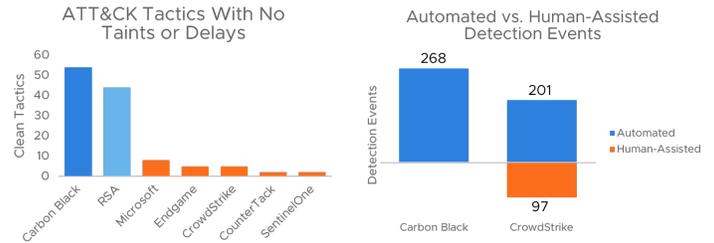


# Carbon Black Outperforms All Other EDR Solutions

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



## Carbon Black.

EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	EXFILTRATION	COMMAND & CONTROL
Command-Line Interface	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Brute Force	Account Discovery	Remote Desktop Protocol	Clipboard Data	Data Compressed	Commonly Used Port
Execution Through API	Create Account	Accessibility Features	Bypass User Account Control	Credential Dumping	Application Window Discovery	Remote File Copy	Data Staged	Data Encrypted	Data Encoding
Graphical User Interface	New Service	Bypass User Account Control	File Deletion	Credentials in Files	File & Directory Discovery	Windows Admin Shares	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Multiband Communication
PowerShell	Registry Run Keys / Startup Folder	New Service	File Permissions Modification	Input Capture	Network Share Discovery		Input Capture	Exfiltration Over Command & Control Channel	Remote File Copy
Rundll32	Scheduled Task	Process Injection	Masquerading		Password Policy Discovery		Screen Capture		Standard Application Layer Protocol
Scheduled Task	Valid Accounts	Scheduled Task	Network Share Connection Removal		Permission Groups Discovery				Standard Cryptographic Protocol
Scripting		Valid Accounts	Process Injection		Process Discovery				
Service Execution			Rundll32		Query Registry				
User Execution			Scripting		Remote System Discovery				
			Valid Accounts		Security Software Discovery				
					System Information Discovery				
					System Network Configuration Discovery				
					System Network Connections Discovery				
					System Owner/User Discovery				
					System Service Discovery				

### Results According to the MITRE APT3 Test

Tactic	Detected	Tainted/Delayed	Not Detected	Not Tested
Account Discovery	Yes	No	No	No
Application Window Discovery	Yes	No	No	No
File & Directory Discovery	Yes	No	No	No
Network Share Discovery	Yes	No	No	No
Password Policy Discovery	Yes	No	No	No
Permission Groups Discovery	Yes	No	No	No
Process Discovery	Yes	No	No	No
Query Registry	Yes	No	No	No
Remote System Discovery	Yes	No	No	No
Security Software Discovery	Yes	No	No	No
System Information Discovery	Yes	No	No	No
System Network Configuration Discovery	Yes	No	No	No
System Network Connections Discovery	Yes	No	No	No
System Owner/User Discovery	Yes	No	No	No
System Service Discovery	Yes	No	No	No

**LEGEND**

■ Detected   
 ■ Tainted/Delayed   
  Not Detected   
   Not Tested

## 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