

SOURCETEKIT VS. **CARBON BLACK**

COMPETITIVE ANALYSIS



**FOR MORE INFORMATION
CONTACT US**



ADVANTAGES

SourcetekIT vs. Carbon Black



SCOPE OF THREAT PROTECTION

SCOPE OF RESPONSE CAPABILITIES

MDR SERVICES

 SourcetekIT	Carbon Black.
Network, user and endpoint bases attacks	Endpoint attacks only
Cross environment automation and orchestration	Endpoint related remediations only
Native part of SourcetekIT core offering	Standalone services by 3rd party provider (eSentire) with additional payment



THE SOURCETEKIT DIFFERENCE

Detailed Explanation



ATTACK PREVENTION & DETECTION

Carbon Black is a traditional endpoint solution that focused on file / process-based threats: malware, exploits, fileless, Macros etc. and typically gain good results on that field. However, it lacks the ability to identify and block attacks that manifests only in anomalous network traffic (lateral movement, data exfiltration and network-based credential theft) or user behavior (anomalous login of compromised user account).

SourcetekIT uses Proprietary technology to continuously collect and analyze endpoint, user and network activities within the protected environment, powering the ability to identify and block both file/process-based attacks, as well network and user based ones, rendering complete coverage beyond the capabilities of Carbon Black.

RESPONSE

Coverage

Advanced cyberattacks target all parts of the environment: endpoints, files, process, user accounts and network traffic.

Unlike Carbon Black that has a limited number of endpoints/file remediations (isolate, kill process and delete/quarantine file), SourcetekIT uses Proprietary technology to provide a complete set of remediation tools for infected endpoints, malicious files/ processes, compromised user accounts and attacker-controlled traffic. Moreover, SourcetekIT can act as a response orchestration interface that communicates with core components such as Firewalls and Active Directory to expand the response process across the entire environment.

Automation

SourcetekIT supports response automation with both provided and user created remediation playbooks that chain together discreet remediation actions to a single flow. These playbooks enable the security team to radically scale their capacity by automating repetitive tasks, increasing the share of attacks that are addressed and resolved by SourcetekIT without need of human intervention.



THE SOURCETEKIT DIFFERENCE

Detailed Explanation

RESPONSE

Managed Detection Services (MDR)

SourcetekIT StOps team operates a 24\7 SOC, providing customers with full MDR services with no additional payment over SourcetekIT core offering. SourcetekIT StOps continuously monitors, trains and optimizes SourcetekIT detection algorithms based on over 30 threat intelligence feeds and detected attacks.

StOps provides SourcetekIT customers with the additional services:

- Alert monitoring
- Attack investigation
- Threat hunting
- Remediation guidance
- Exclusions, whitelisting and system fine tuning

MONITORING & CONTROL

Continuous monitoring of all entities and activities in the environment is enables users to discover exposed attack surfaces and address them (vulnerable systems and apps, unchanged user passwords, etc.), and by that eliminate the risk of up to 60% of common attack vectors.

SourcetekIT uses Proprietary to automate the collection and correlation of executed file/processes, user account activities, file access and network traffic, introducing unmatched speed and ease to all monitoring and control workflows.



SOURCEKIT VS CARBON BLACK COMPARISON TABLE

PREVENTION & DETECTION



PREVENTION & DETECTION

	 SourcetekIT	Carbon Black.
Multi Layered Malware Protection		
Signature Based	✓	✗
ML Based Static Analysis	✓	✗
Dynamic Analysis (Sandbox)	✓	✗
Compromised User Account Detection		
Anomalous User Logins	✓	✗
Preset User Activity Rules	✓	✗
Malicious Network Traffic		
Tunneling Based Data Exfiltration	✓	✗
Credential Theft (LLNMR\NBT-NS Attacks)	✓	✗
Lateral Movement (Pass The Hash etc.)	✓	✗
Reconnaissance (Scanning Attacks)	✓	✗



SOURCETEKIT VS CARBON BLACK COMPARISON TABLE

PREVENTION & DETECTION

	 SourcetekIT	Carbon Black.
Deception		
Decoys: Data Files, Credentials, Network Shares, URL, RDP	✓	✗
Response		
Host Remediation	Isolate, Restart, Change IP, Delete/Disable Service, Delete/Disable Scheduled Task, Run Command, Run Script	Isolate, Run Command, Run Script.
User Remediation	Disable/Enable, Reset Password	✗
Network Remediation Block	Block Traffic, Clear DNS Cache	✗
Orchestration		
Expand Remediation Across The Environment Infrastructure: Firewall, Proxy, AD, etc.	✓	✗
Automation		
Chain discreet remediation actions to a single flow that runs automatically when a predefined alert is triggered	✓	✗

SOURCETEKIT VS CARBON BLACK COMPARISON TABLE

PREVENTION & DETECTION

	 SourcetekIT	Carbon Black.
Infrastructure		
Number of Agents	One	One
Agent Impact on Endpoint Performance		
Clashes with Existing Software, Manual Exclusions, Blue Screens	Lightweight Agent with Minimal to Zero Impact	Three Separately Developed Agents Pieced Together
Deployment Model	Flexible: on-prem, SaaS or Hybrid	On-Prem, SaaS
Agent Impact on Endpoint Performance		
Clashes with Existing Software, Manual Exclusions, Blue Screens		Requires Additional Payment
Managed Detection & Response Services		
Full MDR Integrated in the Product Offering		Requires Additional Payment