

ForeScout Extended Module for IBM BigFix

Date: May 2018 **Author:** Tony Palmer, Senior IT Validation Analyst

Abstract

This report provides a first look at the key benefits of integrating ForeScout CounterACT with IBM BigFix endpoint management and security solution. ESG Lab focused on how the ForeScout Extended Modules can combine ForeScout's endpoint insight, classification, and control capabilities with IBM BigFix. This integration is designed to discover and classify users and devices, verify the presence and operation of BigFix Agents, enforce compliance, and take automated host or network actions when needed.

The Challenges

According to ESG research, strengthening cybersecurity was cited by 44% of respondents as the business initiative that would drive the most technology spending at their organizations in 2018 (see Figure 1).¹

Figure 1. Top Five Business Initiatives Driving IT Spending in 2018



Source: Enterprise Strategy Group

This is hardly surprising, considering the multitude of cybersecurity incidents organizations are experiencing. In a 2016 research project conducted by ESG and the Information Systems Security Association ([ISSA](#)), 39% of cybersecurity professionals said that their organization had experienced one or more incidents resulting in the need to reimage one or more endpoints or servers; 27% reported experiencing a ransomware incident; and 20% stated they had experienced at

¹ Source: ESG Master Survey Results, [2018 IT Spending Intentions Survey](#), December 2017.

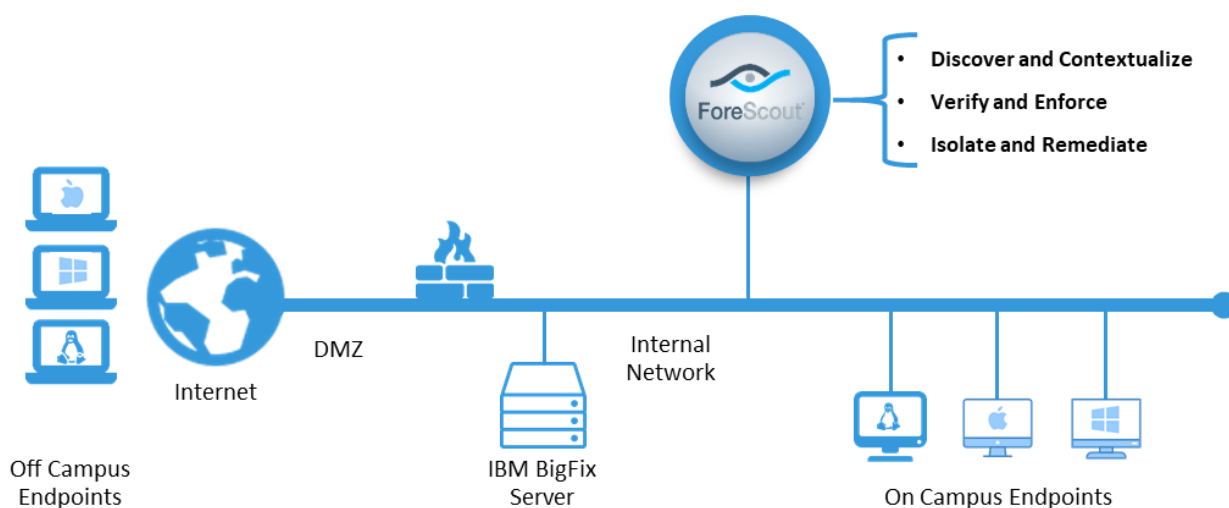
least one security incident that disrupted a business application.² Adding to these challenges is an increasing skills gap in cybersecurity. Fifty-one percent of organizations claim that they have a problematic shortage of cybersecurity skills—the most frequently cited response by a wide margin.³ In addition, the increase in mobile, personal, transient, and even virtual devices leaves many organizations unaware of a significant percentage of the endpoints on their networks. These devices are either not under management, have nonfunctional agents, or are only detected during intermittent scans.

The ForeScout Extended Module for IBM BigFix

The ForeScout CounterACT platform is designed to provide continuous security monitoring and remediation of an organization's devices, both traditional and nontraditional, while they remain connected to the network. ForeScout's goal is to provide IT organizations with comprehensive insight into their endpoint landscape and compliance posture while addressing network access and threat management challenges.

In conjunction with ForeScout CounterACT, the ForeScout Extended Module for IBM BigFix provides visibility, classification, and exchange of real-time contextual information for managed and unmanaged endpoints. CounterACT verifies whether a BigFix agent is installed and operational on an endpoint, and can enroll the client or restart the agent if needed. BigFix then checks the device's compliance status and shares it with ForeScout. If the device is non-compliant, ForeScout initiates appropriate isolation and/or remediation actions leveraging CounterACT for network-level device isolation and BigFix for endpoint patch deployment or configuration changes.

Figure 2. ForeScout Extended Module for IBM BigFix



The joint solution utilizes ForeScout's agentless discovery and control of endpoints on the network, enabling real-time endpoint visibility and profiling of traditional and non-traditional devices that are not managed by BigFix, including network infrastructure, operational technology (OT) systems, BYOD, IoT devices, phones, and tablets. The ForeScout Extended Module for IBM BigFix allows organizations to identify corporate endpoints that are missing and that need the BigFix Agent and to automatically deploy BigFix Agents to those endpoints. In addition, when BigFix sends messages indicating compliance violations, ForeScout triggers automated network actions to isolate and/or remediate endpoints. ForeScout also interfaces with BigFix to verify and enforce an endpoint's compliance state with security and regulatory mandates, and facilitates automated host actions to remediate endpoints.

² Source: ESG/ISSA Research Report, [Through the Eyes of Cyber Security Professionals: Annual Research Report \(Part II\)](#), December 2016.

³ Source: ESG Master Survey Results, [2018 IT Spending Intentions Survey](#), December 2017.

ESG Lab Tested

ESG Lab evaluated the ForeScout Extended Module for IBM BigFix which creates a bi-directional integration between ForeScout CounterACT and IBM BigFix. ESG validated the ability of the joint solution to discover and profile endpoints as they attach to the network, verify whether the BigFix agent is installed and running, and verify compliance.

ESG Lab configured the integration between ForeScout CounterACT and IBM BigFix in just a few steps. First, ESG Lab created an account on the BigFix root server for ForeScout, and then configured the ForeScout Extended Module for IBM BigFix with the IP address of the root server and the login credentials. The whole process took less than a minute, and we used the built-in CounterACT policies for BigFix. Once the integration was configured and endpoints connected to the network, we could see the information collected by the ForeScout Extended Module (Figure 3).

Figure 3. Endpoint Visibility with ForeScout Extended Module for IBM BigFix

The screenshot displays the ForeScout interface. At the top, a table titled 'All Hosts' shows a list of endpoints. The first row is highlighted with a red box, showing the following details:

Host IP	MAC Address	Segment	BigFix Agent Version	Policy IBM BigFix Patch Compliance	Policy IBM BigFix Agent Compliance	Actions
10.1.125.101	005056854cfc	Workstations	9.5.6.63	Critical	IBM BigFix Client Running and checked in within last 30 m...	

Below the table, a detailed view of the selected endpoint is shown. It includes the following information:

- IPv4 Address:** 10.1.125.101
- Hostname:** WIN7
- MAC Address:** 005056854cfc
- Domain:** CORE

The interface also shows a search bar and a list of host classification details:

- Host classification:** Windows
- General:** General
- User:** IP v4 Address: 10.1.125.101
- Network Access:** Admission: VMware vSphere New Endpoint
- Security:** DNS Name: win7-...alliances-lab.net
- Open Ports:** 135/TCP, 139/TCP, 445/TCP, 3389/TCP, 49156/TCP

ESG demonstrated that the ForeScout platform can discover and profile traditional endpoints that can be managed by IBM BigFix, such as the Windows machine shown above, as well as non-traditional endpoints that are not managed by BigFix like network infrastructure devices, BYOD endpoints, and IoT devices. In our tests, ForeScout provided extended visibility and control across device types when they connected to the corporate network. BigFix provided endpoint configuration management and security regardless of corporate network connectivity and bandwidth. ForeScout visibility provided for the discovery of corporate devices that should be protected with configuration management through BigFix. The ForeScout Extended Module for BigFix also leveraged BigFix properties for applicable endpoints, which enhanced real-time insight, enabled refinement of policies and enforcement with automated controls through CounterACT. As seen in Figure 4, the ForeScout Extended Module verified endpoint OS and patch level compliance. Configuration hardening and other configuration requirements can also be verified and enforced for required endpoints.

Figure 4. Compliance Verification and Enforcement with ForeScout and IBM BigFix

Compliance violations can be addressed and resolved with a combination of actions by CounterACT (isolation/quarantine) and BigFix (endpoint patch/configuration change).

The Bigger Truth

The unprecedented diversity of users, devices, and applications on networks—where employees, contractors, guests, and partners often use personal devices to connect to network resources—challenges businesses to efficiently provide them all with appropriate network access.

IBM BigFix delivers multiple management services for corporate managed systems, including real-time device status reporting, patch and software distribution, security policy enforcement, and response and remediation. IBM BigFix is an agent-based solution with a server and console component that provides a real-time view of device status. The BigFix server provides both a control center and a repository for managed system configuration data, software updates and patches, and other configuration and management information.

ESG Lab was quite impressed with ForeScout CounterACT's ability to empower organizations using IBM BigFix to efficiently provide visibility and control of endpoints accessing the corporate network, both internally and from the internet, to boost endpoint compliance, reduce risk, and improve network protection.

ForeScout CounterACT demonstrated that it can provide visibility, intelligence, and policy-based mitigation of security issues by providing real-time agentless discovery of managed and unmanaged devices while coordinating security controls and automating responses with IBM BigFix. If your organization is currently using or considering IBM BigFix for configuration management, it would be worth your time to look at how ForeScout CounterACT can work with IBM BigFix to improve visibility, increase endpoint compliance, and reduce vulnerabilities in devices both on- and off-premises, all while reducing management complexity.

All trademark names are property of their respective companies. Information contained in this publication has been obtained by sources The Enterprise Strategy Group (ESG) considers to be reliable but is not warranted by ESG. This publication may contain opinions of ESG, which are subject to change. This publication is copyrighted by The Enterprise Strategy Group, Inc. Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of The Enterprise Strategy Group, Inc., is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact ESG Client Relations at 508.482.0188.

The goal of ESG Lab reports is to educate IT professionals about data center technology products for companies of all types and sizes. ESG Lab reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objective is to go over some of the more valuable feature/functions of products, show how they can be used to solve real customer problems and identify any areas needing improvement. ESG Lab's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.