# DELIVERING AGILE SECURITY AT SCALE

**Problem:**

- Establishing and sustaining full cybersecurity situational awareness
- Centrally monitoring the security posture of every endpoint within their environment in near real-time
- Providing remote management, mitigation, and software deployment functionality supporting hundreds of remote IT staff

**Solution:**

- Our custom-built Web Console enables over 1,000 customer field Information Technology Support (ITS) staff to report on, manage, and deploy software to their assigned endpoints
- Utilizing the automated data feeds from BigFix, we automated the customer's ability to consolidate asset information, streamlining the monthly reporting requirement such as NIST compliance and RMF

## Customer Challenges

Our IC agency customer needed a way to establish and sustain full cybersecurity situational awareness of their global IT infrastructure dispersed across six continents and multiple enclaves to meet the FISMA mandate for Continuous Diagnostics and Mitigation (CDM). They needed a way to centrally monitor the security posture of every endpoint within their environment in near real-time, while simultaneously providing remote management, mitigation, and software deployment functionality supporting hundreds of remote IT staff.

## AI Solution Features

For over 8 years, AI has led the engineering, implementation, and ongoing operations of the enterprise endpoint management and continuous monitoring project for our customer, leveraging the IBM BigFix product suite as the core framework of our solution. AI provides real time situational awareness via continuous endpoint monitoring of tens of thousands of data points including file integrity, security posture and remediation of any host on the wire. This deep level of reach enables capabilities such as the detection of malicious files, identification of endpoints deviating from the standard baselines, quarantined confinement or selective/automatic remediation of infected assets, as well as a host of other non-security related essential capabilities. AI created an innovative custom

solution around the BigFix product suite, including the development of a customized Web Console that enables visibility and management of endpoints under their control wherever they are located. It was developed to be easy to use without formal training, and to operate in other customer environments supporting field operations. Our solution integrates with SPLUNK, SharePoint, HP (Microfocus) NNM/NA/Service Manager, SCCM, Active Directory and other proprietary enterprise software suites developed as operational needs expand.

## Benefits to the Customer Mission

Our solution provided remote real-time visibility and continuous monitoring for the customer's environment of over 150,000 endpoints across multiple security classifications globally.

- Our custom-built Web Console enables over 1,000 customer field Information Technology Support (ITS) staff to report on, manage, and deploy software to their assigned endpoints.
- Utilizing the automated data feeds from BigFix, we automated the customer's ability to consolidate asset information, streamlining the monthly reporting requirement such as NIST compliance and RMF.