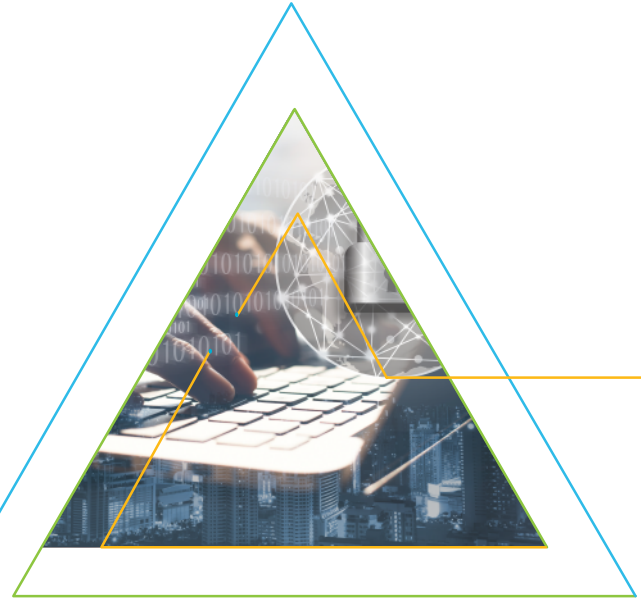# BigFix Insights

Accelerate risk discovery and business decision making

In order to manage and secure a widely distributed endpoint environment that is facing constantly evolving threats, an organization needs a very efficient approach to collect, track and report various endpoint properties across the organization. Reports need to enable executives to quickly identify risks and operational deficiencies so smart business decisions can be made. Reports must be easily customized and filtered so any specific endpoint postures or risks for focused areas or groups can be immediately revealed. Visibility across the entire endpoint environment is necessary, but also historical trends are essential to assess the effectiveness of remediation efforts.

BigFix® Insights enables IT teams to quickly report to executives an elevated picture of how endpoints are managed, patched, and secured to enable effective risk identification and business decision making. This new BigFix offering provides a powerful endpoint Data Lake and integration platform for deeper insights across traditional on-premise, cloud, and MDM-API managed endpoints, regardless of OS, location and connection type. BigFix Insights leverages Business Intelligence (BI) reporting tools to provide out of the box and customizable reports with trending, filtering and a rich set of visualizations, to render immediate value for the commonly concerned IT areas such as device inventory and patch posture. More insights to endpoints can be enabled by integrating the solution with additional business context or security data from other third-party solutions.

Highlights

- Import and consolidate data from all BigFix data sources into a single endpoint Data Lake and integration platform for optimal report generation.

- Leverage Business Intelligence (BI) reporting tools to provide out of the box and customizable reports with a rich set of visualization and filter capabilities, for common key areas such as device inventory, patch posture, OS migration, and deployment progress.

- Consolidated data available for an organization to use a BI tool of its own choice to generate additional reports to meet specific business needs.

- Provide deeper insights through integrations with other third-party solutions and enriched data sets that can include additional business context (e.g., business units, locations) or other endpoint security data (e.g., vulnerability) into the endpoint Data Lake and integration platform.

Accelerate risk identification and decision making

It is an increasingly challenging for organizations to manage a large number of devices spanning desktops, laptops, servers, mobile devices, kiosks, etc. running different operating systems, located on premise, in the cloud, or roaming in the Internet. To effectively manage such a complex environment while protecting all endpoints from constantly evolving threats, an organization must to be able to continuously track the current states of all endpoints, analyze and report the critical data, to quickly identify risks and operational deficiencies and then target those gaps for remediation.

BigFix is a powerful endpoint management solution widely used by organizations of various sizes to ensure endpoints are continuously patched, compliant and secure. For each endpoint, BigFix is able to collect a wealth of data including device attributes, patch statuses, deployment statuses, etc. which is collected and stored centrally. BigFix Insights is the new BigFix platform for reporting, in that it uses an endpoint Data Lake to import and consolidate all data from various BigFix data sources and organizes the data in a manner that is optimized for report generation.

To provide business value out of the box, it leverages Business Intelligence (BI) reporting tools to extract the consolidated data and provide customizable reports with a rich set of visualization and filter capabilities, for common key areas such as device inventory, patch posture, OS migration, and deployment progress. Executives can use these reports as is or customize them based on the organization's specific needs to get an evaluated view of the endpoint posture and quickly discover any risks or operational deficiency that requires immediate attention. This new reporting approach significantly reduces the complexity and effort an organization needs to take to produce actionable and focused reporting for executives.

BigFix Insights is also the new BigFix platform for data integration. Data from all BigFix databases can be consolidated and correlated into a single endpoint Data Lake. Additional data from third-party solutions such as a CMDB or a vulnerability assessment tool can be ingested to the Data Lake to correlate with the BigFix data, to enable even richer reports and deeper endpoint insights.

Data Lake

BigFix Insights uses an endpoint Data Lake to collect and consolidate data from all BigFix data sources. Various endpoint data from all instances of BigFix Enterprise (BFE) databases that span multiple domains can be aggregated into in a single endpoint Data Lake. The endpoint Data Lake allows all BigFix managed data to be available for reporting or other integrations from one single data repository.
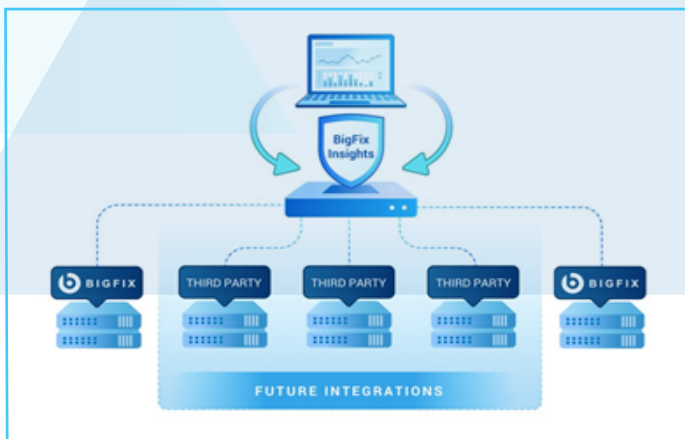
Add Data Lake management functions are performed through BigFix WebUI. With the help of a guided workflow, an administrator can easily set up the data sources to be imported to the

endpoint Data Lake. As BigFix manages all data using sites, an administrator can choose specific sites in each data source to import if not all data sites are desirable. Each data source import can be separately scheduled via a calendar-based approach to optimize server performance.

Out of Box Reports

To demonstrate the benefits of all data consolidated to a single data repository and provide business value out of the box, BigFix Insights leverages Tableau Software® to provide four reports for several important endpoint management areas that many organizations constantly focus on: Patch Rhythm, Device Inventory, OS Migration, and Deployment Progress. Each report contains high level and insightful data summaries grouped by different properties, displayed with a rich set of visualizations. The report can be easily filtered by clicking the shown properties. Each report also displays a historical trend of the data summary, enabling a quick glance of the progress over time and identifying risks or operational deficiency that may not be obvious without it.

The four reports can be used 'as is' or customized to fit an organization's specific needs to give executives an elevated picture of all the endpoints managed by BigFix. They also quickly expose to executives what risks are yet to be mitigated, so business decisions can be made effectively. Using a BI tool can significantly reduce the effort and time spent generating reports for executives.

Patch Rhythm report

The BigFix Insights Patch Rhythm report provides executives with an overview of the patch deploying statuses across all the endpoints. It shows how many unique patches are to be deployed, how many unique devices are missing patches, and an 'exposure' which is an aggregation of the patch and device statistics. It also summarizes the exposure data by different criteria such as severity, age, category and vendor, each of which can be used to filter the data to drill down to specific areas, such as all Microsoft security patches with a critical severity.
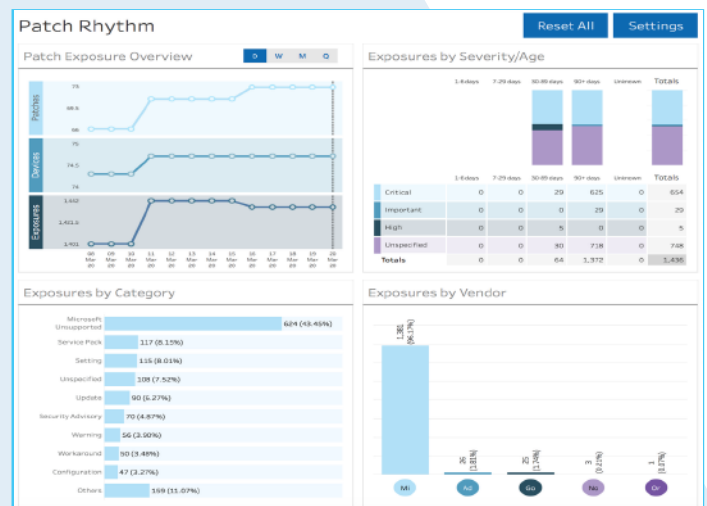

Device Inventory report

Identifying the exact number of devices across the entire environment continues to challenge organizations. The BigFix Insights Device Inventory report provides executives with an overview of device statistics, specifically showing the number of devices (by type) that are discovered and managed by BigFix over time. The report summarizes the device data by different criteria such as device type (including Cloud and MDM introduced in BigFix 10), last report time, device group, and OS version. These can each be used to filter the data to drill down to specific areas, such as Microsoft Windows 2016 servers that belong to the 'HR database' group.
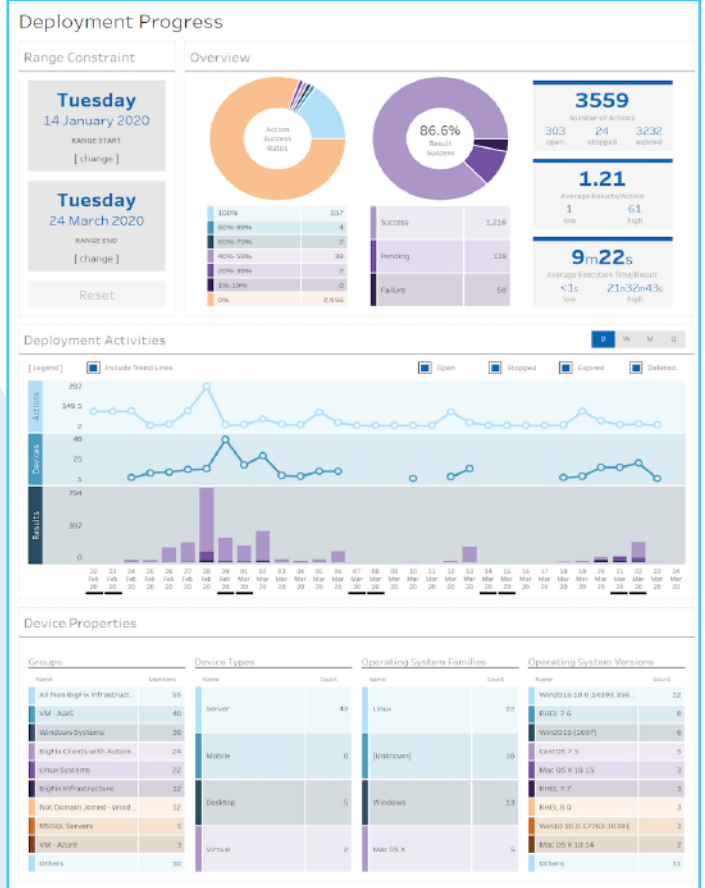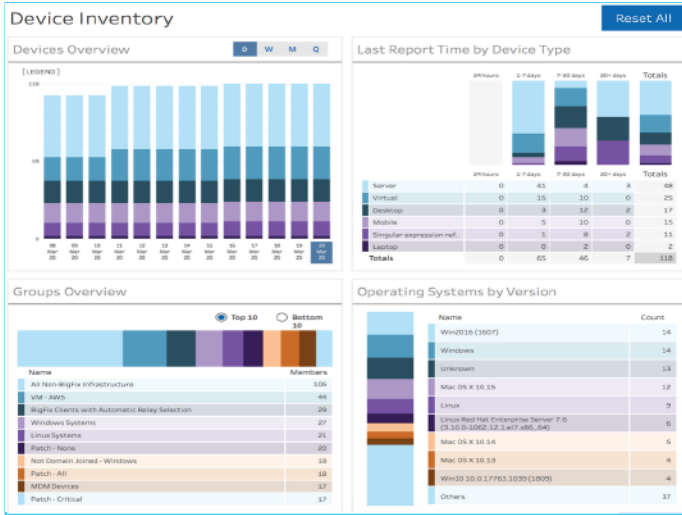
OS Migration report

The BigFix Insights OS Migration report provides executives with an overview of the migration statuses of the devices running unsupported OS versions, which introduce significant security risks as they are no longer updated or maintained by the vendor, to supported versions. Typically, an "OS family" like Windows or Linux is selected first to show how migration for all the endpoints within the same family is progressing over time. The report also summarizes the data by different criteria such as device type, vendor support status, device group, and specific OS version, each of which can be used to filter the data to drill down to specific areas, such as Microsoft Windows 7 devices that have not been migrated.
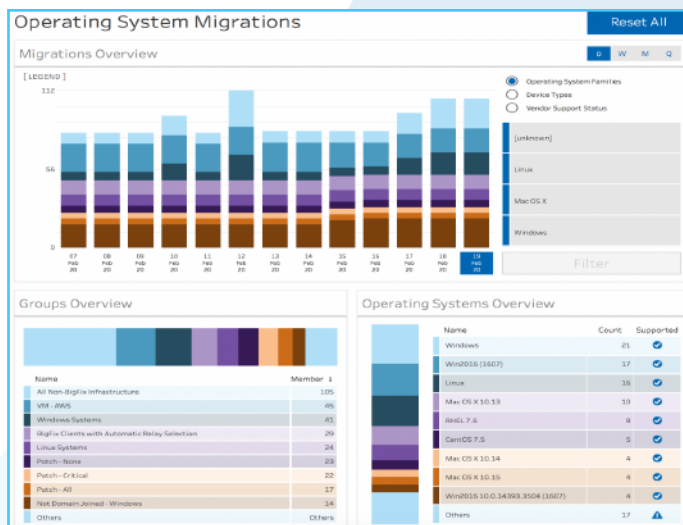
Deployment Progress report

The BigFix Insights Deployment Progress report provides executives with an overview of BigFix deployments so they can understand their effectiveness and remediate issues quickly. It shows how many actions were issued on the devices, over a configurable time period. It also renders some high level statitstics such as the success rates of actions in different percentiles and the overall average. All data is also summarized by different device properties such as device group, device type, OS family or version, each of which can be used to filter the data to drill down to specific areas, such as actions with a success rate below 80% what were deployed to all Windows devices within the past 30 days.

Generating additional reports

In addition to the 'out of the box' reports, an organization can leverage any Business Intelligence tool to extract the data from the endpoint Data Lake and generate other reports to meet their other business needs. The data schema of the endpoint Data Lake is open and fully documented to enable BI specialists to quickly understand the data structure so they can extract the data to the BI tool to generate reports. With this advanced reporting approach, an organization does not need to learn another reporting tool tied to a solution and can leverage its existing expertise and investment in the BI tool to incorporate BigFix endpoint data into its overall reporting portfolio of the organization.

Additional insights through integration

BigFix Insights also allows additional data from third-party solutions such as business unit or location data from a CMDB solution or vulnerability data from a vulnerability assessment tool to be ingested into the endpoint Data Lake to correlate with BigFix data. From this, additional reports can be generated to provide even more insights about all managed endpoints. Conversely, organizations can extract BigFix collected data from the endpoint Data Lake to enrich other solutions' data sets allowing organizations to integrate BigFix with other IT solutions to create greater efficiency and boost business value.

The BigFix family

You can further consolidate tools, reduce the number of endpoint agents, and lower your management costs by extending your investment in BigFix Compliance to include other modules in the BigFix family. Because all functions operate from the same console, management server and endpoint agent, adding more services is a simple matter of a license key change.

The BigFix family includes:

- **BigFix Compliance—** For continuously enforcement of endpoint c onfiguration compliance, BigFix Complince delivers thousands of out-of-the-box security checks aligned with industry-standard security benchmarks published by CIS, DISA STIG, USGCB and PCI-DSS. It provides an automated, simpli-fied, patch process that achieves greater than 98% first-pass patch success rates across Windows, UNIX, Linux, macOS, AWS, Azure, and VMware instances, located on and off the enterprise network. All automation and content streams are curated and tested, and once deployed, they are validated. BigFix Compliance also delivers advanced vulnerability posture reporting and remediation prioritization.

- **BigFix Lifecycle—**Enables IT and Security Operations teams can quickly discover, secure, and manage hundreds of thousands of endpoints within hours or minutes. BigFix Lifecycle delivers the core "must have" endpoint management capabilities. Lifecycle provides an automated, simplified, patch process that achieves greater than 98% first-pass patch success rates across Windows, UNIX, Linux, macOS, AWS, Azure, and VMware instances, located on and off the enterprise network. All automation and content streams are curated and tested, and once deployed, they are validated. BigFix Lifecycle also included OS provisioning, software deployment, remote control, task sequencing automation, and PC & Mac power management.

- **BigFix Inventory—**Enables users to discover and analyze applications installed on desktops, laptops, and servers. Drill-down information about software publishers, titles, and applications—down to the version level—also includes aggre-gated statistics and usage information. BigFix Inventory dramatically reduce the time required to conduct a comprehen-sive software asset inventory for license reconciliation or compliance purposes. It provides valuable insight into what the organization owns—and what it has installed but does not own—along with how often the software is being used.

- **BigFix Modern Client Management—**New with BigFix 10, BigFix Modern Client Management (MCM) helps organizations manage Windows 10 and macOS endpoints, where a BigFix Agent is not installed, by leveraging a Mobile Device Management Applica-tion Programming Interface (MDM API) approach. MCM support provides the ability to manage both modern and legacy endpoints using a single tool and capabilities such as end-us-er-initiated enrollment, detailed inventory of endpoints, and a number of MDM actions such as remote wipe.

Why BigFix?

BigFix is built on a unique, highly scalable infrastructure that distributes decision making out to the endpoints. This provides extraordinary functional and performance benefits across the entire BigFix family while reducing the cost of endpoint manage-ment and infrastructure complexity. BigFix features:

- **A single intelligent agent**—The BigFix Agent performs multiple functions, including continuous self-assessment and policy enforcement, with minimal impact on system performance. The BigFix Agent initiates actions in an intelligent manner, sending messages upstream to the central management server and pulling patches, configurations, or other information, to the endpoint in real-time. The BigFix Agent runs on more than 90 operating systems across Microsoft Windows, Linux, UNIX, and macOS.

- **BigFix Fixlets™**—BigFix Fixlets are small units of automation that allow IT Teams to simplify their daily operations and focus on more complex operations. BigFix provides more than 500,000 Fixlets out of the box. The BigFix team is continuously updating the Fixlet library, with over 130 content updates a month. BigFix users, business partners, and developers can leverage Fixlets to create custom policies and services for endpoints managed by BigFix. A community library of Fixlets is available on BigFix.me.

- **Highly scalable architecture**—A single BigFix Management Server can manage up to 250,000 physical and virtual computers, over private or public networks. Managed endpoints may include servers, desktops, roaming laptops, and specialized devices such as Point-Of-Sale (POS) devices, ATMs, and self-service kiosks.

- **Multicloud support**—Cloud endpoints can be easily discovered and viewed alongside traditional endpoints, in a single user interface, with BigFix 10. Knowing what you have is half the battle, and BigFix 10 allows you to go a step further and deploy the BigFix Agent for complete visibility, control, and security of these endpoints. It allows you to manage endpoints running in multiple cloud environments simultaneously – such as Amazon Web Services (AWS), Microsoft Azure, and VMWare – alongside physical and other on-premise endpoints.

HCL

For more information

To learn more about BigFix, contact your HCL Software representative, HCL Business Partner, or visit **www.BigFix.com.**

About HCL Software

HCL Software is a division of HCL Technologies that develops and delivers a next-generation portfolio of enterprise-grade software-based offerings with flexible consumption models, spanning traditional on-premises software, Software-as-a-Service (SaaS), and bundled managed services. We bring speed, insights and innovations (big and small) to create value for our customers. HCL Software solutions include DevOps, Security, Automation, Application Modernization, Data and Integration Infrastructure, and several Business Applications. HCL embraces the real-world complexity of multi-mode IT that ranges from mainframe to cloud and everything in between while focusing on customer success and building 'Relationships Beyond the Contract.'