Forescout eyeExtend for CrowdStrike®

Strengthen endpoint defenses and accelerate threat response

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 endpoint security solutions such as the CrowdStrike's Falcon platform. However, unmanaged 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 CrowdStrike provides a comprehensive approach to security that spans complete device visibility, helps increase CrowdStrike managed endpoint coverage and security hygiene, extends threat hunting to unmanaged devices and accelerates threat response 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 times and manual processes to address threats in order to avoid lateral threat propagation

The Solution

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

eyeExtend for CrowdStrike leverages the comprehensive device discovery, classification, assessment and context provided by Forescout eyeSight. With complete device visibility, Forescout eyeExtend makes CrowdStrike aware of every single network-attached device—whether managed, unmanaged or transient—the instant it connects. This enables CrowdStrike 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 CrowdStrike agents and helps enforce device compliance at all times by initiating remediation of the nonconforming devices. Forescout also strengthens threat detection and enforcement by extending CrowdStrike endpoint threat intelligence to automatically hunt for, mitigate and remediate threats across device types and

eyeExtend

Benefits

- Reduce security risk by extending CrowdStrike's threat intelligence to automatically hunt for, mitigate and remediate threats across all devices— managed and unmanaged
- Increase operational efficiency by assessing devices in real time and bringing all devices under CrowdStrike's endpoint protection
- Automate threat remediation and response for noncompliant or compromised devices

Highlights

- Get complete visibility across managed, unmanaged and transient devices-on and off-premises
- Validate that all devices have CrowdStrike agents installed, operational, updated and communicating properly with the CrowdStrike cloud
- Prevent noncompliant CrowdStrike-managed devices from gaining access to corporate resources without appropriate remediation
- Dynamically control network access by isolating, restricting or blocking compromised devices in real time

network tiers. Forescout eyeExtend for CrowdStrike helps reduce your attack surface, minimizes malware propagation and limits the impact of security breaches.

Use Cases

Improve device security coverage and compliance

Forescout continuously verifies that the CrowdStrike agent is installed and running on supported devices and communicating properly with the CrowdStrike cloud. After determining if a device is new, unmanaged or has a broken agent, Forescout notifies the administrators and facilitates remediation by redirecting users to a self-help page for agent installation. Devices that leave the network are verified when they reconnect to enforce compliance.

Improve insight into corporate devices on-site or off-premises

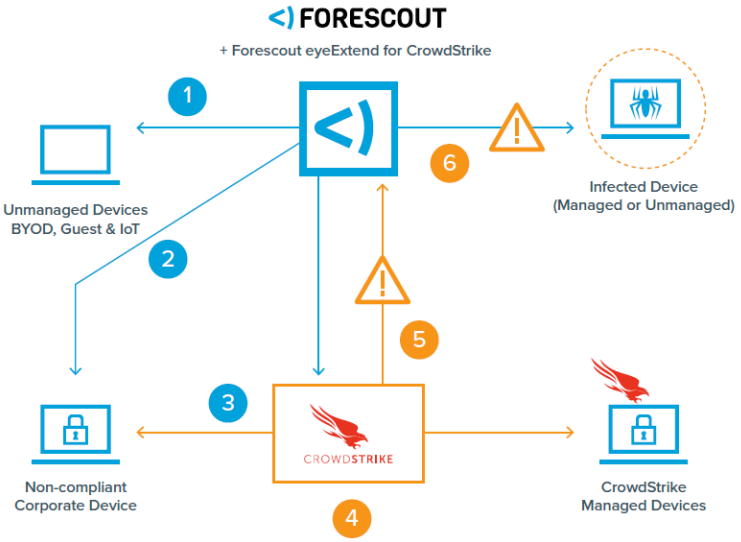
Forescout eyeExtend powered by Forescout eyeSight provides comprehensive visibility across all networked attached devices agentlessly. The Forescout platform also pulls device information on CrowdStrike-managed devices while those devices are on-site or off the enterprise network, providing you with a more comprehensive device inventory.

Leverage shared threat intelligence to maximize joint threat hunting and detection

CrowdStrike identifies malware and Indicators of Attacks (IOAs) on managed devices and notifies Forescout eyeExtend upon detection. Forescout leverages this threat intelligence to monitor the network for IOAs across unmanaged devices such as BYOD, guest and IoT, as well as network infrastructure. Based on your policy, the Forescout platform can limit network access for compromised devices dynamically.

Accelerate and automate policy-driven threat response

Upon detection of malware or malicious behavior, CrowdStrike immediately informs Forescout eyeExtend. Based on threat type and your policies, the Forescout platform automatically takes appropriate network control actions such as restricting or blocking compromised devices in real time. If an on- or off-prem device is found to be infected, CrowdStrike can trigger the Forescout platform to dynamically isolate the device and contain the threat by cutting off all network access except for its access to the CrowdStrike server for remediation. Forescout's network control actions reduce your mean time to respond (MTTR) and limit the impact of threats.



1. Forescout discovers managed and unmanaged devices on the network
2. Forescout verifies that the CrowdStrike agent is operational on managed devices
3. Forescout initiates CrowdStrike agent deployment or updates on noncompliant devices
4. CrowdStrike monitors managed devices
5. CrowdStrike shares IOAs/threat intelligence with Forescout eyeExtend
6. Forescout hunts for CrowdStrike IOAs across all devices, isolates infected devices and initiates remediation per policy

FORESCOUT

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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

Learn more at Forescout.com

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at https://www.forescout.com/company/ legal/intellectual-property-patents-trademarks. Other brands, prod¬ucts, or service names may be trademarks or service marks of their respective owners. **Version 9_20B**