ForeScout Extended Module for IBM® BigFix®

Fortify endpoint defenses, enforce compliance and reduce your attack surface

Today's increasingly mobile users combined with the diversity of IP-connected devices pose formidable security operations challenges. Agent-based approaches work on traditional systems that can support them—assuming agents are present and functional. However, an increasing number of Internet of Things (IoT) and other emerging devices cannot be managed with agents. To protect the network and its assets, operations and security teams need comprehensive endpoint security solutions that provide real-time visibility and control across varied types of connected and remote devices to reduce the attack surface.

Highlights

See

- Discover traditional and non-traditional endpoints as they connect to the network —without requiring software agents
- Profile and classify corporate, BYOD, IoT, OT and network infrastructure devices
- Assess device hygiene and continuously monitor security posture

Control

- Notify end-users, administrators or IT systems about security issues
- Comply with security policies, industry mandates and best practices
- Restrict, isolate or quarantine non-compliant, vulnerable or compromised devices

Orchestrate

- Verify presence of operational BigFix agent and automate enrollment
- Leverage BigFix host properties within CounterACT policies
- Trigger BigFix host-based remedial actions via CounterACT policies to coordinate host and network response

The Challenges

Visibility. Serious efforts to manage security risk must start with knowing what users and devices are on your network and their security posture. Most organizations are unaware of a significant percentage of endpoints on their network because they cannot detect:

- Devices with disabled or broken agents
- Unmanaged guest or bring-your-own devices (BYOD)
- IoT devices
- Transient devices, undetected by periodic scans
- Remote corporate devices not directly connected to the network

Endpoint Compliance. To achieve and maintain compliance with internal policies and external mandates, organizations need real-time solutions to assess device security state and identify security issues. Are management and security agents installed and operational on agent-supported corporate devices? Are BYOD, IoT and other devices that cannot be managed via agents compliant with your security policies? Are you aware of indicators of compromise (IOCs) that may present a high security risk? Can you enforce compliance on corporate devices that are not directly connected to your corporate network?

Response Automation. Traditional risk-management and incident-response techniques rely on manual processes and IT staff to fix endpoint security gaps and maintain compliance with security policies. The velocity and evasiveness of sophisticated attacks that target vulnerable endpoints as launch pads, coupled with the increasing endpoint growth and diversity, can easily overwhelm such labor-intensive methods. Organizations need automated solutions to isolate non-compliant, high-risk or compromised endpoints and initiate network and host remediation actions.

The ForeScout Solution

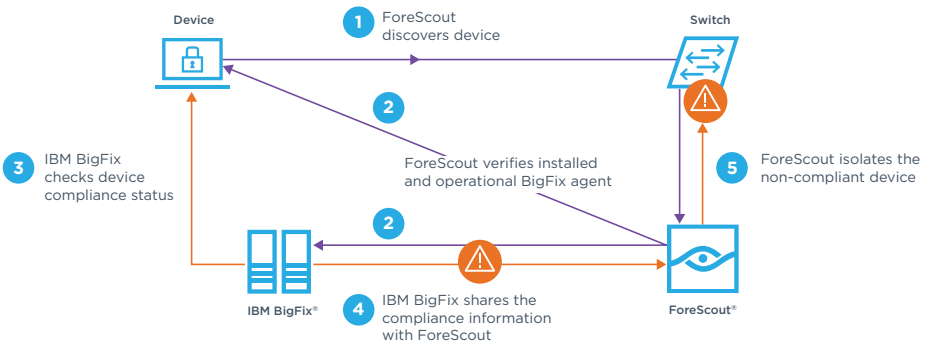

Figure 1: ForeScout Extended Module for IBM BigFix workflow.

The Extended Module for IBM BigFix® leverages the real-time visibility capabilities of ForeScout CounterACT® to discover and profile both managed and unmanaged endpoints, including those that do not support agents. When security or compliance issues arise, ForeScout extends BigFix response and remediation capabilities with network controls to restrict or isolate problematic devices, and orchestrates workflows to trigger host remediation actions. This joint solution provides a range of essential endpoint security capabilities, including:

Comprehensive endpoint visibility

CounterACT extends BigFix endpoint visibility with agentless discovery and profiling of traditional and non-traditional devices, including network infrastructure, BYOD, IoT and operational technology (OT) systems. CounterACT can also leverage BigFix host properties in its own policies. This integration provides a more complete and unified view of connected devices, more granular security policies and reduced management complexity.

Maximizing BigFix agent effectiveness

CounterACT inspects endpoints at the time of connection to verify that the BigFix agent is installed, enabled and fully operational on supported corporate systems. If the agent is absent, broken or disabled, CounterACT can either enroll the device itself or trigger the automated BigFix deployment process.

Endpoint compliance and response

This joint solution enables you to monitor endpoint security posture and compliance across today's diverse range of connected devices. For BigFix-managed devices, the BigFix agent performs a variety of configuration, security and compliance checks and verifications. CounterACT provides complementary assessment of devices that are not managed by BigFix. If either finds a device to be out of compliance, CounterACT can immediately quarantine or move it to a restricted network segment and trigger remediation actions to mitigate risk.

Off-premises endpoint remediation

CounterACT can leverage BigFix to trigger remedial actions on off-premises corporate devices in response to the latest vulnerability information or threat intelligence. Granular actions can include deleting malicious files, removing high-risk applications and forcing configuration changes. When a device reconnects to the network, CounterACT can verify that the remediation actions were performed and allow or restrict network access accordingly.

Learn More about ForeScout Extended Modules

The ForeScout Extended Module for IBM BigFix 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