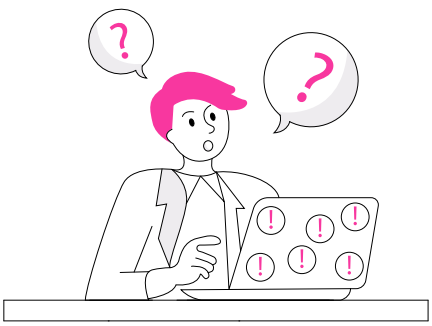
MITRE's use of simulated attacks in a controlled lab environment is a highly helpful approach for comparing the behavior of multiple solutions against the exact same threats introduced in the exact same manner. Along with the myriad benefits of this approach, it's important to note that many important solution capabilities and characteristics are not included in the evaluation.

WHAT IT IS

Let's take it from the top – the MITRE ATT&CK evaluation uses an open, transparent, and unbiased testing process. MITRE provides a level playing field in a controlled environment so that all vendor solutions are tested consistently, without external, extraneous factors influencing the results as is the case in a real-world deployment.

It is not an end-to-end actual attack simulation. Every step and substep is presented regardless of previous detections. Such transparency allows for an evaluation of how effectively a solution can detect an abundance of discrete steps that might be used by a certain threat group to carry out an attack. This coverage ensures multiple attack techniques are tested for each stage of the attack progression through the MITRE ATT&CK framework. Because MITRE uses the techniques of real threat groups, every step represents what is likely to happen in a real-world scenario.

For each technique presented, the evaluation allows vendors to articulate how the threat is (or isn't) detected, the data sources used, and how they correlate with each other to determine a detection. This "under the hood" view contextualizes each capability, in addition to establishing that a detection occurred.



WHAT IT ISN'T

Importantly, MITRE does not include any type of scoring or ranking of results. Any vendor claims of "victory" are based on the vendor's own interpretation of the results and are certainly not endorsed by MITRE.

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.

The MITRE ATT&CK evaluation also does not necessarily test a vendor's full range of threat protection capabilities. As the evaluation focuses on endpoint protection, it doesn't adequately test for other important telemetries that may be included in the vendor solution, such as network traffic, user behaviors, or deception. Nor does it adequately test how a real-world breach protection stack or an XDR solution would perform in detecting and preventing a real-world attack scenario. But, endpoint protection is critical — and the MITRE ATT&CK evaluation remains the best methodology for that component.

While the evaluation includes vendor platform screenshots and other useful measures, it does not evaluate platform usability or implementation and maintenance requirements. It doesn't evaluate false positive rates or breadth and depth of response features and capabilities, or whether individual threats are correlated into incidents. In this year's evaluation, the test's primary focus on detection is complemented with a segment on protection capabilities. As the go-to source for unbiased endpoint protection solution testing, the MITRE ATT&CK evaluation should be an important factor in any buyer's vendor evaluation process — but never the only factor, nor, in many cases, the primary factor.

METHODOLOGY

The 2022 evaluation emulated the attack sequence used by both the Wizard Spider and Sandworm threat groups. MITRE could not have selected a more capable adversary than Wizard Spider, responsible for the development and deployment of several dangerous cybercrime tools.

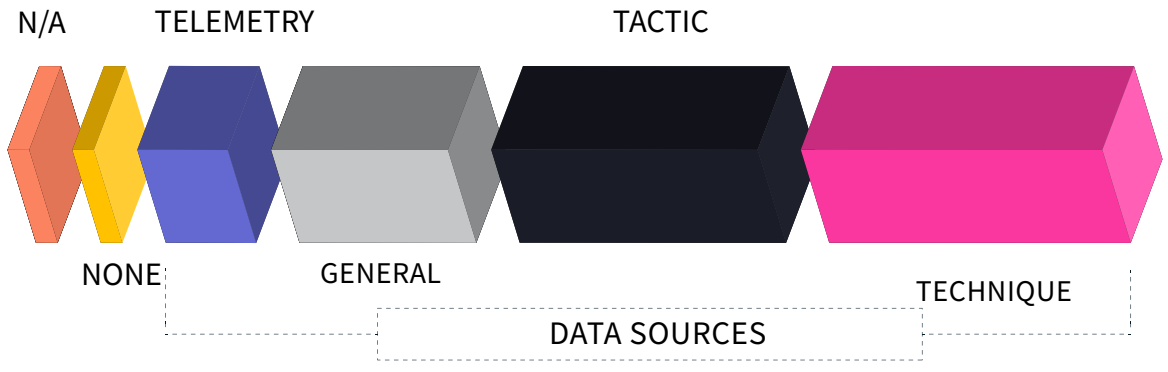
These tools include Conti, Trickbot, and Ryuk ransomware. Wizard Spider has been focused on infecting organizations worldwide with ransomware. Cynet recently discovered Wizard Spider collaborating with threat group Lunar Spider to infect organizations with Conti ransomware.

Often suspected of being a Russian cyber-military unit, Sandworm was responsible for several disruptive cyberattacks against infrastructure targets in Ukraine. The group is also accused of NotPetya malware attacks worldwide and a spear phishing campaign targeting South Korean citizens and officials during the 2018 PyeongChang Winter Olympic Games.

WIZARD SPIDER + SANDWORM THREAT DETECTION ON WINDOWS

After Day one testing focused on attack sequences known to be used by Wizard Spider, Day two focused on Sandworm attack sequences. A total of 54 unique attack techniques were tested to determine the level of detection for each technique on a scale ranging from no detection through identifying the specific technique that was employed.

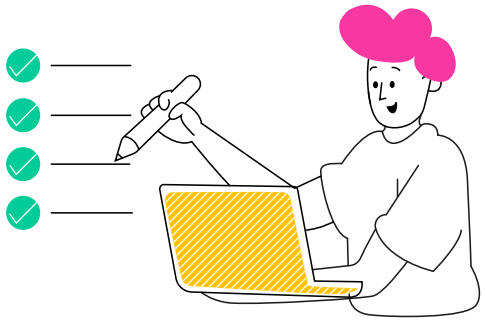
The detection categories indicate increasing levels of context provided to an analyst for each detection, with the best detection outcome specifically identifying the defined MITRE ATT&CK technique or sub-technique.

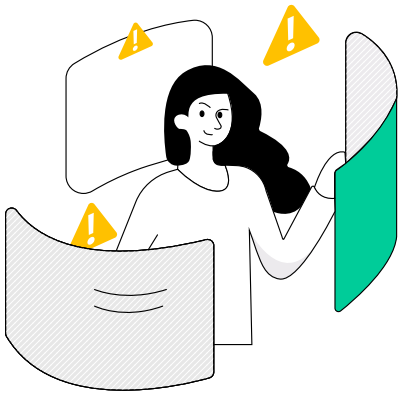


MITRE ATT&CK evaluation detection categories

MITRE ATT&CK EVALUATION DETECTION CATEGORIES

For each of the 30 vendor solutions tested, MITRE lists the detection level(s) achieved for each technique and sub-technique. The test included 109 separate sub-steps over the two days of testing.



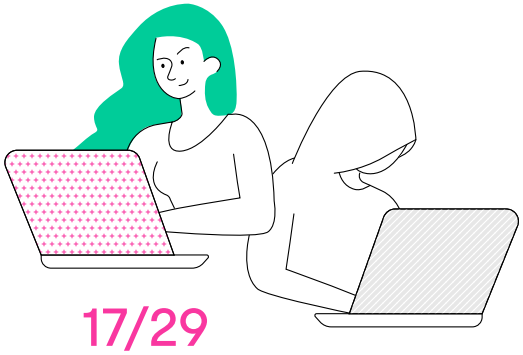


WIZARD SPIDER + SANDWORM THREAT DETECTION ON LINUX

Similar to last year's evaluation, MITRE went beyond Windows and included a separate evaluation of vendor solutions on Linux devices. The Linux evaluation included 22 of the 29 vendors. The expansion to Linux devices confirms the importance of providing protection across the hybrid operating system environments present (and growing) throughout the vast majority of companies. Today, Linux is often used for file servers and domain controllers, both of which are targeted for APT attacks.

WIZARD SPIDER + SANDWORM THREAT PROTECTION

Also, for the first time, MITRE tested each vendor's ability to protect against specific adversary techniques used by these groups. The test involved the solution's ability to block malicious activity across the 10 scenarios tested. Only 17 of the 29 vendors chose to participate in this evaluation.



17/29
Chose to Participate
In This Evaluation

USING MITRE TO EVALUATE ENDPOINT PROTECTION SOLUTIONS

The MITRE ATT&CK results can be a useful element when choosing the best threat protection tool for your organization. As part of any vendor selection exercise, each company will weigh components of the test differently, according to their needs and priorities. Several key measures from the MITRE evaluation will likely be relevant to most organizations at some level, including:

Overall detection across the entire MITRE ATT&CK sequence

Overall protection that measures the ability to block an attack sequence as quickly as possible to prevent subsequent steps from executing

Threat detection in the Linux environment

OVERALL DETECTION CAPABILITIES

Except for so-called “hit and run” attacks, where the attacker may execute malware or ransomware on a single endpoint and steal valuable data or make ransom demands, most meaningful attacks require multiple steps to achieve their goals. The MITRE ATT&CK sequence represents the potential flow of tactics and techniques generally used by attackers for the more dangerous “hit and expand” type of attacks. These attacks begin with an initial endpoint compromise, followed by a long-lasting presence in the environment before valuable data is ultimately exfiltrated.

Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Command and Scripting Interpreter: PowerShell (T1059.001)	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)	Abuse Elevation Control Mechanism: Setuid and Setgid (T1548.001)	Access Token Manipulation (T1134)	Credentials from Password Stores: Credentials from Web Browsers (T1555.003)	Account Discovery: Local Account (T1087.001)	Lateral Tool Transfer (T1570)	Archive Collected Data (T1560)	Application Layer Protocol: Web Protocols (T1071.001)	Exfiltration Over Command and Control Channel (T1041)	Data Encrypted for Impact (T1486)
Command and Scripting Interpreter: Windows Command Shell (T1059.003)	Boot or Logon Autostart Execution: Winlogon Helper DLL (T1547.004)		File and Directory Permissions Modification: Windows File and Directory Permissions Modification (T1222.001)"	Input Capture: Keylogging (T1056.001)	Account Discovery: Domain Account (T1087.002)	Remote Services (T1021)	Email Collection: Local Email Collection (T1114.001)	Encrypted Channel: Symmetric Cryptography (T1573.001)		Inhibit System Recovery (T1490)
Command and Scripting Interpreter: Unix Shell (T1059.004)	Create or Modify System Process: Systemd Service (T1543.002)		Indicator Removal on Host (T1070)	OS Credential Dumping (T1003)	Domain Trust Discovery (T1482)	Remote Services: Remote Desktop Protocol (T1021.001)		Encrypted Channel: Asymmetric Cryptography (T1573.002)		Service Stop (T1489)
Command and Scripting Interpreter: Visual Basic (T1059.005)	Create or Modify System Process: Windows Service (T1543.003)		Indicator Removal on Host: Clear Windows Event Logs (T1070.001)	OS Credential Dumping: Security Account Manager (T1003.002)	File and Directory Discovery (T1083)	Remote Services: SMB/ Windows Admin Shares (T1021.002)		Ingress Tool Transfer (T1105)		System Shutdown/ Reboot (T1529)
System Services: Service Execution (T1569.002)	External Remote Services (T1133)		Indicator Removal on Host: File Deletion (T1070.004)	OS Credential Dumping: NTDS (T1003.003)	Permission Groups Discovery (T1069)	Remote Services: Windows Remote Management (T1021.006)		Non-Standard Port (T1571)		
User Execution: Malicious File (T1204.002)	Scheduled Task/Job: Cron (T1053.003)		Obfuscated Files or Information (T1027)	OS Credential Dumping: /etc/passwd and /etc/ shadow (T1003.008)	Permission Groups Discovery: Domain Group (T1069.002)					
Windows Management Instrumentation (T1047)	Scheduled Task/ Job: Scheduled Task (T1053.005)		Process Injection: Portable Executable Injection (T1055.002)	Steal or Forge Kerberos Tickets: Kerberoasting (T1558.003)	Process Discovery (T1057)					
	Server Software Component: Web Shell (T1505.003)		Signed Binary Proxy Execution: Rundll32 (T1218.011)	Unsecured Credentials (T1552)	Remote System Discovery (T1018)					
			Valid Accounts (T1078)	Unsecured Credentials: Bash History (T1552.003)	System Information Discovery (T1082)					
			Valid Accounts: Domain Accounts (T1078.002)	Unsecured Credentials: Private Keys (T1552.004)	System Network Configuration Discovery (T1016)					
					System Network Connections Discovery (T1049)					
					System Owner/User Discovery (T1033)					
					System Service Discovery (T1007)					

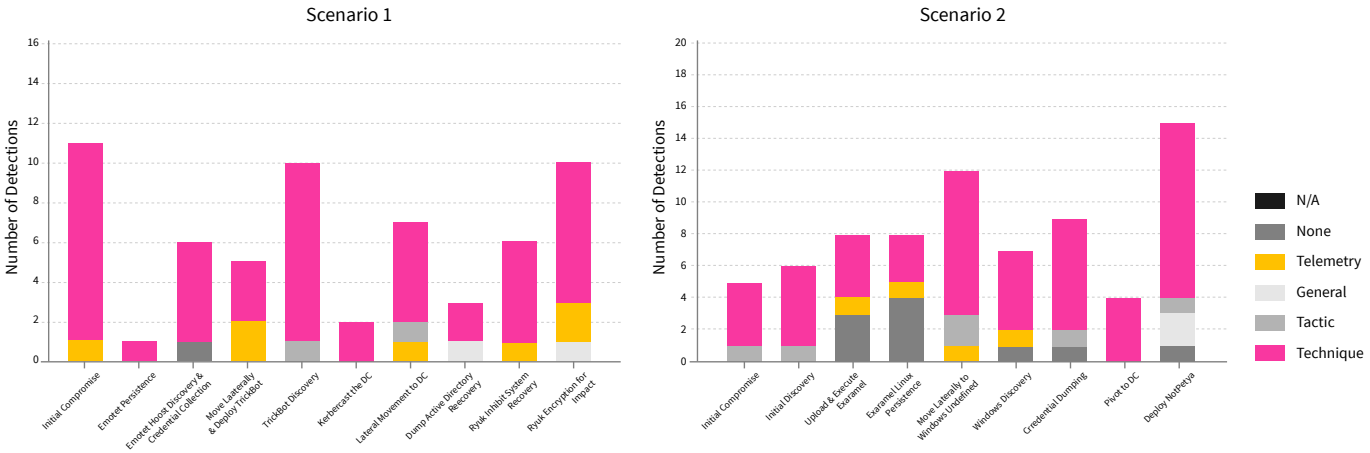
MITRE ATT&CK unique techniques tested in Wizard Spider and Sandworm evaluation

While we don't recommend using the pure "detection count," which could indicate a "noisy" solution that will quickly lead to alert fatigue, several other measures of detection are beneficial. First, did the solution detect steps associated with each MITRE ATT&CK technique? Again, given that most dangerous attacks involve multiple steps over an extended period of time, the solution should detect some activity in each step to accurately alert the client of a threat.

As shown below, **Cynet** was able to **detect 100%** of the 19 MITRE ATT&CK steps evaluated (10 on each day of testing). That means Cynet detected the APT in the environment at every stage of the attack.

100%
of the 19 MITRE ATT&CK steps evaluated
(10 on each day of testing)

Detection Type Distribution by Step

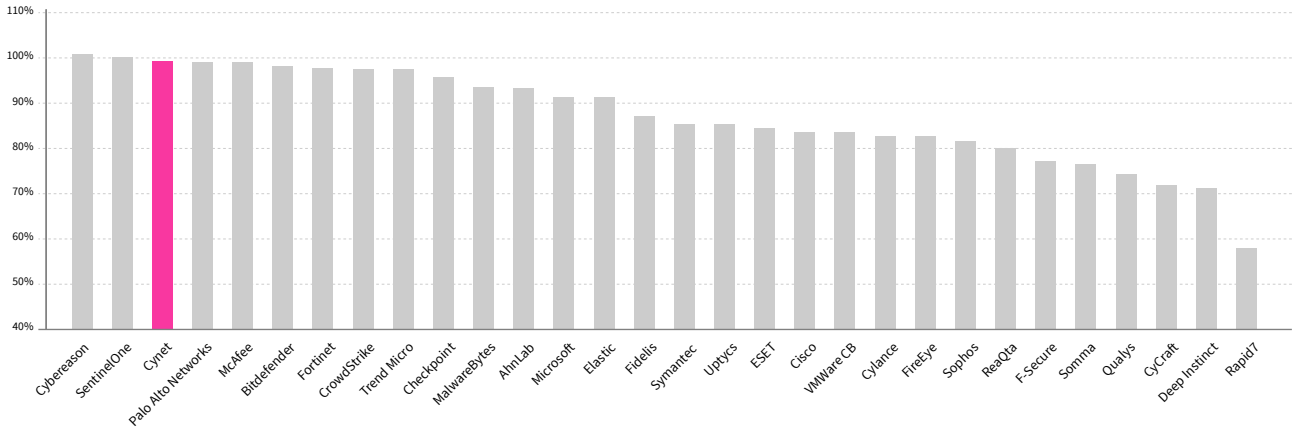


Moreover, Cynet detected 98.5% of the techniques presented across all 109 substeps of the MITRE ATT&CK evaluation.

While no solution is expected to detect 100% of all threat components all the time, the high technique detection rate shows that enough alarms are raised to detect advanced persistent threats across multiple steps of the attack lifecycle.

98.5%
of the techniques presented
across all 109 substeps of the MITRE ATT&CK evaluation

MYTRE 2022 Results: Overall Detection



THE EFFECT OF HUMAN-ASSISTED DETECTION

As mentioned above, this year's evaluation did not include the managed security service provider (MSSP) detection category where "data is presented from a managed security service provider (MSSP) or monitoring service based on human analysis and indication of an incident occurring."

Some argued that including the MSSP detection category is more of an evaluation of the vendor's security analyst team as opposed to the vendor's cybersecurity technology solution. And, to receive the benefits of MSSP detection, clients are forced to spend near double the amount for many of the technology platforms alone. Others argue that it reflects the value of the data being provided by the technology platform to a capable security analyst.

In reality, the data generated by each vendor's technology is typically leveraged by security analysts, whether internal or external, skilled or unskilled, to oversee and enhance protection capabilities. The MSSP detection category may have muddied the water a bit, as every vendor that used MSSP detections demonstrated markedly improved results. This improvement reflects the combination of service on top of the endpoint detection technology — which is more in line with real-world usage.

Cynet recognizes the proven value of human oversight and uniquely provides a full, proactive 24/7 managed detection and response (MDR) service to all clients — at no additional cost. This means that all Cynet clients automatically receive the added benefit of highly skilled cybersecurity experts for help with threat intelligence, threat detection, and threat response. Layering this proactive, advanced threat detection and response oversight atop the technology platform is the most effective defense against today's increasingly sophisticated attacks. The faster the time to resolution, the less potential business impact to your organization.

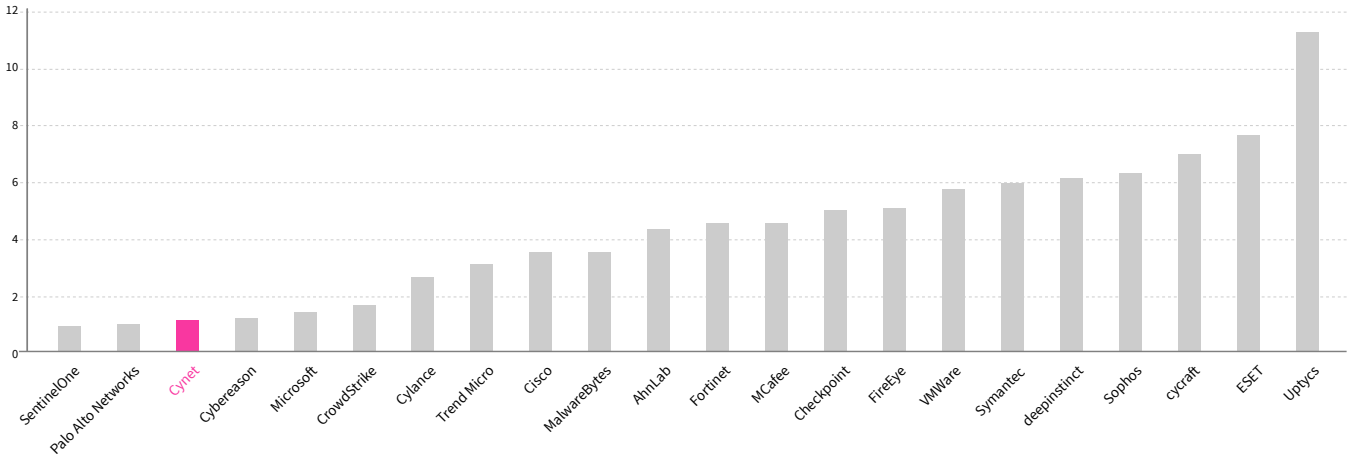
ATTACK PROTECTION

MITRE offered vendors the opportunity to participate in 9 protection scenarios representing a subset of the attack sequences used during the detection assessment. Detection is, of course, important. You can't eliminate what you can't see. As a corollary, preventing detected threats as early as possible in the attack lifecycle is critical to denying the adversary a foothold into your environment. As mentioned above, only 17 of the 29 vendors chose to participate in the protection evaluation.

One important measure of protection is speed. How many substeps are allowed to execute before the threat is detected and eliminated?

Cynet performed in the top quartile of all participating vendors in this measurement. Cynet AutoXDR Breach Protection focuses on protecting against attacks as quickly as possible along the kill chain, with high accuracy and minimal false positive alerts.

MYTRE 2022 Results: Speed of Protection



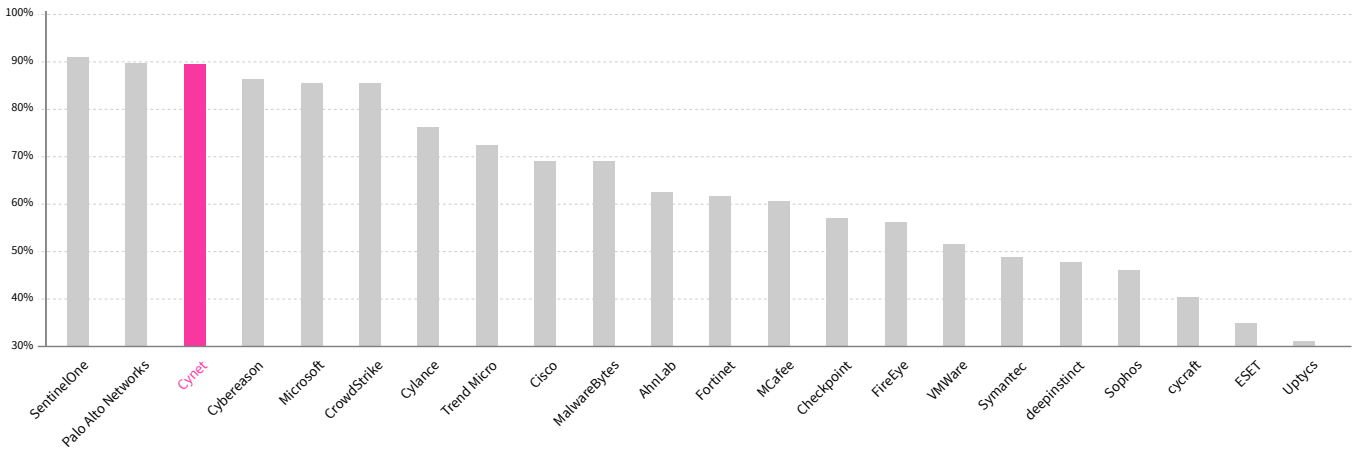
Average number of substeps that execute before a threat is detected and eliminated

Overall Prevention measures how early in the attack sequence the threat was detected so that subsequent steps could not execute. When looking at the number of substeps that did not take place due to preventing earlier stages of the attack, Cynet protection placed in the top three.

TOP 3
Cynet protection

MYTRE 2022 Results: Overall Prevention

Percent of attack substeps prevented from executing due to early blocking of attack sequence



COMBINING DETECTION AND PROTECTION

Another interesting perspective is comparing Overall Detection with Overall Prevention. Both capabilities are important for protecting against cyberattacks and are therefore indicative of a strong endpoint detection solution.

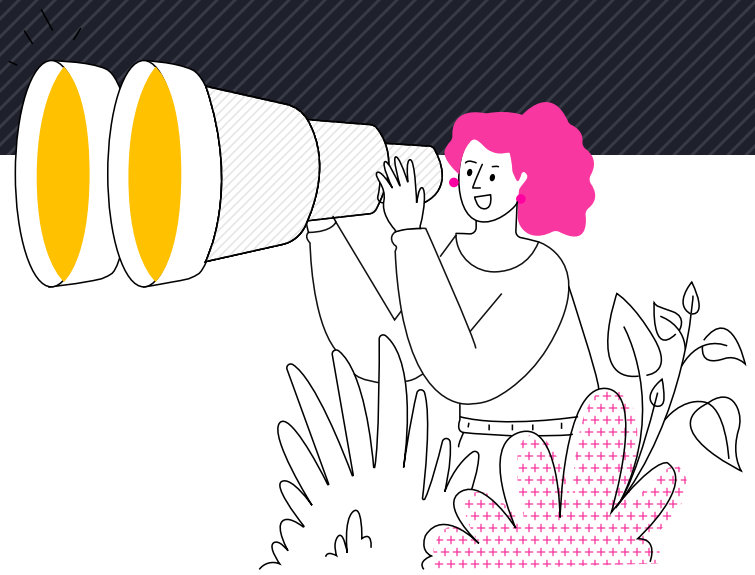
Cynet was among the top 4 performers of all participating solution providers in this year's test.

TOP 4
Performers of all participating solution providers in this year's test

MYTRE 2022 Results: Overall Detection & Protection

BEYOND MITRE WITH CYNET

As important as MITRE testing is to evaluate threat protection solutions, many other factors are equally or more important to the solution selection process. Although Cynet clearly demonstrated industry-leading detection and protection capabilities in the MITRE ATT&CK evaluation, several highly differentiating factors are critical to consider.



END-TO-END, HIGHLY ACCURATE THREAT VISIBILITY

The MITRE ATT&CK evaluation is primarily used to test the capabilities of endpoint detection and response (EDR) platforms.

The rise of extended detection and response (XDR) capabilities expands telemetry beyond the endpoint, to additional critical elements of the environment. For example, some XDR solutions included user-based telemetry to detect behavioral anomalies that are indicative of cyber attacks.

Combining additional telemetry signals with endpoint telemetry signals adds context for more accurate results. When combined with telemetry, seemingly benign signals can signal dangerous attacks.

Conversely, seemingly high-risk signals may be legitimate operations when viewed in full context. Adding telemetry, when done right, provides the rich information necessary to detect threats far more accurately than when analyzed alone or separately.

A tool that fires off alerts with too little or too much data isn't very helpful, even if it detects something that should be investigated. Cynet leverages telemetry from endpoint, network, user, and deception technology to ensure highly accurate alerts while minimizing false positives.

EASE OF USE

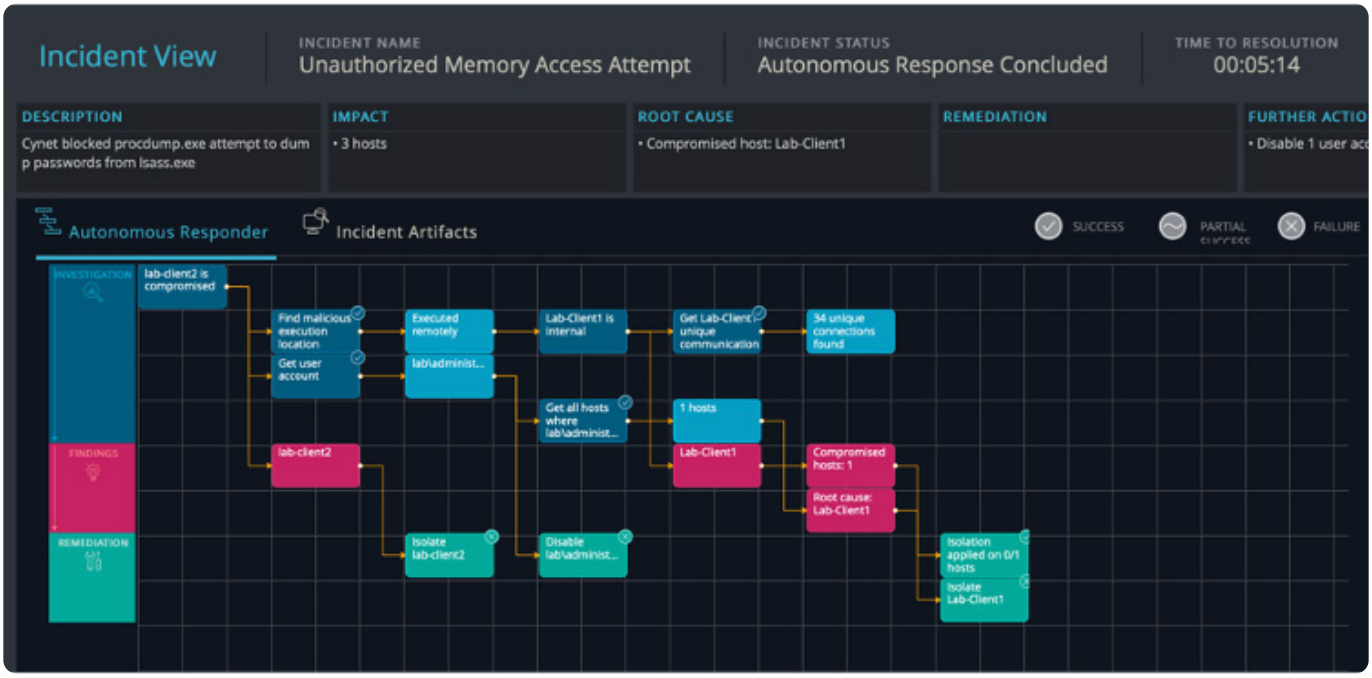
While the tested vendors supply detection screenshots that can be viewed on the MITRE ATT&CK evaluation site, the solution's efficacy and ease of use was not evaluated. While it's important to select a provider that scored among the top of the MITRE evaluation measures, it's also important to select a user-friendly, intuitive product. Security analysts spend significant time interacting with vendor technology, so ensuring the platform is intuitive and easy to use should be an important component of your evaluation criteria.

This advice holds especially true for smaller security teams with limited budgets and skills. A tool that typically requires a small army of cybersecurity experts may work for a large, well funded security team, but will end up being mostly ignored without the necessary internal support resources. Cynet is purpose-built for lean security teams that don't have the bandwidth to work through overly complex interfaces designed for large security teams at large organizations.

Cynet is purpose-built for lean security teams

AUTOMATED INCIDENT INVESTIGATION AND RESPONSE

Cynet goes beyond traditional alerts, to generate a comprehensive incident view. Cynet's Incident Engine uses data to automate threat investigation, moving beyond responding to the single threat at hand to helping determine if the detected threat is only one part of a larger attack, and if so, uncovering related attack components.



When a threat is detected, Cynet's Incident Engine first launches an automated investigation to uncover the root cause of the threat. Was it downloaded from a specific site, embedded in a document, or attached to an email? Was it spawned by a yet undetected malicious process or planted from an RDP connection? Automated root cause analysis peels back these layers to ensure all elements of the attack are exposed, and ultimately uncovering the so-called "patient 0" — the origin of the attack.

Once additional components of a threat are uncovered, the entire environment is searched to expose the full scope of the attack. This includes taking appropriate remediation actions across the environment to eradicate all attack components automatically or manually, depending on your preference. You cannot be assured of safety until the attack is fully rooted out.

Manually performing these investigation steps takes time and skills and effort. Every alert becomes a lot of work. Unfortunately, many security teams do not have the bandwidth, and many smaller security teams lack the skills, to perform the necessary investigative steps. Automating this workflow, at a minimum, provides security teams with a considerable head start on incident response. And, in many cases, it eliminates the need for manual intervention.

EXTENDED PLATFORM CAPABILITIES

Many large enterprises operate an extensive array of highly specialized IT security technologies that are integrated into a comprehensive security stack. Significant expertise and resources are required to design, build, integrate, operate, and maintain such a stack. Most companies, however, do not have the budget or bandwidth to take this approach.

It behooves resource-constrained companies to adopt security solutions that provide multiple capabilities. This way, organizations can obtain protections that might otherwise be unobtainable due to budget and/or resource constraints. Modern XDR tools that include multiple sources of telemetry, for example, help companies avoid the expense and burden of acquiring and integrating multiple third-party technologies to expand threat visibility across their environments. So-called "open XDR" solutions, conversely, still require companies to purchase multiple detection technologies that are integrated into the open XDR solution.

The Cynet 360 AutoXDR platform includes telemetry from endpoint, network, users and deception technologies. The solution is fully integrated out of the box, making it highly effective yet highly affordable.

Moreover, the Cynet platform offers additional security technologies, including SaaS Security Posture Management (SSPM), Cloud Security Posture Management (CSPM) for Azure, and Centralized Log Management (CLM). These options allow clients to easily obtain such important capabilities with the flip of a switch, fully integrated into the Cynet platform.

The solution is highly effective yet highly affordable

MDR SERVICES

Some vendors offer in-house MDR services for an optional fee, others outsource to a third party, and some offer neither of these options.

Because many organizations rely on MDR services, ensure the vendor's offering and price point are in line with your budget and expectations. Using the platform providers in-house or outsourced MDR team ensures familiarity with the platform, maximizing effectiveness and efficiency. It's also a boon to resource-constrained teams that rely on outside help to protect their organization.

Cynet includes MDR services at no additional cost to all clients. This includes 24x7 monitoring to ensure that no dangerous threats are missed and 24x7 on-demand expert advice and guidance.

Cynet includes MDR services at no additional cost to all clients

FINAL THOUGHTS

The MITRE ATT&CK evaluation is a valuable resource that can be used to inform your decision when selecting a security vendor. A top-performing MITRE ATT&CK evaluation indicates a vendor whose solution will perform well in detecting real world threats.

The Cynet 360 AutoXDR platform was a top performer in the 2022 MITRE ATT&CK evaluation. The key is knowing how to get the most out of these resources. We hope you found this guide helpful. If you have any questions or want to learn more about Cynet, let us know. We'd love to chat.

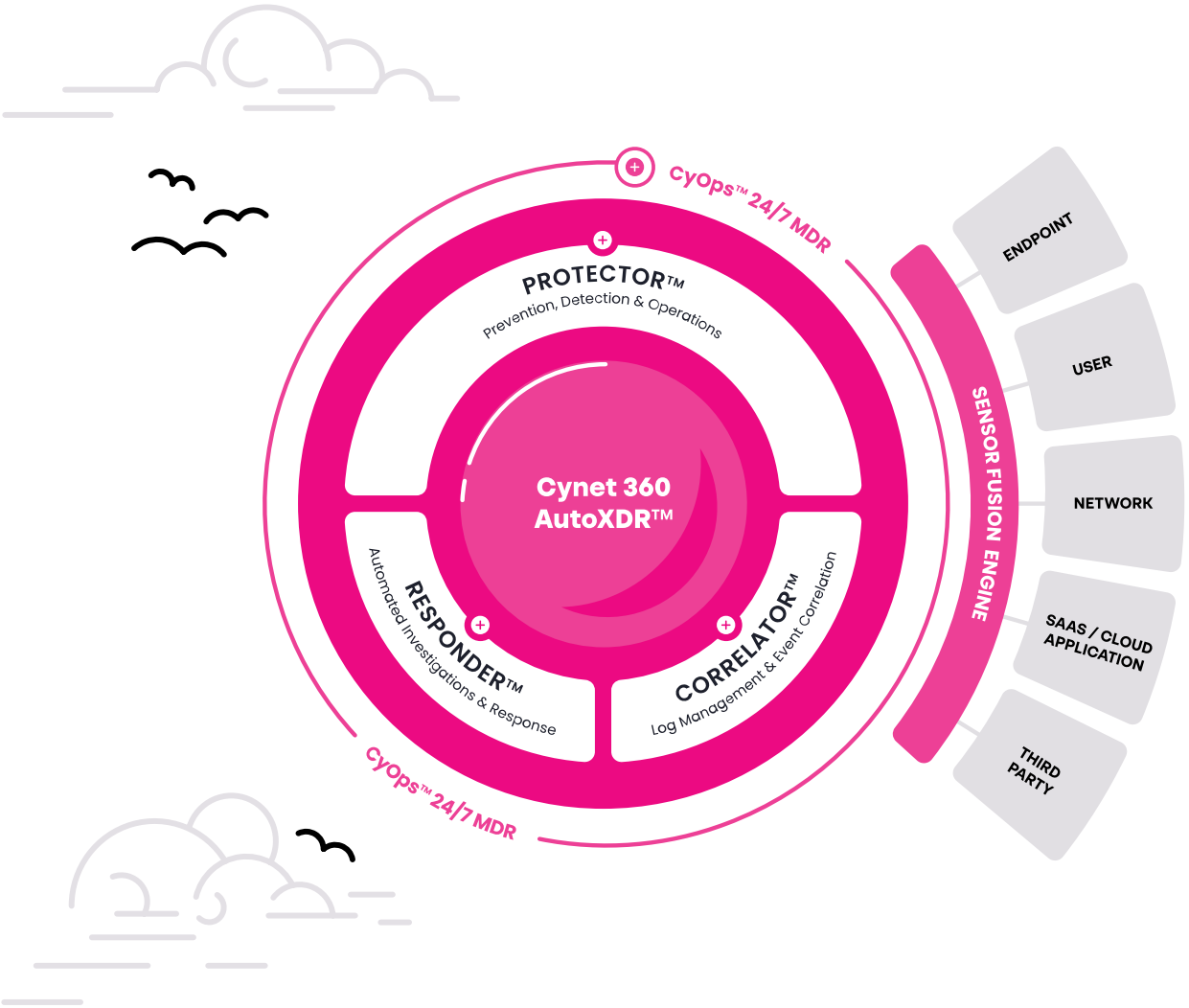
ABOUT CYNET

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

Cynet delivers the prevention and detection capabilities of EPP, EDR, NDR, Deception, UBA rules and CSPM, together with alert and activity correlation and extensive response automation capabilities.

Our vision is to enable security teams to put their cybersecurity on autopilot and focus their limited resources on managing security rather than operating it.

Bring sanity back to cybersecurity with a fresh approach that makes protecting your organization easy and stress-less.



cynet

www.cynet.com