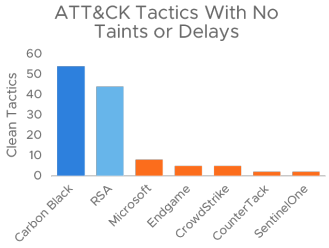
MITRE ATT&CK™ EVALUATION RESULTS: APT3

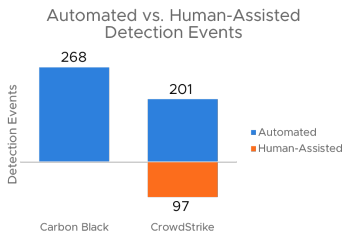
Carbon Black Outperforms All Other EDR Solutions

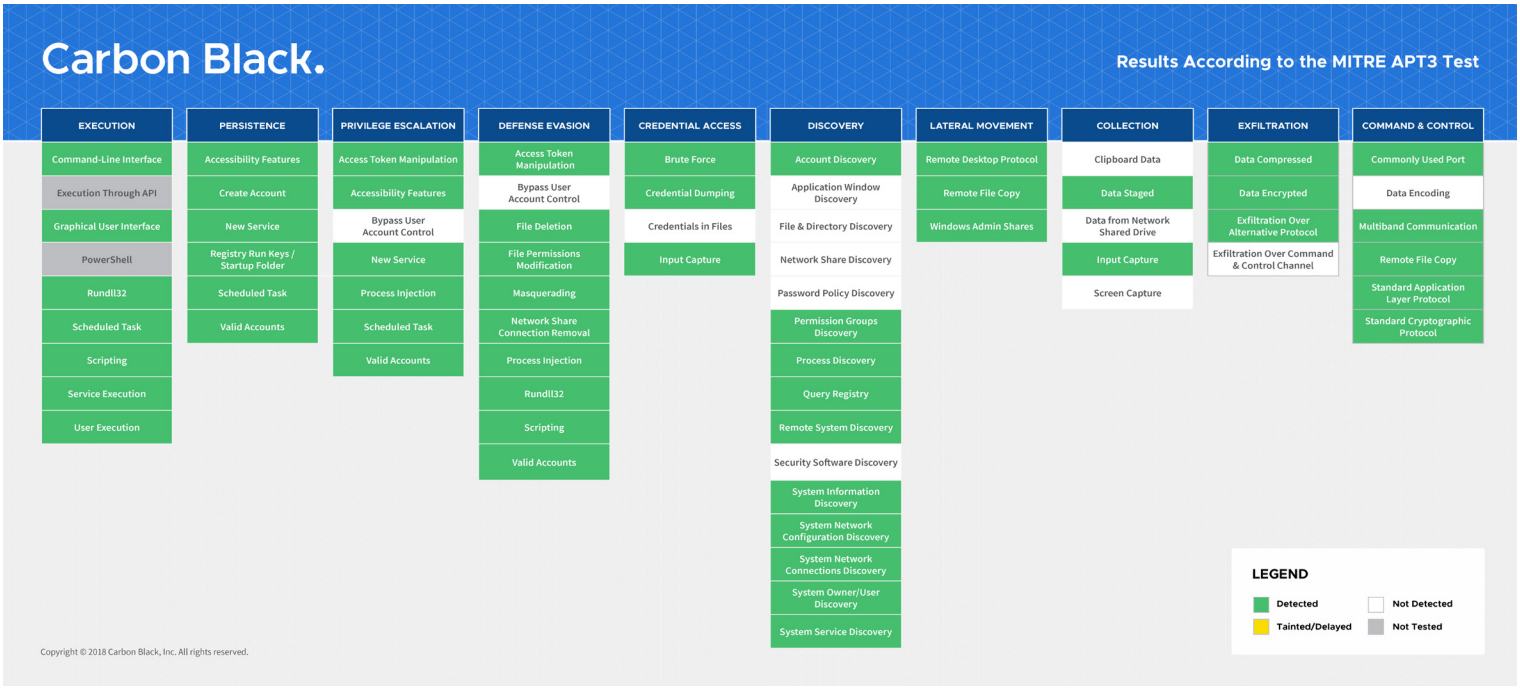
MITRE's public evaluation of endpoint detection and response (EDR) products demonstrated why Carbon Black is a top choice of security and IT professionals and showcased how Carbon Black detects sophisticated attacks quickly, so teams can respond confidently.

This test was based on MITRE's popular ATT&CK™ framework and represents a new approach to EDR testing: open, sophisticated, rigorous, and reflective of the real world. In the first test, which mirrored the tactics, techniques and procedures of APT3, Carbon Black demonstrated strong results that set us apart from the rest of the security products tested. Carbon Black showed:

- **Speed:** Zero delayed detections, so you can respond faster before the attack gets worse
- **Confidence:** Zero tainted detections, so you know that threats will be detected even as attackers change tactics
- **Predictability:** Zero reliance on humans in the loop, so you know detections will not be dependent on human intervention







Speed: Zero Delayed Detections

Many vendors had delayed detections, which happens when the capability does not detect the activity in real time or near-real time. Hours may pass as events are sent off out-of-band for either human or machine analysis. Delayed detections mean attackers have more time to spread throughout your environment and infect additional systems.

Carbon Black had no delayed detections, so when events happen you can respond much faster — in minutes instead of hours.

Confidence: Zero Tainted Detections

While many vendors did about the same in coverage, not all coverage is equal. Dig one layer deeper into the results and you'll see that many vendors' coverage models were tainted — meaning that detections *only* happened because the initial vector (e.g., PowerShell) was being monitored. The risk is that if the attacker uses a different initial approach, the detection may not happen.

Carbon Black had zero tainted detections, meaning we will still detect the same events even as attackers change their tactics.

Predictability: Zero Humans in the Loop

Other vendors — especially newer next-gen security providers — have an over-reliance on a human element in the process. While it's important to have people involved, requiring them for basic detection can introduce human error and delay.

Carbon Black had no humans in the loop during this evaluation. Every detection was produced automatically through the native product, without requiring a person to see, investigate, or send a note about it.

"Objective, transparent and open testing is critical as a means of driving the industry forward, and the MITRE ATT&CK™ framework offers a critical look at how real-world attacks play out. We believe MITRE has set an excellent standard for how testing should be conducted in an open, rigorous and sophisticated way. We thank MITRE for its leadership."

— SCOTT LUNDGREN, CHIEF TECHNOLOGY OFFICER, CARBON BLACK