Forescout eyeExtend
for Carbon Black®

Fortify endpoint defenses and proactively combat threats

Enterprise IT and security teams are managing increasingly complex environments with exponential growth in the volume and diversity of devices connecting to the network. The rise in network-connected devices increases the attack surface and allows threat actors to capitalize on the weakest link to gain a foothold on your network. To combat cyberthreats, organizations use the Carbon Black endpoint security solution. However, unmanaged— bring your own devices (BYOD), Internet of Things (IoT) and transient devices that connect to the network unnoticed pose a risk that must still be addressed. If compromised devices are left undetected, they can be used as launch pads to target higher-value assets, gain access to sensitive information and cause significant business impact.

Forescout eyeExtend for Carbon Black provides a comprehensive approach to security that spans complete device visibility, helps enforce device compliance, extends threat hunting to unmanaged devices and automates network access control for threat mitigation in real time.

Challenges

- Understanding the entire attack surface to plan and execute protection against advanced threats

- Minimizing IT and security staffs' manual workload of managing device compliance

- Reducing lengthy response time and manual processes for limiting network access of the compromised devices to contain threats in order to avoid lateral threat propagation

The Solution

Forescout eyeExtend for Carbon Black orchestrates information sharing and security workflows between the Forescout platform and Carbon Black to improve device hygiene, proactively detect threats across the entire network and automate threat response.

Leveraging the real-time device discovery, classification and assessment provided by Forescout eyeSight, eyeExtend for Carbon Black notifies Carbon Black as soon as a device connects to the network. This enables Carbon Black to bring more devices under its endpoint protection management and detect threats across the entire enterprise attack surface. The Forescout platform continuously validates the integrity of Carbon Black agents and helps enforce device compliance at all times by initiating remediation of the nonconforming devices. Forescout platform also strengthens threat detection and enforcement by extending Carbon Black endpoint threat intelligence to automatically hunt for, mitigate and remediate threats across device types and network tiers.
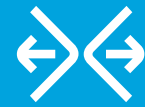
eyeExtend

Benefits

- Reduce security risk by extending Carbon Black's threat intelligence to automatically hunt for, mitigate and remediate threats across device types and network tiers

- Increase operational efficiency by assessing devices in real time and bringing all devices under Carbon Black endpoint protection

- Automate threat remediation and response for noncompliant or compromised devices

Highlights

- Get complete device visibility without requiring agents

- Verify that devices have Carbon Black agents properly installed and operational at all times

- Share threat intelligence to hunt for indicators of compromise (IOCs) across managed and unmanaged devices

- Dynamically control network access by isolating, restricting or blocking compromised devices in real time

- Get out-of-the box integration with CB Protection and CB Response

Forescout eyeExtend for Carbon Black helps reduce your attack surface, minimizes malware propagation and limits the impact of security breaches

Use Cases

**Improve device security coverage and compliance**

The Forescout platform continuously verifies that Carbon Black Response sensor and Carbon Black Protection agent are installed, running and operating properly on managed corporate devices. When new devices connect to the network, the Forescout platform informs administrators on the agent status of the devices. If a connecting device does not comply with the security policy, the Forescout platform notifies the administrator and facilitates remediation by redirecting users to a self-help page for agents installation. Devices that leave the network are verified when they reconnect to enforce compliance.

Leverage shared threat intelligence to maximize joint threat hunting and detection

When Carbon Black identifies malware and IOCs on managed devices, it immediately notifies Forescout eyeExtend for Carbon Black. The Forescout platform extends this threat intelligence to the entire network and monitors unmanaged connected systems such as BYOD, guest and IoT devices for IOCs. Based on your security policies, the Forescout platform can restrict, isolate or block network access for compromised devices in real time.

Accelerate and automate policy-driven threat response

Carbon Black informs Forescout eyeExtend for Carbon Black upon malware or threat detection on a device. Based on threat severity and the security policy, the Forescout platform can automatically take appropriate actions, such as restricting, isolating or blocking compromised devices, and initiating remediation workflows. The Forescout platform's network control actions reduce your mean time to respond and limit the impact of threats.
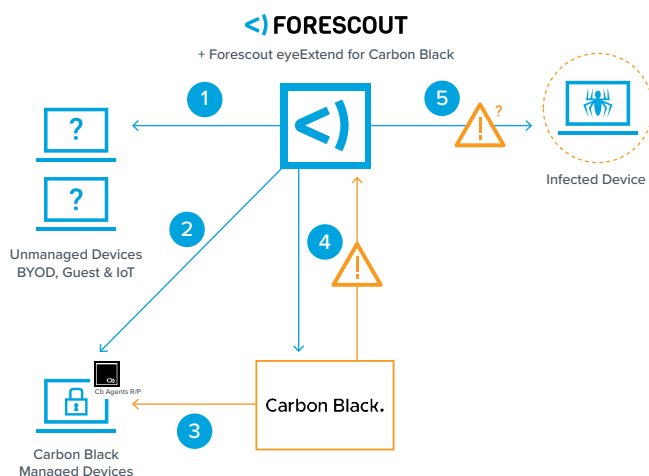
1. The Forescout platform discovers managed and unmanaged devices on the network
2. Forescout platform verifies that the Carbon Black agent is operational on managed devices
3. Forescout platform initiates Carbon Black agent deployment or updates on noncompliant devices
4. Carbon Black monitors managed devices for threats and shares IOCs with the Forescout platform
5. Forescout platform hunts for Carbon Black IOCs across the network and isolates, restricts or blocks infected devices per policy

Learn more at Forescout.com