MITRE Engenuity ATT&CK Evaluations : Quick Guide

Carbanak+FIN7 Evaluation Results

Date: Evaluation results published April 20, 2021

ABOUT MITRE ATT&CK

MITRE ATT&CK is a public knowledgebase of adversarial tactics and techniques, which can be used as a foundation for the development of specific cyber threat models and methodologies.

In short, it helps the industry define and standardize how to describe an attacker's approach. MITRE ATT&CK collects and categorizes common attack tactics, techniques, and procedures (TTPs), then organizes this information into a framework. This framework can be used to help explain how adversaries behave, what they are trying to do, and how they are trying to do it.

Having a common language and framework is important in the ability to communicate, understand, and respond to threats as efficiently and effectively as possible.

It also helps SOC/IR teams understand what coverage they have against various attack techniques. The framework is updated regularly with new techniques contributed by those in the cybersecurity industry, including Trend Micro.

The MITRE ATT&CK evaluations have focused on the Enterprise Matrix for Windows systems but for this year included Linux as it is increasingly used in many types of attacks.

There are multiple framework matrices:

- **Enterprise** (Microsoft® Windows®, macOS®, Linux®),
- **Cloud** (AWS, Microsoft® Azure™, Google Cloud Platform™, Office 365®, Azure AD, Software as a Service (SaaS))
- **Mobile** (Android™, iOS)
- **Industrial control systems** (ICS)

How the evaluation works:

The MITRE Engenuity ATT&CK Evaluation offers transparency to customers and real-world attack scenarios. This ensures that customers can actively evaluate security products to protect themselves from the latest advances from attackers based on their areas of greatest need.

The evaluation uses adversary emulation to ensure customers can address today's threats. Using techniques, tools, methods and goals inspired by that of an attacker.

The simulations are executed in a controlled lab environment to ensure fair and accurate testing. Attacker techniques are then used in logical step-by-step in order to explore the breadth of ATT&CK coverage. Over the two scenarios 174 attacker steps were executed.

The evaluation this year emulated Carbanak and FIN7 tradecraft and operational flows to simulate attacks similar to the behavior used in the wild by these groups.

After the simulation has been run, results are processed and publicly released, including the methodology.

This year also marks the first time an optional protection scenario was made available with **17 of the 29** vendors choosing to participate, including Trend Micro.

For the Carbanak and FIN7 evaluation, 65 ATT&CK techniques across 11 ATT&CK tactics were in scope for this evaluation. This included 12 ATT&CK techniques across 7 ATT&CK tactics for the Linux portion of the Carbanak evaluation.

Executive Summary - Highlights of Trend Micro's results from the MITRE Engenuity ATT&CK Evaluation

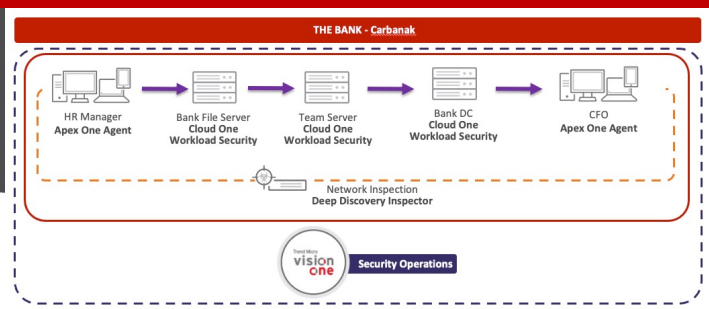
This year's strong performance in MITRE Engenuity's ATT&CK Evaluation is the second in a row for Trend Micro, whose capabilities also impressed in the 2020 tests.

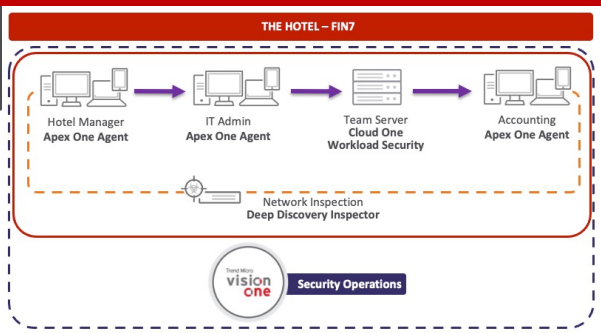
Trend Micro Vision One recorded the following impressive results:

- **Top three performer in visibility with 96% attack coverage to provide visibility of 167 of 174** simulated steps across the evaluations. This broad visibility allows customers to have a clear picture of the attack and respond faster.
- **#1 performer in Linux, with 100% of attacks against the Linux host detected and prevented,** capturing attacker steps and preventing a simulated attack, which is especially important considering Linux is the most used OS in cloud-native applications .
- **A top performer in detection enrichment, with Trend Micro Vision One enriching 139 pieces of telemetry** to provide extremely effective threat visibility that helps SOC analysts to better understand and investigate attacks.

MITRE Engenuity ATT&CK Evaluations : Quick Guide

Trend Micro Solutions included in the evaluation





Day 1 Scenario (Linux included)
Emulated Group: Carbanak Group / Anunak / Carbon Spider
Victim: Bank / financial institution
Scenario: Breach HR Manager, access target, elevate privileges, and obtain credentials, move laterally and locate CFO's system from which they can collect sensitive data and spoof money transfers

Additional Resources:
Link to configuration and setup
Operational Flow (Carbanak)

Day 2 Scenario
Emulated Group: FIN7
Victim: Hotel
Scenario: Breach Hotel Manager, maintain access until credentials are collected and new victim systems are discovered, move laterally to IT admin system, observe then replicate connection to accounting system, set up persistence and skim customer payment data

Additional Resources:
Operational Flow (FIN7)

Trend Micro Results

How is the Evaluation scored?
MITRE ATT&CK does not score or rank the evaluation against other vendors. However new with this evaluation is the "Evaluation Summary" which can be used to explore a variety of metrics on the underlying data from each participant.

This is something we have aligned to in this report and compared these to other vendors. The results are available directly from the website in full transparency for customers to also do self analysis in evaluating how to best protect themselves.

Additional Resources :
ATT&CK Evaluations Carbanak and FIN7: How to Get Started with the Results and Navigate the New Content and Trend Micro Public Results

Evaluation summary high level results for Trend Micro

What are substeps? *These are the individual attacker tests carried out as part of the emulation – in total there were 174 across both simulations*

Detection Count	Analytic Coverage	Telemetry Coverage	Visibility
338 across 174 substeps	**139 of 174** substeps	**162 of 174** substeps	**167 of 174** substeps
3rd of 29 vendors	**6th of 29 vendors**	**2nd of 29 vendors**	**3rd of 29 vendors**
This is a positive metric to **identify adversary behavior** across the evaluated attacker steps.	These are **enriched detections** that add context by adding ATT&CK technique mappings or alert descriptions.	This is a key metric to understand the activity of the attacker in detail on each attacker step evaluated (e.g., process start, file create)	Attacker visibility allows customers to **build a clear picture of the attack** and respond faster. This shows where analytic or telemetry information was available.

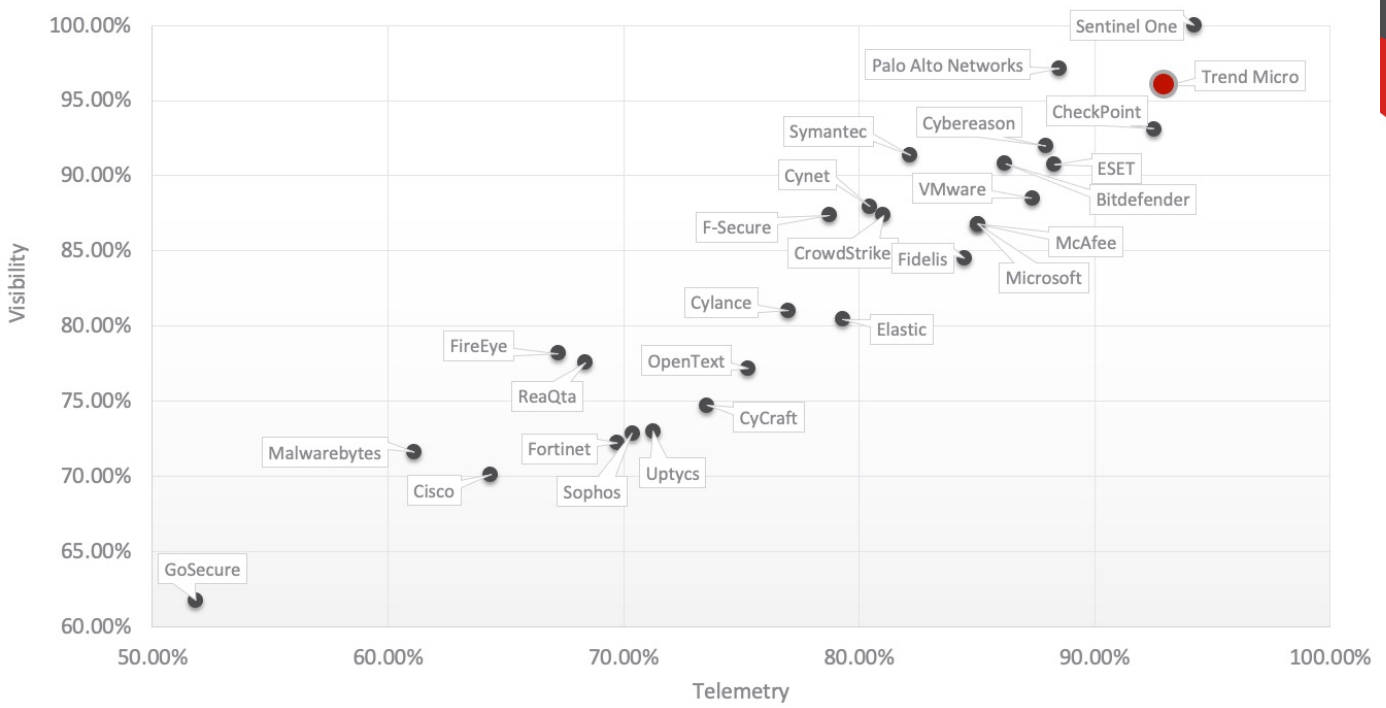
USEFUL DATA FOR
SOC Level 1 Analyst - Triage

USEFUL DATA FOR
SOC Level 2 / 3 Analyst - Hunters / Incident responder

MITRE Engenuity ATT&CK Evaluations : Quick Guide

Trend Micro Results:

A complete attack story with visibility and telemetry



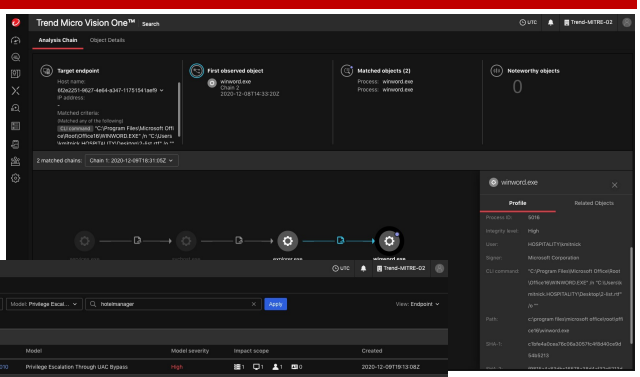
Trend Micro is Top 3 - for visibility and telemetry across 29 vendors

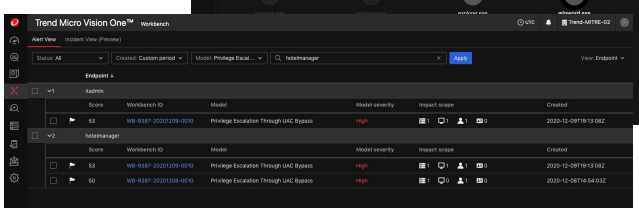
Creating a story of an attack with Trend Micro Vision One

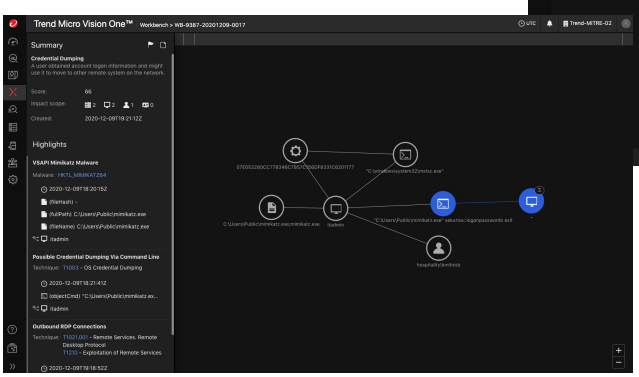
Trend Micro Vision One allows you to provide a complete story of the attack.

Automatically correlating threat data from different areas of the endpoint, server and network provides better alerts to security teams.

We don't just tell you these individual events have all occurred – we connect the dots for you, showing that they might be related and have similar indicators of compromise as a certain attack group or type.





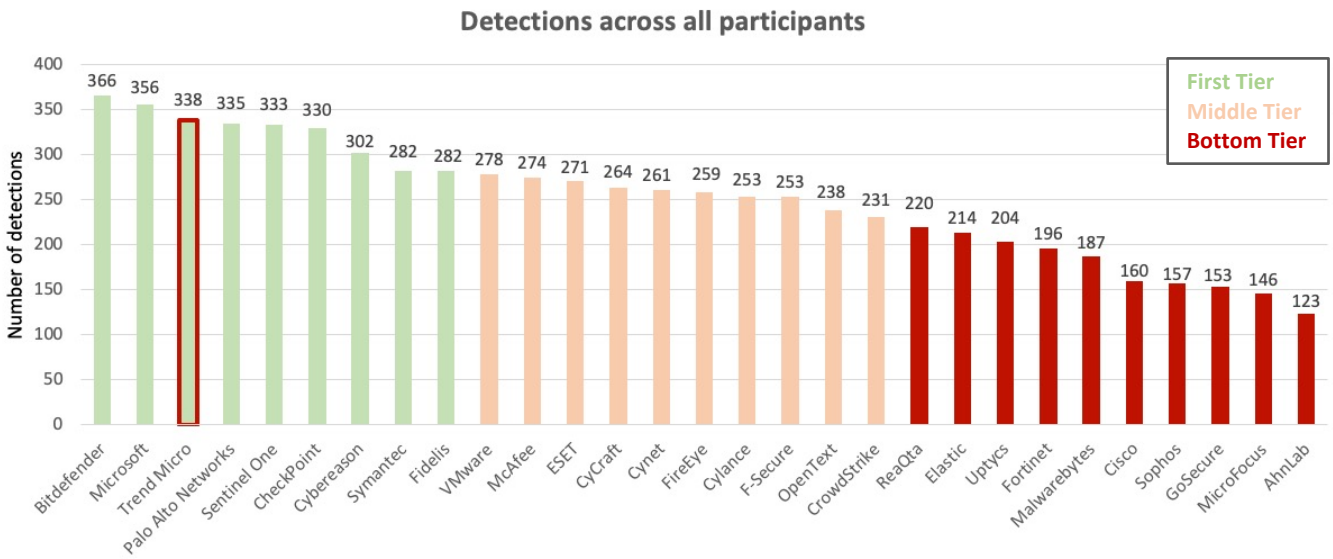


MITRE Engenuity ATT&CK Evaluations : Quick Guide

Trend Micro Results:

Detections

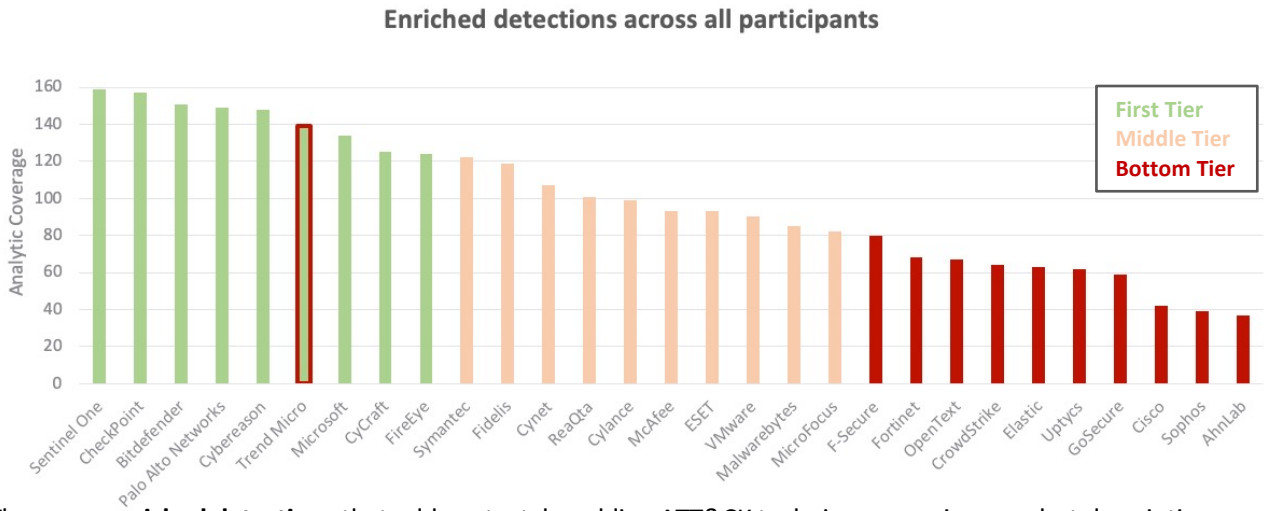
Any information, raw or processed, that can be used to identify adversary behavior.



This is a positive metric to **identify adversary behavior** across the evaluated attacker steps.

Analytic Coverage

Any processed detection, such as a rule or logic applied to telemetry – ATT&CK technique mappings or alert descriptions



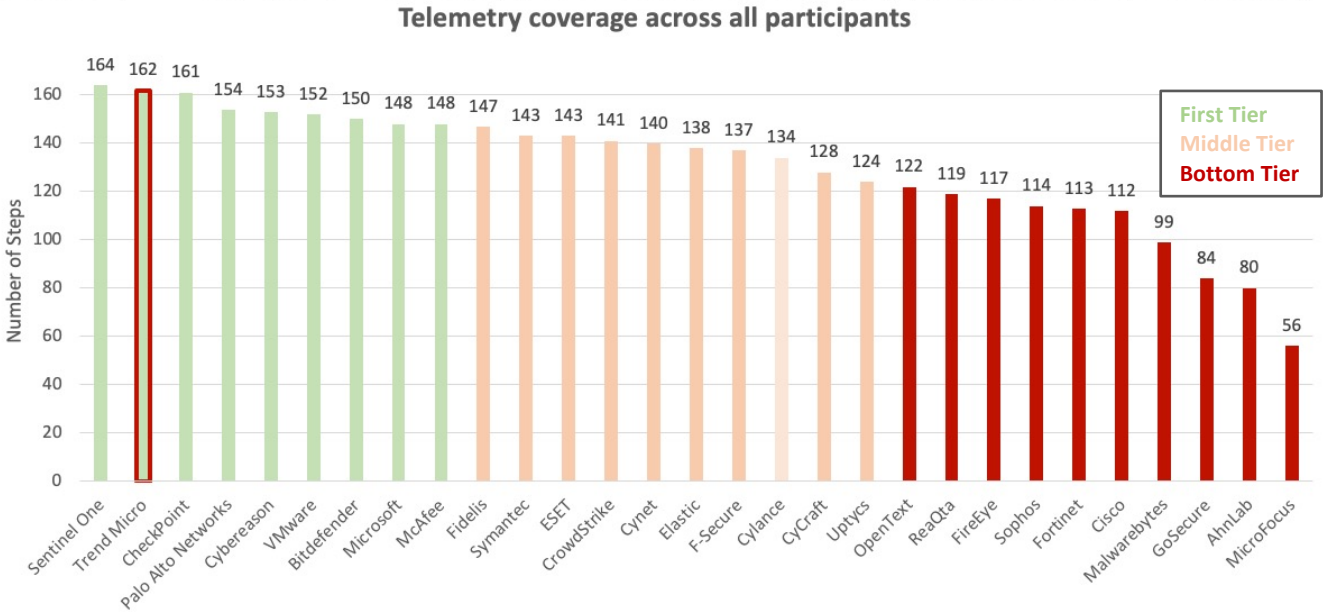
These are **enriched detections** that add context by adding ATT&CK technique mappings or alert descriptions.

MITRE Engenuity ATT&CK Evaluations : Quick Guide

Trend Micro Results:

Telemetry

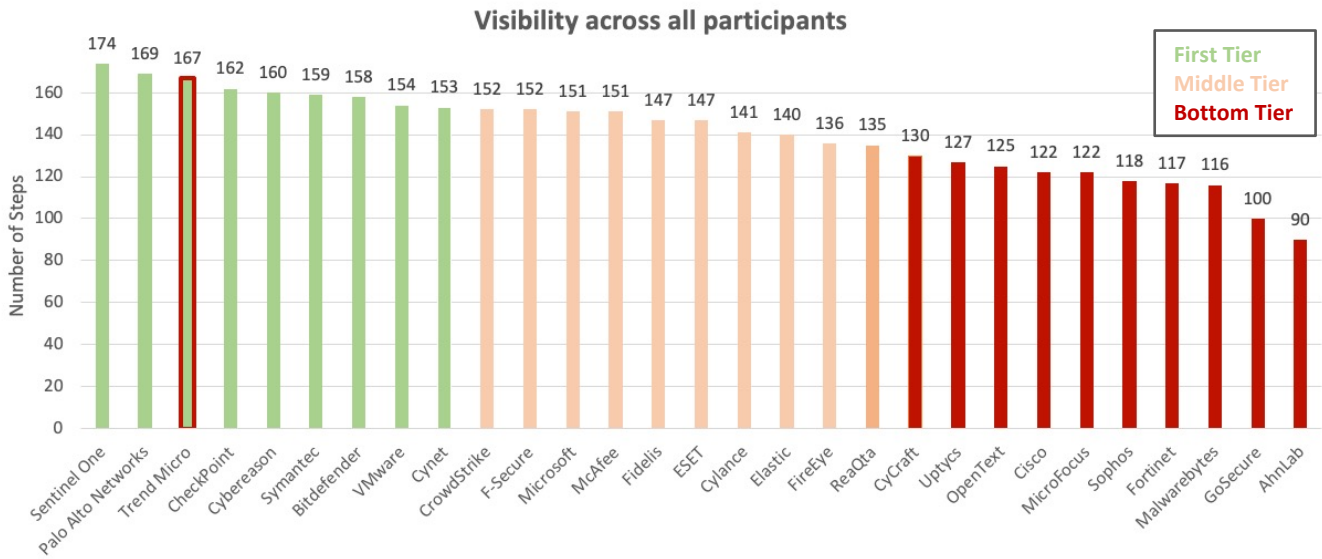
Telemetry — Any raw or minimally processed detection (e.g., process start, file create)



This is a key metric to understand the activity of the attacker in detail on each attacker step evaluated (e.g., process start, file create)

Visibility

Visibility — the number of sub-steps where an analytic or telemetry was available



Attacker visibility allows customers to **build a clear picture of the attack** and respond faster. This shows where analytic or telemetry information was available.

MITRE Engenuity ATT&CK Evaluations : Quick Guide

Trend Micro Results:

Linux detection

#2 — 91.6% — paloalto NETWORKS

#1 — 100% — SentinelOne, TREND MICRO, Microsoft

#3 — 83.3% — Check Point SOFTWARE TECHNOLOGIES LTD

Wait... What about...

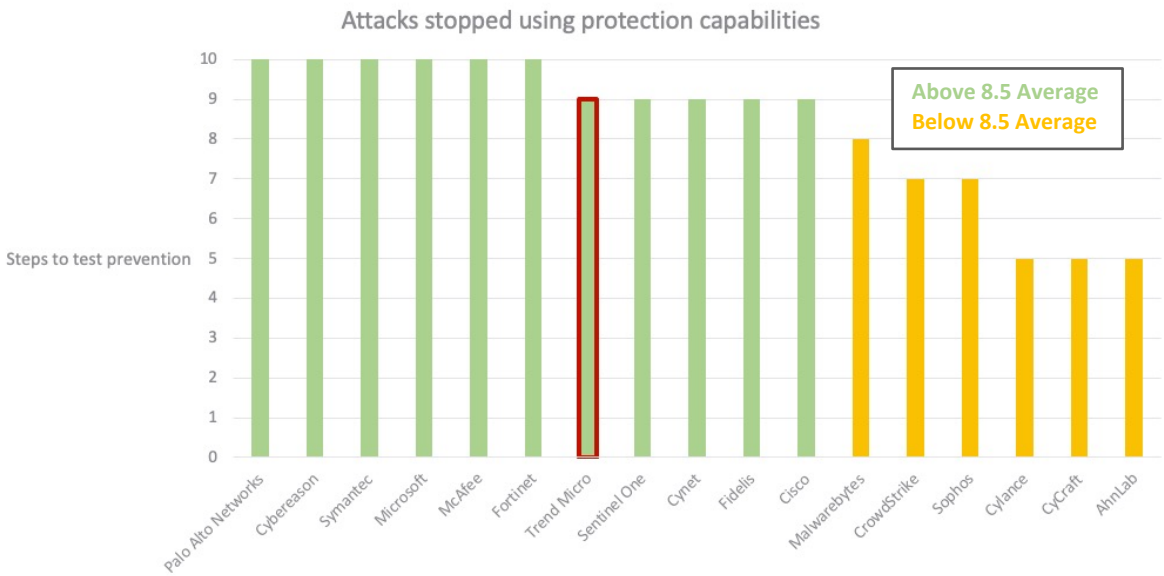
CROWDSTRIKE — #8 — 16.6%

vmware Carbon Black. — #6 — 41.6%

With Linux gaining huge popularity amongst many organizations, especially moving to the cloud, 100% of attacks against the Linux host were detected, capturing 12/12 attacker steps.

Note : Fidelis, OpenText, Cisco, Sophos, Malwarebytes, GoSecure, AhnLab did not participate in the Linux protection test.

Prevention



Prevention is a key addition to the emulated attacks this year. Deflecting risk early on frees up investigation resources, allowing teams to focus on the harder security problems to solve.. Trend Micro demonstrated capabilities through use of automated detection and response to block attacks very early on in each successful test.

Note : CheckPoint, Bitdefender, Vmware, F-Secure, ESET, Elastic, FireEye, ReaQta, Uptycs, OpenText, MicroFocus and GoSecure did not participate in the prevention tests.

MITRE Engenuity ATT&CK Evaluations : Quick Guide

Want to understand more about the ATT&CK Framework?

MITRE ATT&CK Framework	MITRE ATT&CK Evaluation
This type of framework is extremely useful to information security professionals helping to keep them updated on new attack techniques and to prevent attacks from happening in the first place.	The evaluations are not a competitive analysis. There are no scores, rankings, or ratings. Instead, they show how each vendor approaches threat detection in the context of the ATT&CK knowledge base.
Why are Organizations using ATT&CK Framework? Organizations use ATT&CK to standardize community conversations, defense testing, and product/service evaluations.	**Why are Organizations using ATT&CK Evaluations** ATT&CK Evaluations provide vendors with an assessment of their ability to defend against specific adversary tactics and techniques.

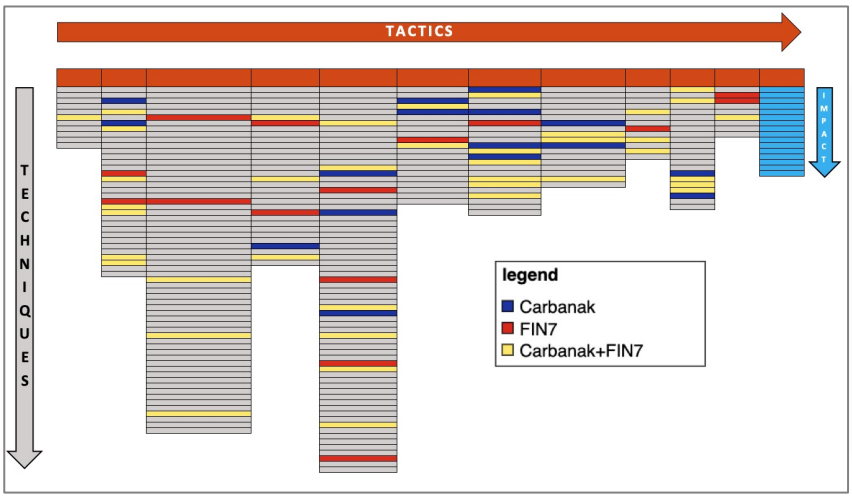
Anatomy of MITRE ATT&CK Framework

TACTICS are the description of what attackers are trying to achieve.

Tactics are similar to a chapter of a book. A CISO can outline a story they want to tell with the high level tactics used in an attack and then refer to the techniques to tell the story of how they accomplished the attack which provides extra detail.

TECHNIQUES

The are are how attackers accomplish those steps or goals.



IMPACT

Used by adversaries to follow through on their end goal or to provide cover.

Playbooks should be in place to defend against these.

Example Story : Building an attack story in a common language

The goal of the attacker was to gain initial access to the network. Using a drive-by compromise with a spear-phishing link and trusted relationship, the attacker gained initial access using this technique. ***Note : The framework lists all the known ways that an attacker can gain initial access.***

How does Trend Micro help?

Trend Micro maps our products to the ATT&CK Framework, showing tactics and technique on detections which demonstrates how we can can help you address the challenges of detecting and responding to threats.

What about prevention?

Preventative controls are an important part of a threat mitigations strategy which add resilience when under attack. Preventative controls were tested in the latest round with the ability to deflect risk early on allowing organizations to spend more time on harder security problems.

Learn More

https://resources.trendmicro.com/MITRE-Attack-Evaluations.html

MITRE ATT&CK vs Cyber Kill Chain

MITRE ATT&CK is designed to provide a deeper level of granularity in describing what can occur during an attack which is step forward from the Cyber Kill Chain.

MITRE ATT&CK	CYBER KILL CHAIN
Initial Access	Reconnaissance
Execution	Intrusion
Persistence	Exploitation
Privilege Escalation	Privilege Execution
Defense Evasion	Lateral Movement
Credential Access	Obfuscations / Anti Forensics
Discovery	Denial of Service
Lateral Movement	Exfiltration
Collection	
Command and Control	
Exfiltration	
Impact	