CYBERNORDIC

CrowdStrike Achieves 100% Ransomware Protection Accuracy and 100% EDR Rating in SE Labs Test

November 6, 2023 Sagar Gulhane - Brad Moon - Liviu Arsene Endpoint & Cloud Security

100%
Ransomware Prevention.
CROWDSTRIKE
AAA Enterprise Advanced Security Award
2023 SE Labs Enterprise Advanced Security (EDR) Ransomware Test

- In the 2023 SE Labs Enterprise Advanced Security (EDR) Ransomware test, the AI-native CrowdStrike Falcon® platform achieved a 100% ransomware protection rating and scored a 100% EDR rating.
- Testing was even more challenging than last year, with 615 ransomware variants from 10 different ransomware families (including LockBit) employed in direct attacks on a Windows environment, in addition to sophisticated deep attacks mimicking the real-world observed tactics of cybercriminals.
- This marks the second year in a row the industry-leading Falcon platform detected and blocked all ransomware files during testing.

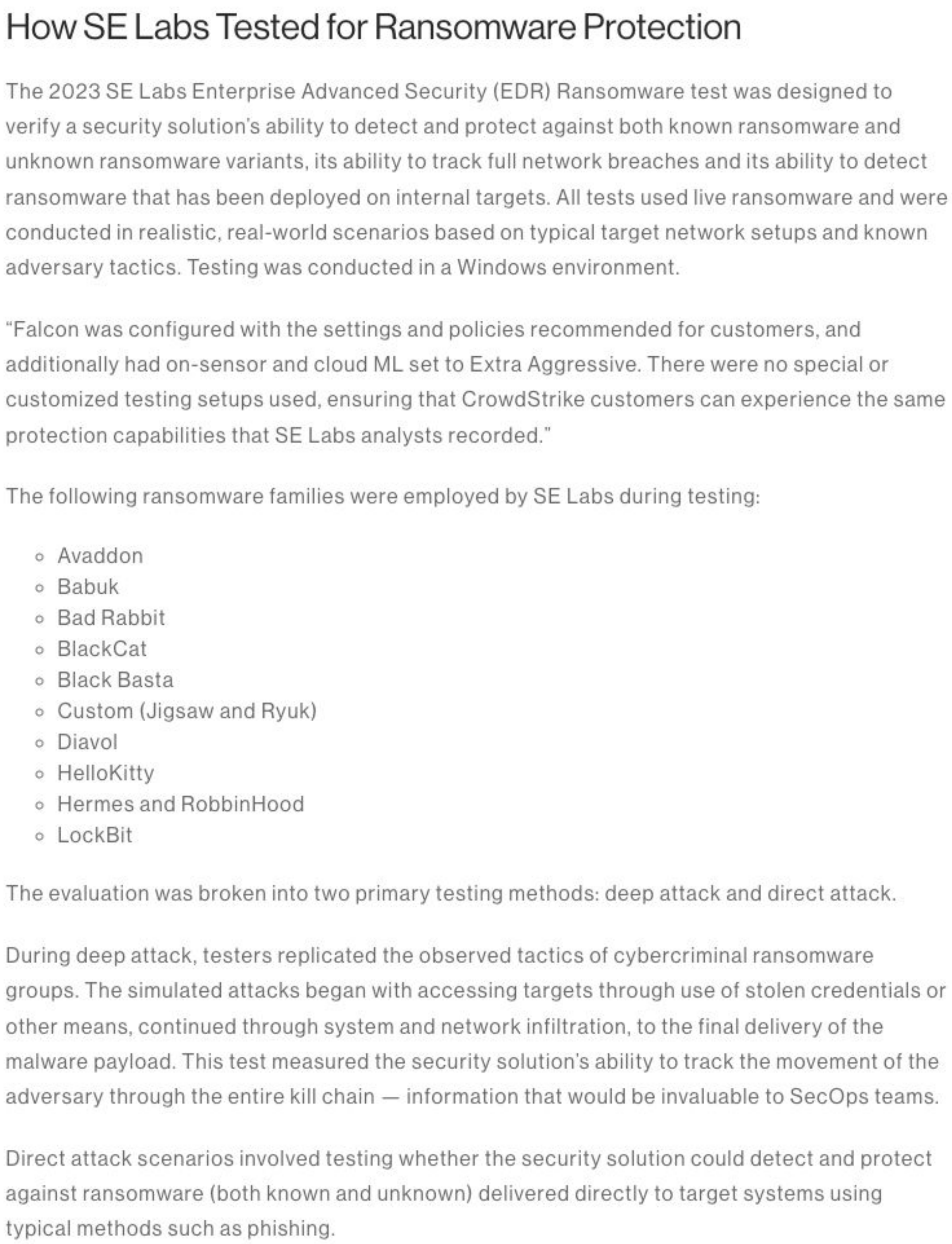
Ransomware is a scourge that is on track to inflict over $30 billion in damages in 2023. Businesses and organizations that are hit by a ransomware attack face a potentially devastating data breach, with system downtime, recovery, negative publicity and the likelihood of a ransom payment to deal with. Many small businesses are unable to recover from the ordeal and end up permanently shutting their doors within months of being hit.

Ransomware protection is a critical service that prevents data breaches from happening. However, not all cybersecurity solutions provide the same degree of protection. SE Labs is a leading third-party testing organization that performs independent evaluations of security products to determine how effective they are. The results of these tests are an important resource, helping companies to make an informed choice when comparing cybersecurity solutions.

The SE Labs Enterprise Advanced Security (EDR) Ransomware test pits cybersecurity solutions deployed in a Windows environment against the most sophisticated ransomware, employed in real-world scenarios that simulate both direct attacks and the deep attack tactics observed in use by cybercriminals. In last year's test — the first from SE Labs to feature endpoint detection and response (EDR) ransomware detection and prevention — the Falcon platform achieved 100% ransomware protection with zero false positives. This comprehensive evaluation tested the Falcon platform's protection effectiveness against sophisticated ransomware, and the impressive results show why Falcon dominates the endpoint security market.

The 2023 version of the SE Labs ransomware evaluation ratcheted up the intensity of the multi-week testing effort, making it even more challenging for participants. SE Labs uses a combination of original malware samples representing current threats, plus new variants created specifically to test the ability of cybersecurity solutions to detect and protect against previously unknown ransomware. While the 2022 evaluation employed 270 different ransomware samples, the total number of ransomware sample variations the Falcon platform faced in 2023 more than doubled to 615.

Once again, CrowdStrike demonstrated why Falcon is the cybersecurity platform of choice for so many businesses, companies and organizations — it detected and blocked all attempted Windows ransomware attacks during testing while also earning a perfect 100% EDR rating. This is the second straight year that Falcon delivered 100% ransomware protection in this test.



How SE Labs Tested for Ransomware Protection

The 2023 SE Labs Enterprise Advanced Security (EDR) Ransomware test was designed to verify a security solution's ability to detect and protect against both known ransomware and unknown ransomware variants, its ability to track full network breaches and its ability to detect ransomware that has been deployed on internal targets. All tests used live ransomware and were conducted in realistic, real-world scenarios based on typical target network setups and known adversary tactics. Testing was conducted in a Windows environment.

"Falcon was configured with the settings and policies recommended for customers, and additionally had on-sensor and cloud ML set to Extra Aggressive. There were no special or customized testing setups used, ensuring that CrowdStrike customers can experience the same protection capabilities that SE Labs analysts recorded."

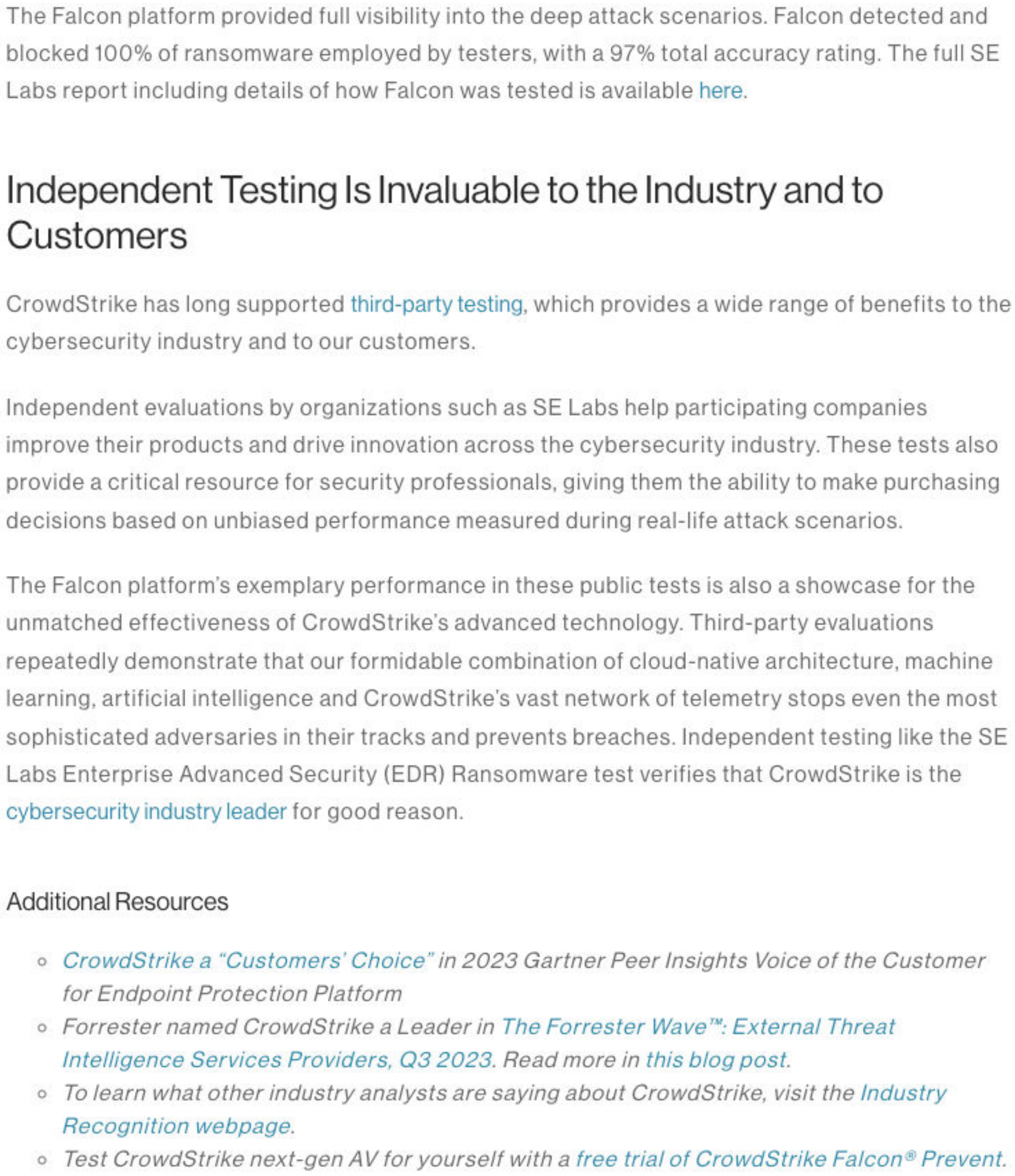
The following ransomware families were employed by SE Labs during testing:

- Avaddon
- Babuk
- Bad Rabbit
- BlackCat
- Black Basta
- Custom (Jigsaw and Ryuk)
- Diavol
- HelloKitty
- Hermes and RobbinHood
- LockBit

The evaluation was broken into two primary testing methods: deep attack and direct attack.

During deep attack, testers replicated the observed tactics of cybercriminal ransomware groups. The simulated attacks began with accessing targets through use of stolen credentials or other means, continued through system and network infiltration, to the final delivery of the malware payload. This test measured the security solution's ability to track the movement of the adversary through the entire kill chain — information that would be invaluable to SecOps teams.

Direct attack scenarios involved testing whether the security solution could detect and protect against ransomware (both known and unknown) delivered directly to target systems using typical methods such as phishing.



The Falcon platform provided full visibility into the deep attack scenarios. Falcon detected and blocked 100% of ransomware employed by testers, with a 97% total accuracy rating. The full SE Labs report including details of how Falcon was tested is available here.

Independent Testing Is Invaluable to the Industry and to Customers

CrowdStrike has long supported third-party testing, which provides a wide range of benefits to the cybersecurity industry and to our customers.

Independent evaluations by organizations such as SE Labs help participating companies improve their products and drive innovation across the cybersecurity industry. These tests also provide a critical resource for security professionals, giving them the ability to make purchasing decisions based on unbiased performance measured during real-life attack scenarios.

The Falcon platform's exemplary performance in these public tests is also a showcase for the unmatched effectiveness of CrowdStrike's advanced technology. Third-party evaluations repeatedly demonstrate that our formidable combination of cloud-native architecture, machine learning, artificial intelligence and CrowdStrike's vast network of telemetry stops even the most sophisticated adversaries in their tracks and prevents breaches. Independent testing like the SE Labs Enterprise Advanced Security (EDR) Ransomware test verifies that CrowdStrike is the cybersecurity industry leader for good reason.

Additional Resources

- *CrowdStrike a "Customers' Choice" in 2023 Gartner Peer Insights Voice of the Customer for Endpoint Protection Platform*
- *Forrester named CrowdStrike a Leader in The Forrester Wave™: External Threat Intelligence Services Providers, Q3 2023. Read more in this blog post.*
- *To learn what other industry analysts are saying about CrowdStrike, visit the Industry Recognition webpage.*
- *Test CrowdStrike next-gen AV for yourself with a free trial of CrowdStrike Falcon® Prevent.*