FortiEDR MITRE ATT&CK Evaluation Fact Sheet

The MITRE Foundation conducts a cyber-defense test of endpoint security products every year called the ATT&CK Enterprise Evaluations. Its transparent evaluation process and publicly available results help organizations identify solutions best suited to address their cybersecurity concerns. While solutions aren't ranked, evaluations focus on the technical ability of a solution to address known adversary behavior. FortiEDR has participated in the MITRE ATT&CK Evaluations for the past two years.

FortiEDR Blocks all Attacks

FortiEDR successfully blocked all attacks in every round of tests it has participated in—validating FortiEDR's commitment to reducing the attack surface and stopping attacks before, during, and after execution.

Signature-Free Protection[1]

FortiEDR didn't just block every attack in each test we participated in (Windows: tests 1-6 & 8-9). They were blocked out-of-the-box, without reliance on the signatures other solutions require. Signature-based security introduces gaps in protection. We recommend that organizations review the screenshots on the protection tests for each vendor under consideration and look for signs of signature-based antivirus (AV) if this is a red flag for your organization.

Detects 97% of Sub-Techniques

Out of the 90 sub-techniques used in the eight Windows tests FortiEDR participated in, it detected 87 of them for a Visibility Rating of 97%. This places FortiEDR in the top five of the thirty vendors evaluated. This level of reliable visibility helps organizations see the full scope of cybercriminal activity.

Accurate Analytic Rate of 94%

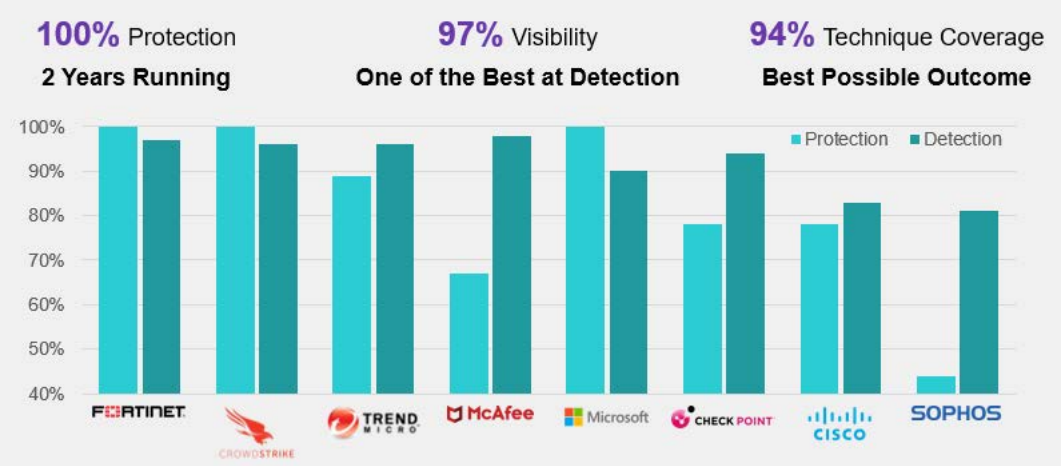
Out of those same 90 sub-techniques, FortiEDR also recognized the correct technique 94% of the time. This high detection rate ensures that admins receive accurate information using industry-specific terminology so they can quickly understand what FortiEDR is seeing and take appropriate action.

No Delayed Configuration Changes

Configuration changes happen for a variety of reasons, and some can be ignored (e.g., changes in logic). Readers of the MITRE ATT&CK Evaluation should look for configuration changes that cause delays, such as waiting for a verdict from an analyst or sandbox. Such delays can sometimes allow an attack to continue along the kill chain, potentially negatively impacting the organization. FortiEDR demonstrated no delayed configuration changes.

Summary

For the second year in a row, FortiEDR blocked all attacks without the use of signatures and fielded a top-five result in terms of total and analytic detection. For a step-by-step guide on how to read the report for yourself, please consult our white paper, How to Interpret MITRE ATT&CK Evaluations.



[i] It is worth noting that in round four, FortiEDR didn't participate in test seven for Linux since the threat hunting model for this operating system was in beta at the time of the test. Fortinet looks forward to participating in all tests in the next round.

June 20, 2022 9:55 AM
1636692-0-0-EN