ForeScout Extended Module for Carbon Black

Fortify endpoint defenses and proactively combat threats across the network

Enterprise IT and security teams are managing increasingly complex environments characterized by exponential growth and increase in diversity of devices connecting to the network. The rise in network-connected devices increases the attack surface and allows cybercriminals to capitalize on the weakest link to gain a foothold on your network. If undetected, compromised devices can be used as launch pads to target higher-value assets, gain access to sensitive information and cause significant business impact.

Highlights

- Verify Carbon Black agents are installed, operational and communicating properly with Carbon Black
- Share system and user information for Carbon Black-managed devices with ForeScout while they are on-site or off enterprise networks
- Leverage Carbon Black threat intelligence for threat hunting for Indicators of Compromise (IOCs) across endpoint and network tiers
- Prevent infected devices from gaining access to corporate network resources without appropriate remediation
- Isolate, restrict or block compromised devices on the network in near real-time and initiate remediation actions

Benefits

- Comprehensive visibility across network-connected devices including BYOD, guest, IoT and off-premises corporate devices
- Improved security hygiene and Carbon Black agent coverage on supported corporate devices
- Reduced mean time to detect (MTTD) and mean time to respond (MTTR) for advanced threats
- Automated threat response and reduced manual processes for improved security operations

The Challenges

- Achieving consolidated visibility into managed and unmanaged devices, including BYOD, guest, IoT and off-premises corporate devices
- Verifying device hygiene and ensuring requisite security agents such as Carbon Black agents are installed and operational on all supported corporate devices
- Identifying Indicators of Compromise (IOCs) on targeted or compromised devices
- Ensuring that infected devices cannot gain access to the corporate network without appropriate remediation actions
- Reducing lengthy response time and manual processes for isolating compromised endpoints, containing threats to avoid lateral propagation and minimizing risk of data loss

The ForeScout Solution

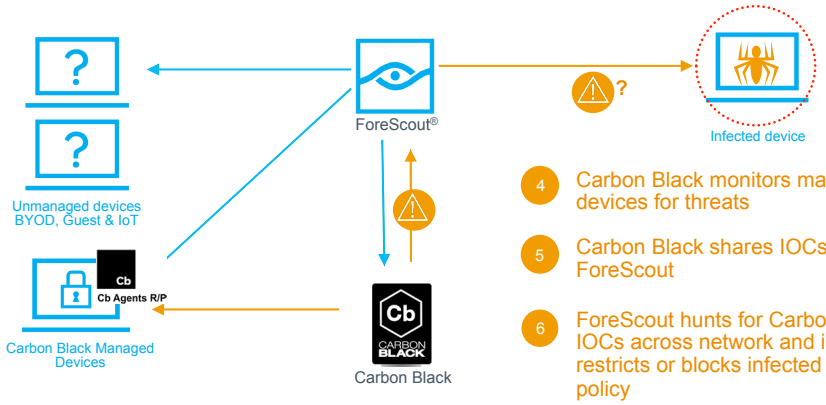
The ForeScout Extended Module for Carbon Black orchestrates information sharing and security workflows between ForeScout CounterACT® and Carbon Black to improve device hygiene, proactively detect threats across the network and automate threat response. This solution combines the agentless visibility and control capabilities of the ForeScout platform with the threat intelligence and advanced endpoint protection of the Carbon Black solution.

The ForeScout platform discovers, classifies and assesses devices connecting to your network, including BYOD, IoT, virtual and other non-traditional devices that are not managed by Carbon Black. Based on your policy, ForeScout can limit or block access to the network for non-compliant or infected devices, and initiate remediation actions to fix endpoint security gaps. Devices that leave the network are verified when they reconnect to enforce compliance and identify possible infections before being allowed appropriate network access.

Carbon Black's endpoint threat hunting and incident response solution leverages advanced techniques to detect IOCs and identifies devices infected by malware. It can prevent ransomware and malware detonation, and collect forensic data for investigation and response.

The joint solution between ForeScout and Carbon Black (including Cb Protection and Cb Response) allows you to leverage Carbon Black threat intelligence to proactively combat threats across both Carbon Black- and ForeScout-managed endpoints, and orchestrate workflows to isolate and remediate compromised devices. This enables you to accelerate threat response, limit malware propagation and reduce potential negative business impact.

1. ForeScout CounterACT® discovers managed & unmanaged devices
2. ForeScout verifies Carbon Black agent is operational
3. ForeScout initiates Carbon Black enrollment or other remediation actions on non-compliant devices



4. Carbon Black monitors managed devices for threats
5. Carbon Black shares IOCs with ForeScout
6. ForeScout hunts for Carbon Black IOCs across network and isolates, restricts or blocks infected devices per policy

Learn More about ForeScout Extended Modules

The ForeScout Extended Module for Carbon Black is an add-on module for ForeScout CounterACT that is sold and licensed separately. It is one of many ForeScout Modules that enable CounterACT to exchange information, automate multivendor workflows and accelerate system-wide response.

For details on our licensing policy, see www.forescout.com/licensing

Use Cases

Enhanced device visibility

ForeScout provides you with enhanced discovery, classification and assessment of managed and unmanaged devices on your network across campus, data center, cloud and OT environments— in short, across the extended enterprise. In addition, ForeScout leverages host properties received from Carbon Black for your ForeScout policies.

Verify and enforce Carbon Black agent hygiene

ForeScout improves security hygiene by verifying that Carbon Black agents are installed, running and operating properly on supported corporate endpoints. ForeScout detects not-yet-enrolled devices and incorrectly functioning agents, and triggers workflows to enforce client-side and server-side compliance.

Leverage shared threat intelligence for joint threat hunting

Carbon Black identifies malware and IOCs through advanced techniques and notifies ForeScout upon detection. ForeScout leverages this threat intelligence to monitor the network for IOCs, including unmanaged connected systems such as BYOD, guest and IoT devices as well as network infrastructure components. Based on your policy, ForeScout can restrict, isolate or block network access for compromised devices.

Accelerate and automate policy-driven threat response

When Carbon Black identifies malware or malicious behavior, it informs ForeScout in near real-time. Based on threat severity and your policy, ForeScout can automatically take appropriate actions such restricting, isolating or blocking compromised devices, and initiating remediation workflows. The combination of Carbon Black host actions and ForeScout network actions allows you to reduce your mean time to respond (MTTR) and limit the impact of threats.

Learn more at
www.ForeScout.com

ForeScout

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591