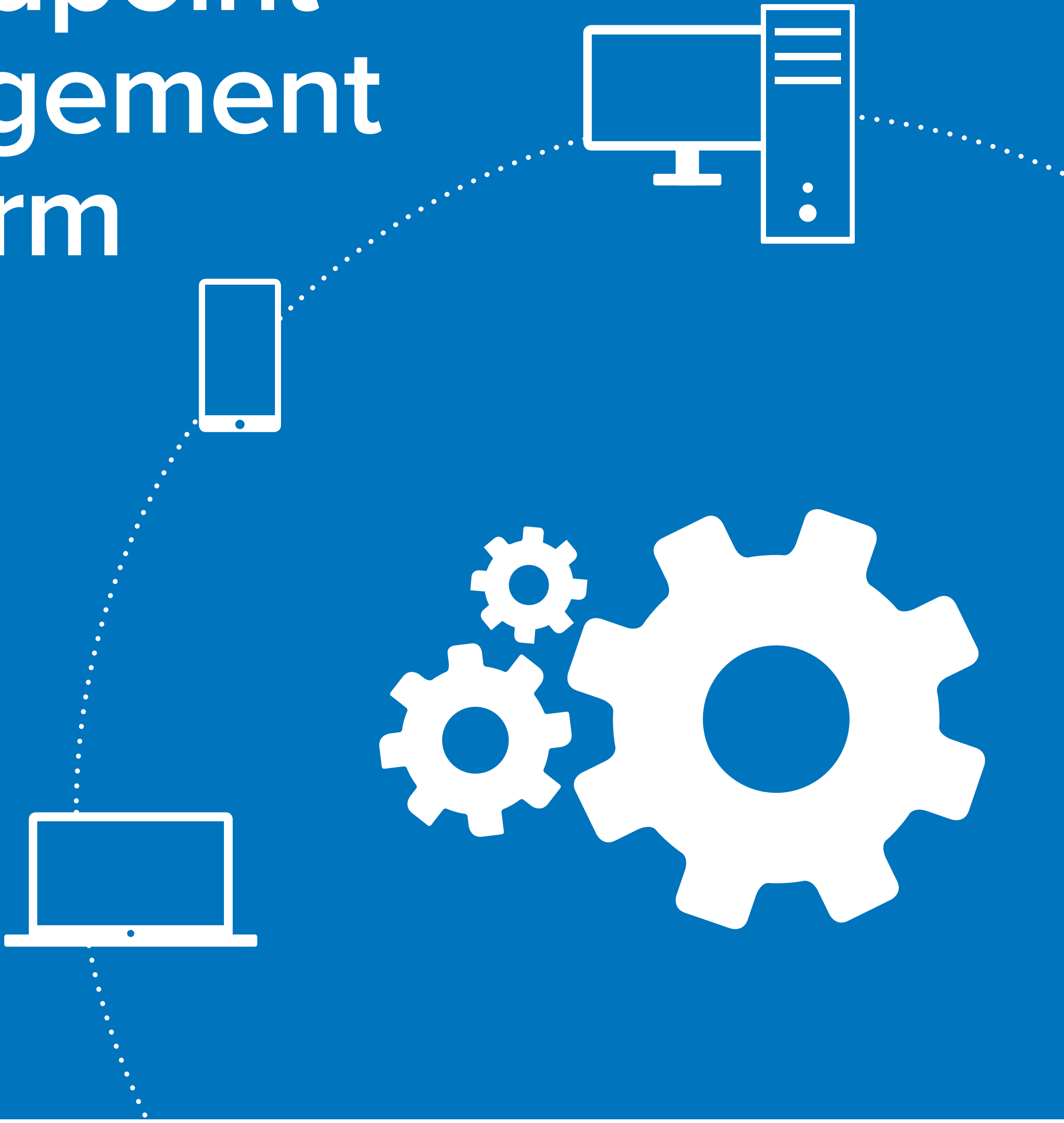
PeerPaper Report

Top Considerations for Choosing an Endpoint Management Platform

Based on Real User Reviews of BigFix



IT Central Station
Unbiased reviews from the tech community

CSO
FROM IDG

ABSTRACT

With serious cyber threats on the rise, enterprises are focusing more intensely on keeping Windows, Mac, Unix and Linux PCs, laptops and servers continuously compliant with patching security policies. Board members, supply chain partners and high-value clients are demanding it. To accomplish this goal, companies are turning to next-generation Endpoint Management Platforms (EMPs), also referred to as Client Management Tools. These platforms reduce the time between detection and remediation of configuration issues, regardless of OS, location or connectivity. What does it take to find the right EMP? IT Central Station members offer their suggestions based on customer experiences with HCL BigFix, emphasizing scalability, automation, role-based access control, high first-pass success rates and instant visibility into all endpoint configurations, regardless of OS and network status.

CONTENTS

INTRODUCTION

The inexorable rise of serious cyberthreats like WannaCry and Petya, which have brought business operations to a halt, has led to an intensified focus on more effective OS and 3rd party application patch management and keeping all endpoints continuously compliant with security controls. For the purpose of this paper, the term “endpoint” refers to any device that requires management, including servers, PCs and roaming, internet-facing laptops.

Today, supply chain partners now want to know if your systems—all of them—are compliant with patch management policies. To achieve desired levels of patch and security compliance, many organizations are faced with the need to deploy multiple tools for each of their operating systems and third-party applications. However, this approach significantly increases cost and complexity.

The need for a multi-platform Endpoint Management Platform (EMP) is clear and compelling for anyone who had held the responsibility for endpoint security. By consolidating tools, organizations can improve operational efficiencies and enforce consistent security policies across all endpoints. In so doing, they lower both operating and capital costs. With continuous patching and configuration compliance, they can mitigate the risk of attack vectors by minimizing the time when an endpoint drifts out of compliance and when remediation occurs.

What does it take to find the right EMP? IT Central Station members offer suggestions based on their experiences with BigFix. They emphasize automation, role-based access control and a high first-pass success rate for all tasks performed. SecOps managers also need to manage remote and disconnected endpoints, with ”near real time” visibility to compliance status of endpoints across the enterprise.

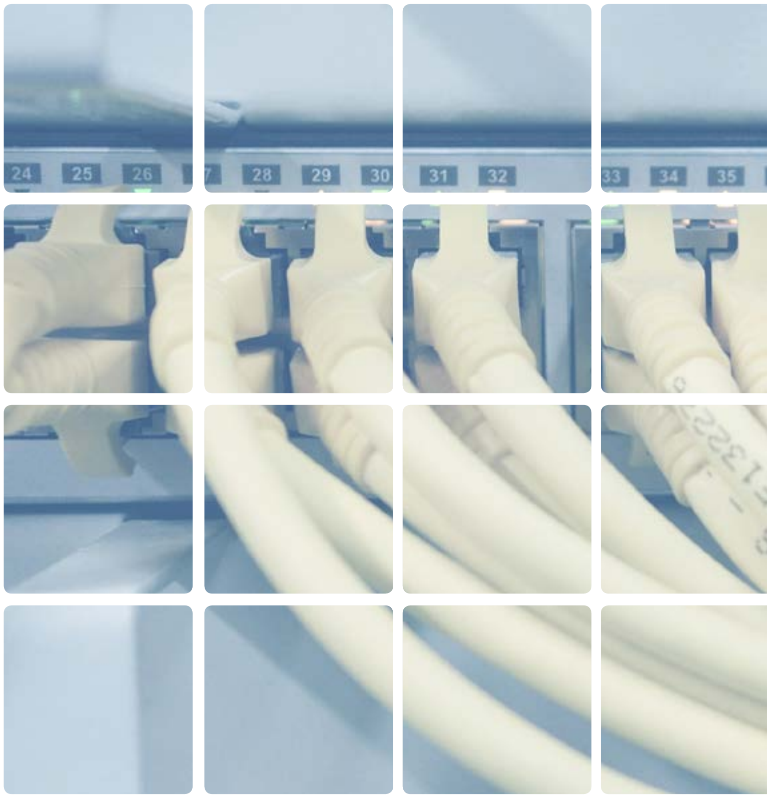
Overview:
The challenge of securing endpoints

The intensification and acceleration of cyber risk management has led to an overlap between cyber security and IT operations. While the security team may be responsible for threat detection and establishing security policies, IT Ops is responsible for implementing the vast majority of those policies. IT and SecOps must keep systems patched with the latest security updates for both OS and 3rd party applications. They have to keep anti-virus and anti-malware software up-to-date and running and provide visibility into installed hardware and software regardless of OS, location or connection type.

Endpoint Management Platforms help to address these challenges. Their functionality spans the installation of operating systems, middleware and applications; keeping OS and 3rd party applications patched; facilitating configuration compliance with regulatory or organizational security policies; and providing endpoint visibility, on and off the network.

Use case examples

Users of BigFix describe how it provides an automated, simplified patching process that is administered from a single console which provides real time visibility to endpoints and the ability to deploy and manage patches, software updates and configuration settings.



A Senior Consultant at a tech services company with over 10,000 employees, addressed the value of this kind of common user interface, saying, "BigFix console provides a single pane view into the entire environment. This also provides a common interface for taking actions, such as patching, to any operating system with a similar look and feel." A single patching solution that covers Windows, Linux, UNIX and MacOS simplifies training and operations as well as the IT management infrastructure.

In addition, to BigFix being an automated patching solution, reviewers on IT Central Station discuss how the platform facilitates four other significant use cases: configuration and regulatory compliance, security management, lifecycle management and inventory management.
IT Central Station members use BigFix for a variety of use cases related to configuration management. A Product Line Manager at a tech company with over 10,000 employees, for example, said, "Our primary use of this solution is for compliance management, patching and security configuration management."

Given the importance of endpoints in cyber security, it makes sense that users would apply BigFix to security operations tasks. A small company Founder/Director uses Big Fix for security compliance, for example. A Systems Analyst at a university with over 10,000 employees explained that his primary use for BigFix is "for patching all of our systems and maintaining their security compliance."

> “
>
> One of the biggest benefits BigFix has had for our organization is the ease and efficiency to perform many different tasks, across pillars and platforms, all from one pane of glass.

Regarding the lifecycle management use case, a Principle Consulting Architect described how he supports "multiple customers who use BigFix for many uses including for security compliance, list-deployment, remote control, software distribution, patching, etc." He noted, "One of the biggest benefits BigFix has had for our organization is the ease and efficiency to perform many different tasks, across pillars and platforms, all from one pane of glass."

According to a Rational Architect at a mid-sized tech services company, "Software distribution is another powerful and strong feature that automates deploying software and saves a ton of time." Software distribution, server automation and operating system deployment are additional capabilities of lifecycle management that lower the cost of endpoint management.

Lastly, BigFix reviewers describe how the platform can dramatically reduce the time required to conduct a comprehensive software asset inventory for license reconciliation or compliance purposes. A Systems Engineer at a large retailer remarked about the importance of speed, "Clearly, with Inventory Services, the speed is really key. In retail, we need answers very, very quickly. Other competitor products (which we do have in house) just don't compare."

The overall need for an enterprise-class, comprehensive platform

BigFix Users on IT Central Station emphasize the need for a powerful, enterprise configuration management platform capable of scaling to manage hundreds of thousands of endpoints and being able to support multiple update cycles per week. Deep, strong capabilities are required, including the ability to deploy agents rapidly. The Senior Consultant at the tech services company praised BigFix in this context by saying, “To deploy to one system will take about two minutes, but the tool is capable of parallel deployment, so deploying to 20 systems would take about five minutes. We were able to deploy about 400 Windows agents in a morning.”

A System Analysis staffer at a healthcare company with over 10,000 employees rated BigFix a “ten out of ten” because “it’s very useful, very powerful, and you can do a lot with it.”

“

I would rate it a ten out of ten. It’s very useful, very powerful, and you can do a lot with it.

Top considerations for choosing an Endpoint Platform

Users of EMPs have many needs, but as a group, they identify a number of considerations for choosing the right platform at the outset. These include a highly scalable architecture, support for many popular and legacy operating systems, support for low-speed network connections, automation of operational tasks, a high first-pass success rate for patching, real time visibility, endpoint lifecycle management, quick remediation of configuration issues and role-based access control.

Scalability

Scalability is key to being able to effectively manage thousands of endpoints, distributed across multiple sites worldwide. An enterprise-class EMP allows the IT department to easily scale to support business growth and agility. An Offering Manager at a tech services company validated this perspective, sharing, “Scalability is a place where BigFix really shines. One of the environments I worked on had over 250K endpoints on a single server.“

Several IT Central Station members commended BigFix on the ease of scaling to support large number of endpoints without performance issues. The Principle Consulting Architect said “I’ve built [implementations] with customers that are a couple thousand to a couple hundred thousand endpoints. I’ve also looked at other competing technologies out there, and it is definitely one of the leading tools on the marketplace in terms of the scalability performance.”

Mergers and Acquisitions (M&A) present immediate scalability challenges. A Technical Engineer at a company with more than 10,000 employees remarked about the scalability of BigFix and how it simplified the effort of bringing in new servers and workstations into management, safely and securely. He said, “It’s very scalable. We’ve had mergers that have come in and put a relay out there, and immediately get the information back for their clients.” New endpoints can be patched and brought into compliance before they are added to the enterprise network.

Support for current and legacy Operating Systems

Endpoints run many different Operating Systems (OS’s), including Windows, Mac, Linux, Solaris, HP UX, AIX and more. Endpoint security configuration tools should be able to support all these operating systems and the applications that run on them without needing unique hardware and software or dedicated IT/Sec Ops staff for each operating system platform.

Having a single server, single console platform that addressed multiple OS’s was the appeal of BigFix for an IT Operations Manager at a tech services company with over 10,000 employees. He uses BigFix for server management, patch management and software deployment on multiple platforms, such as Windows Servers, Linux and Unix. The Senior Consultant at the tech services company added, “BigFix supports [patching] most of the major OS’s with natively packaged patches. This includes Windows, MacOS, Oracle Linux, Solaris, AIX, RedHat, Ubuntu and others.” Along these lines, a Senior Security Consultant at a tech services company praised BigFix over a competitor that does not support MacOS or Linux.

A Senior Server Systems Engineer at a healthcare company with hundreds of employees related, “The most valuable feature would be its flexibility. It’s one product that works across multiple OS’s. We have one agent that will sit on six to seven different OS’s in our environment. I can use one console to push a patch to six or seven different OS’s in one view.”

> **“The most valuable feature would be its flexibility. It’s one product that works across multiple OS’s.**

BigFix reviewers note that the platform enables an organization to deploy a consistent security policy across all endpoints at a lower total cost compared to the cost and complexity of using multiple OS-centric management silos. An IT Engineer at a pharma/biotech company with over 1,000 employees spoke to this benefit, saying that with BigFix, “[our] servers are patched more consistently than they have been previously.” This issue is becoming more pronounced over time as technically skilled resources grow more expensive and difficult to recruit and hire. Training and then leveraging one skill set to keep all endpoints patched and compliant is the most effective way of lowering the total cost of endpoint management.

Support for low speed network connections

Managing endpoints can be challenging in places where bandwidth is limited or when people are on the move. Indeed, many network environments have limited bandwidth between certain geographic locations, between offices and home users using VPNs, etc. Deploying large patches (e.g., the 537 MB Windows 7 SP1 update) or Windows feature updates can easily overwhelm limited bandwidth connections and cause bandwidth problems for users or applications. To avoid such problems, EMP solutions should provide mechanisms to optimize bandwidth between various components.

In this vein, IT Central Station members expressed a need for their EMP to support low-speed network connections. For example, a BigFix Solution Manager at a large manufacturing corporation noted, “[BigFix’s] software deployment is fast and the product can be tuned for poor bandwidth networks.” Similarly, a Systems Administrator at a mid-sized tech services company remarked, “It [BigFix] has helped to reduce network traffic when it comes to downloading patches. It helps a lot because we have the ability to customize the uses of the bandwidth in our company, and it helps us to reach every region no matter the size of the link that we have in the network.”

> “
> **[BigFix’s] software deployment is fast and the product can be tuned for poor bandwidth networks.**

The Senior Security Consultant noted that BigFix is “incredibly powerful.” He added, “It’s very extensible. Meaning, it’s very easy for us to customize the platform to solve a number of different tasks for us.” He then added, “We enjoy using peer-to-peer file transfers as a peering system for files. It provides built-in redundancy and we can control it all from the console, which is nice.” In a peer-to-peer setup, endpoints in a subnet coordinate their download activities in order to download binaries only once, thus reducing the network traffic outside of the subnet, facilitating fast and direct exchange of binaries between endpoints, and eliminating dedicated relays from branch offices.

A Project Lead at a small tech services company summarized, “If you have a very high bandwidth in your network infrastructure, it will work very well. If it doesn’t have an internet connection, it also works very well. If you have a lower bandwidth within your offices, it will also work very well. This is lacking in many other tools.”

The ability to automate repeatable tasks

Manual processes impede IT operation’s ability to be effective and timely. EMPs should therefore enable as much automation as possible. As the biotech IT Engineer explained, “Our primary use case of this solution is for automated server patching. It integrates with our change management tool.” The Senior Consultant at the tech services company discussed the automation benefits for BigFix by saying, “We have also reduced the number of ‘manually’ patched servers as we have more flexibility for scheduling.” According to the Rational Architect, “The BigFix framework also gives you the ability to remove software and updates files, like configuration.”

BigFix provides prebuilt automation scripts but also enables users to create and re-use their own automation scripts and workflows. A Project Engineer at a tech services company with over 10,000 employees spoke to this capability, saying, “Customization as per the requirements is one of the best [features] it offers and almost any form of scripts and any OS can be supported for those customizations.”

The System Analysis staffer at the healthcare company used BigFix to speed up their Tivoli Workload Scheduler (TWS) deployments, saying “We’ve been able to fully automate our TWS installs, to the point where a user requests it and we don’t do anything.” This capability is enabled through BigFix's Software Distribution Self Service Portal which delivers fully-automated, user self-provisioning that eliminates the need for IT staff to get involved in satisfying common requests for pre-approved software.

Highest possible first-pass success rate lowers remediation effort and costs

SecOps managers like getting things done right the first time. Since patch remediation is very time consuming, it is important the EMP deliver a high "first-pass" success rate. The Senior Security Consultant at the tech services company put it like this: "We went from manually patching machines or doing our best and having very little visibility into it to us being able to 'set it and forget it' and getting really good results on first-pass patching."

The Principle Consulting Architect offered, "We've set up and started using BigFix to patch and have had much higher patch saturation rates than in the past. We do historical tracking with BigFix, and we can see that the success rate's gone way up."

He then noted an additional benefit of BigFix's consistently high first-pass success rate, saying "It has also helped to reduce help desk calls because of the success rate that we have with the patching. As the success rate goes up, we get fewer calls." The Technical Engineer agreed, "It has helped to reduce help desk calls by 60-70%. Using the self-service portal allows our users a lot of access to fix their own problems as far as errors, as well as policies that auto-resolve issues as they come up without the user even knowing."

The Offering Manager at the tech services company commented about the ease of creating and reliably deploying custom content with BigFix. She said, "Having built-in continuous delivery content was a major time saver and increased the first-pass success rate. Having the flexibility and freedom to deploy content custom-made for the environment is what enabled all use cases to be addressed."

Real time visibility

SecOps needs to know what's going on with its endpoints in real time. Endpoint Management Platforms should provide accurate information fast, preferably in real time or near real time, so problems can be fixed quickly and cost effectively. As the Technical Engineer framed the issue, "If you're considering BigFix look at the power that it allows you to have visibility into your system. If you don't have visibility into your systems, it takes a lot longer to get something resolved. Whereas if you can instantly get that information back from your client that's having a problem, being able to know that that issue needs to get fixed on that client's machine and being able to fix it instantly, could save you hundreds of hours."

> “
> **It has helped to reduce help desk calls by 60-70%.**

An Endpoint Management Engineer at a retailer with more than 1,000 employees commented, "Having higher visibility on patching level, on patching successful, and non-successful has been a way that BigFix has improved my organization." Further to emphasize the value of endpoint visibility, a Company Founder shared, "We rely on BigFix as part of our consulting engagements. It's more efficient from a visibility and discovery standpoint on the initial phase, the consulting engagement."

Real time visibility to new devices connecting on the network is also key to mitigating security risk and maintaining a secure environment. Periodic scanning for unmanaged devices is not enough. EPMs need to provide real time visibility.

> “The architecture for patching and the 100% correct reporting makes BigFix stand apart from other solutions.

They should automate discovery of unmanaged devices so they can be validated and have agents installed they can be brought into patch and security compliance. The Company Founder emphasized the point, saying, “With BigFix, the ability to do device discovery and the installation of our CyFIR agent across the environment is a very autonomous, automatic-type function that is a very significant feature for us.”

Endpoint lifecycle management

Endpoint configurations follow a lifecycle. The lifecycle starts with provisioning. It continues through regular updates and remote support and concludes with end-of-life decommissioning or re-imaging of the endpoint. Lifecycle management is an important capability in an EMP. An Information Security Analyst spoke to this need, saying, “BigFix has helped us in improving the overall endpoint posture and lifecycle management of the workstations as well as applications.”

Automated lifecycle management capabilities, including agent updates, appealed to BigFix reviewers on IT Central Station. As the Offering Manager explained, “Deploying the agent is really quick and easy. Migrations are less difficult [with BigFix] than competing solutions.”

Ability to quickly identify and remediate issues

When something goes wrong on an endpoint, SecOps staffers need to know quickly so they can remediate the issue. The ability to quickly identify and remediate vulnerabilities and non-compliant systems is a critical requirement when selecting an EMP. To this point, an Offering Manager praised BigFix for “configuration and vulnerability management of a complex and varied fleet of endpoints with a single pane of glass to see what is in the environment and a single agent to remediate all discovered issues.”

The Senior Consultant at the tech services company similarly noted that he was able to rapidly remediate a potential vulnerability. He said, “With BigFix, we were able to quickly identify out of compliance systems and remediate them and validate the successful completion of the installation.” For a Rational Architect, the value of BigFix came from knowing exactly what was happening with his endpoints. He said, “The architecture for patching and the 100% correct reporting makes BigFix stand apart from other solutions.”

Role-based access control

Controlling access of endpoint administrators is a critical aspect of security. Therefore, role-based access control is a best practice and key to any effective EMP. This functionality mattered to a BigFix Admin / Win SysAdmin at a retailer, who was pleased that “we’re able to single console manage all departmental Windows, Linux, AIX servers and from a single console, we can grant access via role base depending on department status and access. It’s just easy to get a big picture on a single screen.”

CONCLUSION

Enterprises today must enforce strong security management policies and practices to mitigate risks from cyber threats. Policies may be dictated by regulatory agencies and as well as by high value business partners and stakeholders. EPMs must manage a vast range of configuration settings, patches, software versions and updates—shortening the time between detection and remediation of all potential vulnerabilities. They need to include broad and deep visibility along with a comprehensive set of controls to effectively safeguard the enterprise. EMPs also need to provide real time visibility to endpoints and provide accurate inventory information to support IT and Security operations. Additional capabilities like OS provisioning and migration and automation of repetitive, operational tasks is also key to managing endpoints throughout their life span.

According to IT Central Station members, the best EPMs provide a high degree of automation, a high first-pass success rate when patching and the ability to continuously enforce compliance across heterogenous endpoints. Other preferred qualities include complete, real time visibility into endpoint configurations, role-based access management, fast remediation and lifecycle management. Effective endpoint management is a challenging job, but with the right platform, it is possible to maintain an effective and robust security across endpoints regardless of OS, location or connection.

ABOUT IT CENTRAL STATION

User reviews, candid discussions, and more for enterprise technology professionals.

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. However, in the world of enterprise technology, most of the information online and in your inbox comes from vendors when what you really want is objective information from other users. IT Central Station provides technology professionals with a community platform to share information about enterprise solutions.

IT Central Station is committed to offering user-contributed information that is valuable, objective and relevant. We validate all reviewers with a triple authentication process, and protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

www.itcentralstation.com

IT Central Station does not endorse or recommend any products or services. The views and opinions of reviewers quoted in this document, IT Central Station websites, and IT Central Station materials do not reflect the opinions of IT Central Station.

ABOUT HCL BIGFIX

BigFix is the world leader in endpoint management solutions. Leveraging a single management platform, BigFix enables organizations to keep all endpoints continuously patched and compliant, regardless of operating system and network status.

Founded in 1997, BigFix was acquired by IBM in 2010. HCL assumed responsibility for development in 2017 and acquired BigFix from IBM in 2019. BigFix is a product of HCL Software, a division of HCL Technologies.

www.bigfix.com