2021 | CARBANAK/FIN7

MITRE ENGENUITY ATT&CK® EVALUATION

The *2021 Round*

Bitdefender®

WWW.BITDEFENDER.COM

A test unique in the industry

MITRE Engenuity ATT&CK Evaluation

MITRE Engenuity ATT&CK® Evaluation

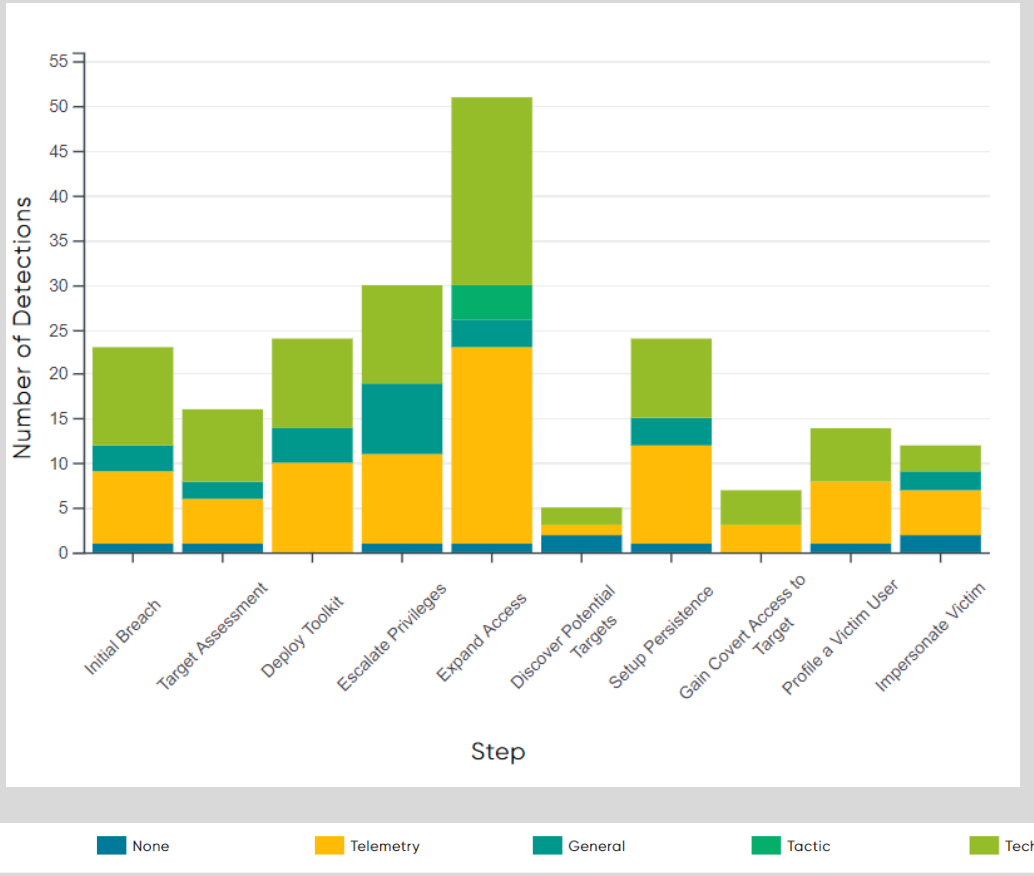
Testing Robustness and Completeness

MITRE meticulously emulates the full behavior of two sophisticated attacks - Carbanak and FIN7 -

to **reveal in detail the capabilities** of the various technology layers embedded in security solutions **to detect, analyze, provide telemetry and visibility** on all phases/sub-phases of the attack kill-chain.

More info on methodology: here.

Full results of the evaluation: here.



Detections for each step of the Carbanak kill-chain (Bitdefender results)

Bitdefender®

MAY 10, 2021

Why Carbanak and FIN7?

Two of the most damaging attacks on the financial sector

Carbanak has generated more than **$300 million in damages** so far, for hundreds of banks while FIN7 has exfiltrated more than **15 million credit card records** worldwide.

Evaluating the security solutions against very sophisticated attack scenarios, like Carbanak and FIN1, provides a realistic view into the capabilities of the tested solutions (including to protect Linux systems).

Security Researchers from Bitdefender Threat Intelligence Lab studied these attacks in the wild and published their findings in a special publication. Check their Blog Post and Paper to learn more.

29 tested solutions

Multiple metrics

No rankings provided

How to *read* the results?

Key Results Metrics

Detections

- any information, raw or processed that can be used to identify adversary behavior (includes raw and analytic detections)

Telemetry & Telemetry Coverage

- any raw or minimally processed detection (e.g., process start, file create)
- the number of sub-steps where telemetry was available.

Analytic & Analytic Coverage

- any processed detection, such as a rule or logic applied to telemetry (e.g., ATT&CK technique mappings or alert descriptions).
- the number of sub-steps where 1 or more analytics were available.

Visibility

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

Which Metrics are relevant for Your Organization?

The **Detections** are relevant for any organization - the more elements of the attack the solution is capable of detecting, the more effective it is.

Telemetry is a valuable metric in the context of an organization that has a security operations center (SOC) where tools, resources, and know-how exists for further analysis of the raw information.

Analytic metric provides context for the detections - actionable analytics help reduce the risk of alert fatigue and the investigation effort required from security analysts.

Visibility is a combination of raw detections (Telemetry Coverage) and contextualized alerts (Analytics Coverage) - the solution's overall ability to provide visibility into the attack elements.

Bitdefender results

2021 MITRE Engenuity ATT&CK Evaluation

Bitdefender

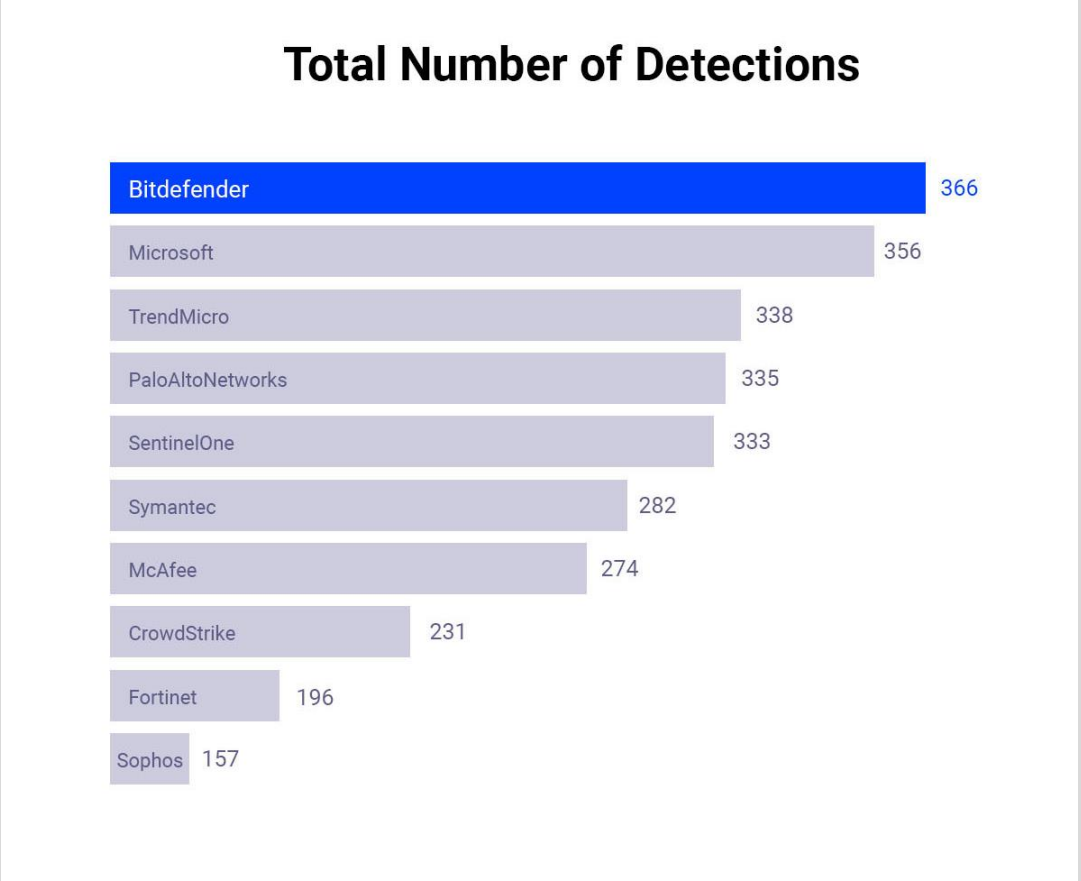
MAY 10, 2021

Highest number of detections

among all 29 solutions evaluated

Bitdefender is the leader in overall detections, with the most detections across all attack steps/sub-steps.

This confirms the results obtained in other industry 3rd party tests and sets apart Bitdefender GravityZone as the best solution in detecting the full range of cyber-threats.



Selected vendors.

Source: https://attackevals.mitre-engenuity.org/enterprise/participants/bitdefender/?adversary=carbanak_fin7

Analytics Insights for all detected sub-steps

Provides rich and actionable security context

100% visibility and context for the major attack steps and a staggering 96% of the total number of detected sub-steps provided with context.

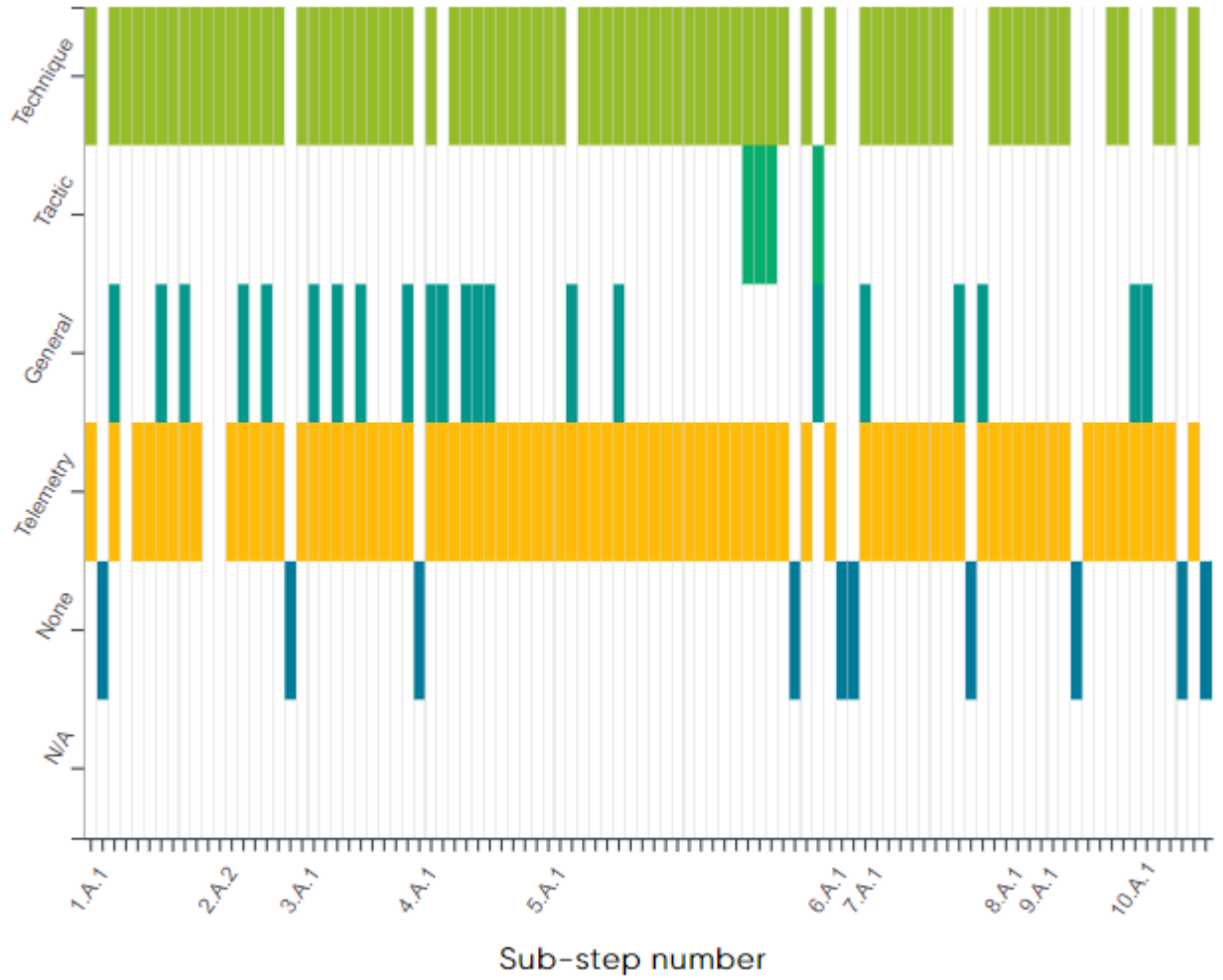
The very low rate of "no-context telemetry" illustrates Bitdefender's commitment to accuracy and security operations effectiveness.

Selected vendors.

Source: https://attackevals.mitre-engenuity.org/enterprise/participants/bitdefender/?adversary=carbanak_fin7

Analytic Detections for each sub-step of the Carbanak attack scenario

The sub-steps detections are complemented with General details and/or insights into the used Tactics or Techniques. The Analytics Insights enable efficient security operations and reduce the risk of alert fatigue.



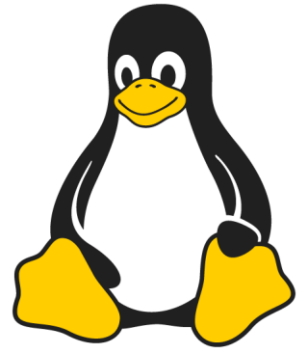
Source: https://attackevals.mitre-engenuity.org/enterprise/participants/bitdefender/?adversary=carbanak_fin7

Complete detection

of attack techniques for Linux systems

Bitdefender GravityZone demonstrated that it is a smart choice for organizations looking to enhance the cyber resilience of their heterogeneous environments with a unified cybersecurity platform.

100% detection



Linux

MITRE Engenuity ATT&CK Evaluation

Complements other industry tests through in-depth understanding of the tested solutions' behavior

AV Test, 4 awards in 2020

Most #1 rankings in from 2018 up to 2021 in AV comparatives tests.

'The Biggest EDR Vendor You Haven't Considered, But Should Have'

Forrester® Wave™:
Enterprise Detection and Response, Q1 2020

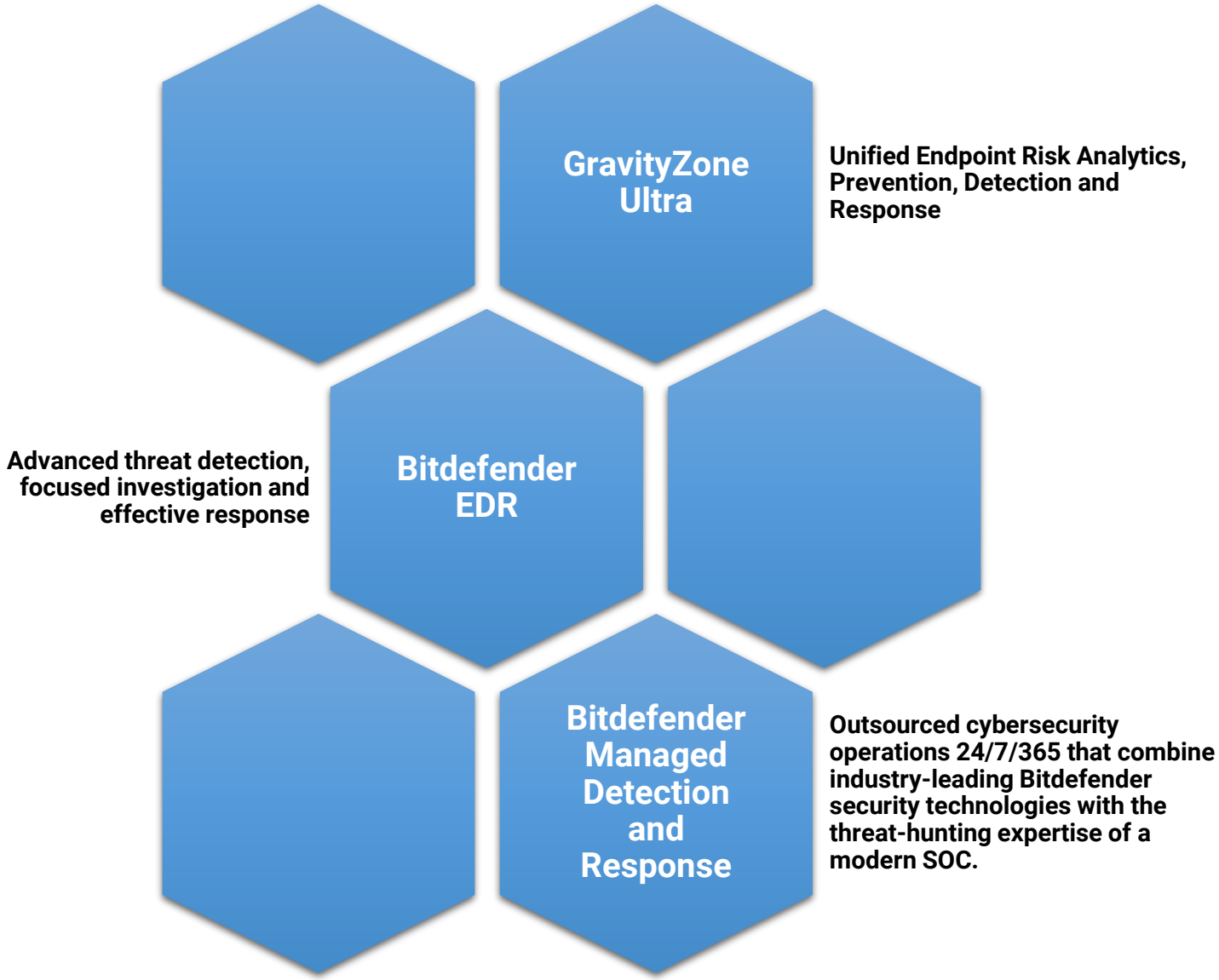
FORRESTER®

Leader in the Cloud Workload Security Forrester Wave

Top Player in the Advanced Persistent Threat (APT) Radicati Market Quadrant analysis

Bitdefender products

featuring the complete set *Detection and Response* capabilities tested during MITRE ATT&CK Evaluation




Bitdefender
WWW.BITDEFENDER.COM