F-SECURE: EXCEEDINGLY GOOD EDR

The MITRE ATT&CK® is a globally-accessible, continually updated knowledge base of known state-sponsored and criminal groups and the tactics, techniques, and procedures that they use. It enables organizations to prioritize detection around the most persistent threats and threat groups.

To help provide organizations with a more detailed analysis of tooling, MITRE evaluates cyber security products (EDR/MDR) using an open methodology based on their ATT&CK® framework to effectively provide a publicly available impartial benchmark.

The MITRE ATT&CK round one evaluation for all the major EDR vendors involved a simulated scenario that pitted F-Secure’s EDR capabilities against an entire intrusion by APT3, a China-based threat group.

- F-Secure scored highest with commonly used simple scoring method (376)
- F-Secure’s telemetry coverage was the broadest with a score of 89%
- F-Secure’s number of real-time alerts was the highest with 56
- F-Secure was one of the best performers in terms of total misses, with 14

INDEPENDENT ANALYSIS OF THE RESULTS

“In an industry desperate for objective efficacy testing, the introduction of the MITRE ATT&CK evaluation of endpoint detection and response (EDR) security products is a much-welcomed event. However, when MITRE published its results, it did so as a scientific data set, leaving security pros to interpret individual vendor performance on their own. This report is Forrester’s guide to understanding the results and our analysis of what each vendor’s results say about its offering. MITRE has now added McAfee and F-Secure to the MITRE ATT&CK evaluation for EDR, and we’ve updated our analysis accordingly.”

The Forrester MITRE ATT&CK Evaluation Guide November 2019
The round 1 evaluation results are based on 20 attack phases broken down into 105 test cases, which then expands to 136 total items for which each EDR vendor can demonstrate advanced attacks detection capabilities.

MITRE focuses on articulating how detections occur, rather than assigning scores to vendor capabilities. However, Forrester has provided publicly available evaluation scripts (attack-eval-scoring at GitHub) to analyze the results (attackevals.mitre.org) and with key metrics to measure how each vendor performed.

As such, we don’t recommend using this evaluation in isolation as a means to assess EDR products since the capabilities of the end user or managed services aren’t measured but have a massive impact on outcomes. Also, the test environment was completely noiseless, no prioritization of techniques included, no workflow/response evaluated, and their scoring criteria was limited. Since MITRE didn’t directly record correlation for detection and investigation, even though it was used, we exclude it from our analysis.

**Metric 1: Simple score** is a way to score each vendor by adding up detections across 56 ATT&CK techniques and 136 procedures. **F-Secure’s simple score** of 376 is the highest.

**Metric 2: Telemetry coverage** measures logging raw data corresponding to the activity performed. **F-Secure’s telemetry coverage** is the highest with 89%.
**Metric 3: Real-time alerts** represent in how many cases the activity performed resulted in immediate alert. F-Secure’s real-time alerts the highest with 56.

![Histogram of real-time alert performance](chart_real-time_alerts.png)

**Metric 4: Total misses** is a reverse measure to detections for how many of the activities performed did not result in either an alert or telemetry. F-Secure only missed 14, one of the smallest totals.

![Histogram of total misses](chart_total_misses.png)

**Metric 5: Kill chain analysis** provides visibility into detection capabilities across 10 different stages of attack measured from initial compromise to execution of persistence across two scenarios. F-Secure only missed one item, making the detection coverage and capability to alert one of the broadest across the kill chain.

<table>
<thead>
<tr>
<th>Cobalt Strike</th>
<th>Initial compromise</th>
<th>Initial discovery</th>
<th>Privilege escalation</th>
<th>Discovery for lateral movement</th>
<th>Credential access</th>
<th>Lateral movement</th>
<th>Persistence</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Execution of presence</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Alert</td>
<td>Alert</td>
<td>Alert</td>
<td>Enrichment</td>
<td>Enrichment</td>
<td>Enrichment</td>
<td>Alert</td>
<td>None</td>
<td>Alert</td>
<td>Alert</td>
</tr>
<tr>
<td>Empire</td>
<td>Alert</td>
<td>Alert</td>
<td>Alert</td>
<td>Enrichment</td>
<td>Alert</td>
<td>Alert</td>
<td>Telemetry</td>
<td>Alert</td>
<td>Alert</td>
<td>Alert</td>
</tr>
</tbody>
</table>
ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We’re closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry’s best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world’s most potent threats.

Together with our network of the top channel partners and over 200 service providers, we’re on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com | twitter.com/fsecure | linkedin.com/f-secure