ForeScout

Datasheet

ForeScout Extended Module for CrowdStrike

Fortify endpoint defenses and proactively combat threats across the network

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. 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.

The Challenges

- Lack of 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 CrowdStrike Falcon® are installed, operational and communicating properly with their management services on all supported corporate devices
- Identifying Indicators of Attacks (IOAs) and targeted or compromised endpoints across the varied device landscape
- Ensuring that devices infected on public networks cannot gain access to the corporate network without appropriate remediation actions
- Reducing lengthy response times and manual processes required to isolate compromised endpoints and contain threats to avoid lateral propagation and minimize risk of data loss

The ForeScout Solution

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

ForeScout discovers, classifies and assesses devices connecting to your network, including BYOD, IoT, virtual and other non-traditional devices that are not managed by CrowdStrike. Based on your policy, ForeScout can limit or block access to the network for devices that are non-compliant or infected, 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.

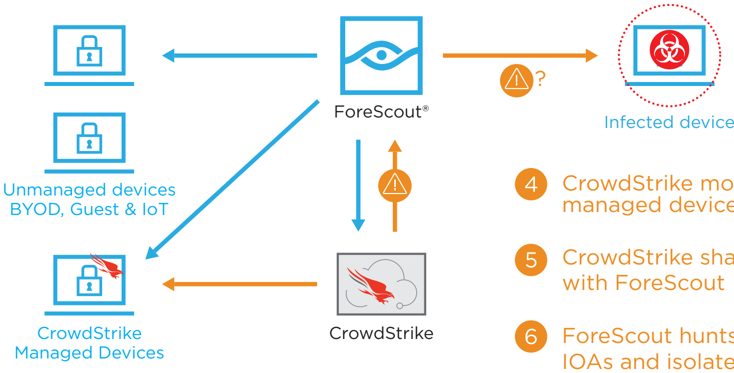
Highlights

- Verify CrowdStrike Falcon agent is installed, operational and communicating properly with CrowdStrike Falcon cloud
- Share system and user information for CrowdStrike-managed devices with ForeScout while they are on-site or off enterprise networks
- Share threat intelligence across solutions for joint threat hunting for Indicators of Attack (IOAs) across endpoint and network tiers
- Prevent infected and non-compliant CrowdStrike-managed 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 managed devices off-premises
- Improved security hygiene and CrowdStrike 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

1. ForeScout CounterACT® discovers managed & unmanaged devices
2. ForeScout verifies CrowdStrike agent is installed, operational and communicating properly with CrowdStrike cloud service
3. ForeScout initiates CrowdStrike enrollment or other remediation actions on non-compliant devices



4. CrowdStrike monitors managed devices for threats
5. CrowdStrike shares IOAs with ForeScout
6. ForeScout hunts for CrowdStrike IOAs and isolates, restricts or blocks infected devices per policy

CrowdStrike is a cloud-delivered endpoint-protection solution that leverages advanced techniques to detect IOAs and identify devices infected by malware. It can prevent ransomware and malware detonation, and collects forensic data for investigation and response.

The joint solution allows you to leverage CrowdStrike threat intelligence to proactively combat threats across both CrowdStrike- 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 business impact.

Use Cases

Improve Endpoint Security Coverage and Compliance

ForeScout improves security hygiene by verifying that the CrowdStrike Falcon agent is running on supported corporate endpoints and communicating properly with CrowdStrike Falcon cloud. ForeScout detects not-yet-enrolled devices and incorrectly functioning agents, and triggers workflows to enforce managed endpoint compliance.

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

CrowdStrike shares device properties for CrowdStrike-managed devices with ForeScout while those devices are on-site or off enterprise networks, providing you with a more comprehensive device inventory. This allows you to leverage CrowdStrike device properties within ForeScout policies for on-the-move transient devices. If CrowdStrike determines that a remote device is compromised, ForeScout can prevent access to corporate networks and services until the device is remediated.

Leverage shared threat intelligence to maximize joint threat hunting and detection

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

Accelerate and automate policy-driven threat response

When CrowdStrike identifies malware or malicious behavior, it informs ForeScout right away. 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 CrowdStrike host actions and ForeScout network actions allows you to reduce your mean time to respond (MTTR) and limit the impact of threats.

Learn More about ForeScout Extended Modules

The ForeScout Extended Module for CrowdStrike 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

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