cybereason© | MITRE | ATT&CK®

ENTERPRISE EVALUATION 2022 RESULTS

Outclass a sophisticated adversary

Sophisticated threat actors are generally effective attacking underprepared environments. This makes it essential to invest in highly-effective security solutions.

The MITRE ATT&CK evaluations measure that effectiveness. In the 2022 evaluation that features 30 vendors, it's challenging to sift through the noise. As you review the results, here are five high-impact metrics to consider: Protection, Detection Coverage, Real-Time Detections, Visibility, and Analytic Coverage.

100% PROTECTION COVERAGE

Comprehensive prevention coverage across every Windows and Linux based threat.

100% DETECTION COVERAGE

Cybereason achieved 100% threat detection across all 19 attack steps exhibited by Wizard Spider & Sandworm.

100% REAL-TIME DETECTION

Every Cybereason detection occurred in real-time, giving your team the fastest possible response.

100% VISIBILTY

Complete visibility, with **ZERO missed detections** across all operating systems for both Windows and Linux systems.

99% ANALYTIC COVERAGE

Analytic detections are the deepest possible and leverage more subtle telemetry. Cybereason had **100% Linux Analytic coverage and 99% Windows Analytic coverage.**

Best of all, effective out-of-the-box: 97% of our MalOp detections required no special configuration.

Why Does MITRE ATT&CK Matter?

The **MITRE ATT&CK** evaluations are a Meritocracy. It's an equal playing field where every vendor submits their best endpoint security solution and all go through the same evaluation process. Today, these yearly rounds are the gold standard in technical testing across attack prevention and detection.

ATT&CK is a standardized framework that maps adversarial tools, tactics and procedures (TTP's) and is the gold standard for both Endpoint Security vendors and security practitioners. This catalog of TTP's creates structure and organization for detection and response where it previously did not exist through a digestible framework. ATT&CK is always expanding to incorporate new threats.

ATT&CK emulations test detection and response efficacy on a yearly basis. MITRE is extremely reputable and is the most qualified organization to conduct these attack emulations. Their mission is to help global users better understand adversary behaviors. Most importantly, vendors can't pay more for better results. MITRE evaluations of Endpoint Security solutions are unbiased and transparent.

The Enterprise Evaluation 2022 was based on sophisticated threat groups (Wizard Spider & Sandworm) who use Ryuk and other forms of advanced ransomware. The primary intention of this round of evaluations was to test a vendor's ability to detect data destruction, data encryption, and other ransomware-centric cyber activities.

EVALUATION RESULTS

Wizard Spider and Sandworm

100% PROTECTION

The more threats that are prevented at the onset means that there are fewer threats that require investigation and response. Cybereason boasts a perfect prevention score in the Enterprise Evaluation 2022.

100% DETECTION

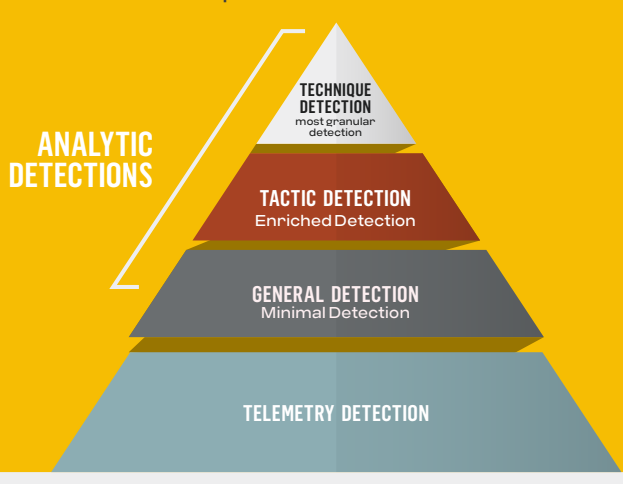
Cybereason achieved 100% threat detection across all 19 attack steps exhibited by Wizard Spider. Every Cybereason detection occurred in real-time, giving your team the fastest possible response.

100% VISIBILITY

Cybereason is mapped tightly to the overall ATT&CK framework, with 100% visibility into ATT&CK TTP's included in the Enterprise Evaluation 2022. The MalOp Detection Engine is the core of how Cybereason provides this level of visibility to our customers, and in this round we demonstrate the complete picture of the threat.

99% ANALYTIC COVERAGE

Analytic detections are deeper detections that are constructed from subtle signals and indicators. Analytic detections are built from a broader data set and are a combination of technique + tactic detections. This produces a nuanced view of what took place for enriched detections.

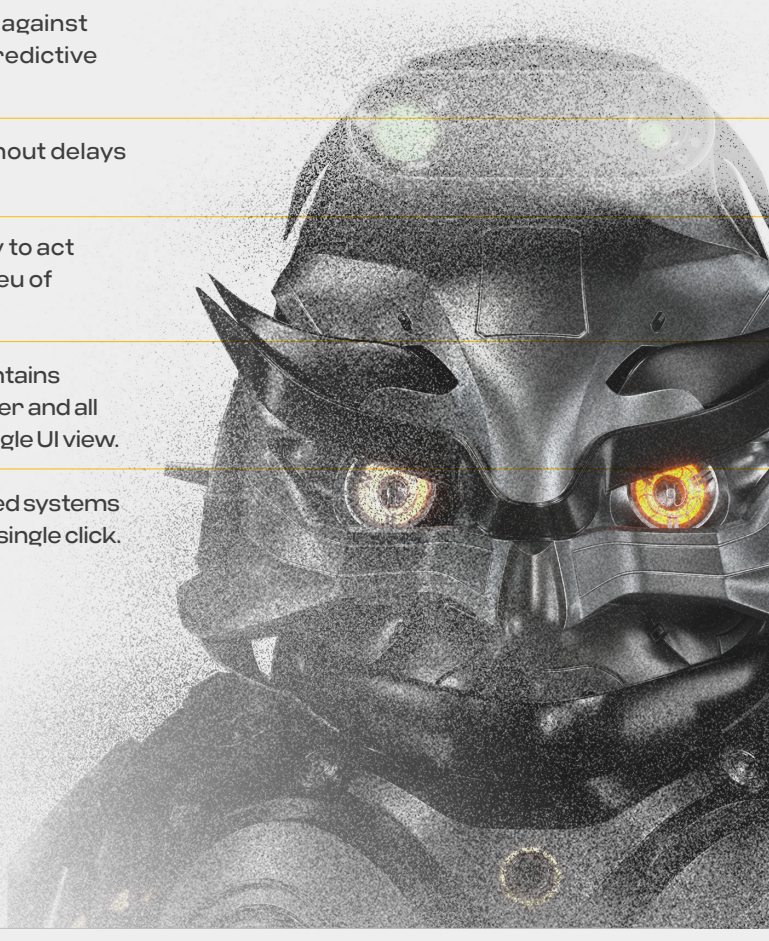


100% REAL-TIME

Delayed visibility leads to more entrenched adversaries and harder-to-remediate threats. Cybereason uses machine learning to analyze more than 30 telemetry sources in real-time to produce zero delays in detection during the 2022 Enterprise Evaluations, providing immediate visibility into the malicious operation. Ransomware is a race against time, and real-time detection of ransomware indicators is a massive boost to infosec teams.

Why Cybereason

Results When It Matters	Cybereason security solutions are reliable and perform in the field against the most sophisticated adversaries.
Ransomware Ready	Cybereason is undefeated in the fight against ransomware and our defenses are predictive and multi-layered.
Immediate visibility	See threats in real time and react without delays to minimize impact and reduce risk.
Bulletproof Prevention	Defenders can rely on our technology to act competently to block and prevent in lieu of manual investigation and response.
Actionable Detections	The MalOp™ is highly actionable and contains scope, timeline, tools used by the attacker and all telemetry that led to a conviction in a single UI view.
One Click Response	Immediately restore trust to all impacted systems and users across the enterprise with a single click.



Cybereason is tightly aligned with the ATT&CK framework and includes MITRE tagging on every ATT&CK-related detection for added context and to streamline response. We have consistently performed as a front-of-the-pack participant in every ATT&CK evaluation to date.

Learn more about our MITRE ATT&CK R4 evaluation HERE or request a DEMO today.

LEARN MORE AT CYBEREASON.COM