LEVERAGING BIGFIX
IN OPERATIONAL TECHNOLOGY ENVIRONMENTS

In the rapidly evolving Operational Technology (OT) landscape, the need for robust, adaptable, and secure solutions for software updates and patch management is only increasing. This whitepaper provides a comparative analysis between BigFix and Windows Server Update Services (WSUS), two widely used tools for managing software updates. Real-world scenarios and expert input point to BigFix as the superior choice for complex OT settings.

Interstates has been working with enterprise organizations for many years assisting with designing, implementing, maintaining, and securing their OT environments. One area of discipline is Endpoint Security where our team focuses on proactive measures to keep operational machines safe from cyber exploits.

Today's OT environments are complex, involving various systems and endpoints crucial to industrial operations. This complexity becomes challenging when you are faced with cybersecurity threats that demand rapid response. Patch management is a cornerstone of a well-rounded security solution, especially in IT/OT environments where the stakes are high. Timely software updates are not merely a task to check off your list but a strategic necessity. They serve as the first line of defense against vulnerabilities that could compromise system integrity, disrupt operations, and put safety at risk.

BigFix vs. WSUS: A Comparative Analysis

While BigFix and WSUS are tools that have some overlapping capabilities, their differences make one more suitable than the other in certain situations. Consider this analysis of their benefits and limitations:

vs. Windows

1. BREADTH OF OPERATING SYSTEMS SUPPORTED

BigFix offers support critical to OT environments that frequently require a mix of different operating systems. BigFix supports a wide range of Windows, Mac, Linux, and Unix operating systems, and even the VMware ESXi hypervisor and mobile platforms like Android and iOS.

WSUS is restricted to Microsoft environments, limiting its applicability in OT settings that often involve diverse non-windows operating systems. WSUS is capable of patching Windows based workstations and servers but cannot help with other operating systems.

2. TIMELY MONITORING AND REMEDIATION

BigFix offers "near-time" monitoring and the capability for rapid remediation actions, a vital feature where any downtime or security breach can have severe consequences. The BigFix agent is configured to check in at specified intervals, and it can be remotely triggered to "wake up" and query the server for new actions. These features allow for something close to real-time data, which we call "near-time" monitoring. The status of your endpoints is known continuously, and the impact and results of globally distributed remediation actions are reported quickly. In an emergency you can deploy a patch and see results from around the globe within minutes.

WSUS relies on group policies and Active Directory communications which primarily occur at system logon. Windows Update is configured to check in once every 22 hours by default, and typically relies on Background Intelligent Transfer System (BITS) for file movements across the network. That protocol is designed for operations during periods of inactivity. WSUS offers priority and deadlines for distributing content, but to trigger a machine to update, check in, and query for actions or to download new content requires manual intervention outside the WSUS platform. These features were designed to keep WSUS quiet and avoid network disruption, but they unfortunately hamper the ability to respond to urgent issues.

3. CUSTOMIZABLE REMEDIATION CONTENT

BigFix provides the ability to create custom content as a standout feature. It allows for targeted updates, ensuring that critical systems receive the necessary patches without affecting other functionalities. Interstates uses these features to deliver patches for custom applications, or to deliver only tested and approved Microsoft OS patches based on the software inventory of the endpoint.

You can patch or replace vulnerable files or sub-components of applications. The capability to build a script, deliver an executable, or instruct the endpoint to query, download, and take specified actions brings features not available on other platforms.

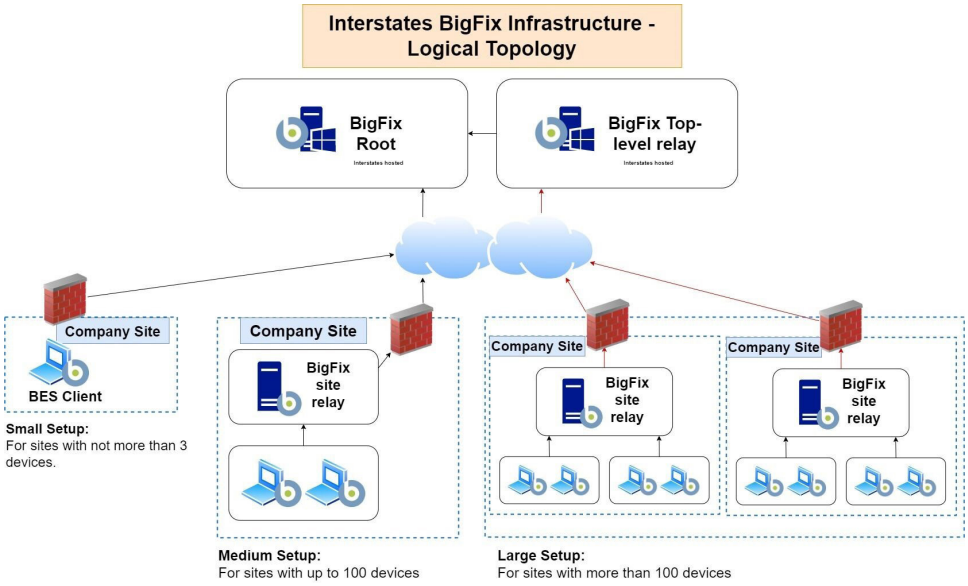
Capability	BigFix	WSUS
Asset Discovery	X	
Microsoft OS Support	X	X
Microsoft Application Support	X	X
Multiple Platform Support	X	
Multi-Cloud Patch Management	X	
Off-line VM Guest Patching	X	
3rd Party Application Patching Content	X	
Security Analytics Reports	X	
Endpoint Inspection (Query)	X	
Software Distribution (self-service)	X	
Task automation	X	
Bare metal OS Deployment	X	
Remote Desktop Control	X	
PC/Mac Energy Management	X	
Compliance Enforcement (PCI, DISA-STIG)	X	
Multi-vendor anti-malware management	X	
Software Inventory	X	
Hardware Inventory	X	
Remote wipe / lock for laptops / mobile devices	X	
Automated custom content distribution	X	
Near time reporting	X	

Comparing features available on Big Fix compared to WSUS

WSUS is designed to deliver Microsoft patch content for Microsoft applications. It was not designed to have the flexibility nor the capability to deploy other content nor perform scripted actions on endpoints. WSUS does not allow for customized patching, which results in the need to develop additional processes to update vulnerabilities for non-Microsoft content. For large deployments, customers might use Microsoft's Systems Center Configuration Manager (SCCM) in addition to WSUS to add some of these capabilities. The OT space relies on many software applications that are not from Microsoft, which means that WSUS can be a limitation in complex OT environments.

4. SCALABILITY

BigFix is known for its scalability and can efficiently manage tens, to hundreds, to thousands of endpoints across a single site, multiple sites, and even the distributed infrastructure required by global organizations, a common scenario in industrial OT. The tool is uniquely suited to the OT environment based on a relay architecture. A relay allows us to limit any ingress or egress from the protected Industrial Control Systems / Manufacturing Control Systems (ICS / MCS) network to a single specified machine, which also serves as a cache for content and centralized data gathering point. This design fits extremely well with the desire in OT to prevent critical endpoints from being exposed to the public internet.



Example of BigFix network architecture

WSUS is primarily designed for small deployments. Customers using WSUS in larger deployments almost always add SCCM or other Microsoft tools to bring the enterprise features required in their organizations. While it can function on many machines in a flat IT environment, WSUS faces many challenges in managing large-scale OT environments. The varied landscape requires significant administrative effort to group and maintain your systems and control the distribution of wanted versus unwanted content. Controlling the time of delivery, or when the deployments must be complete, is difficult and requires substantial time and effort. WSUS allows you to utilize replica servers and branch office servers, which allow some caching capability, but lacks the precision of control needed in the manufacturing space to reliably predict downtime and meet schedules for return to production operations.

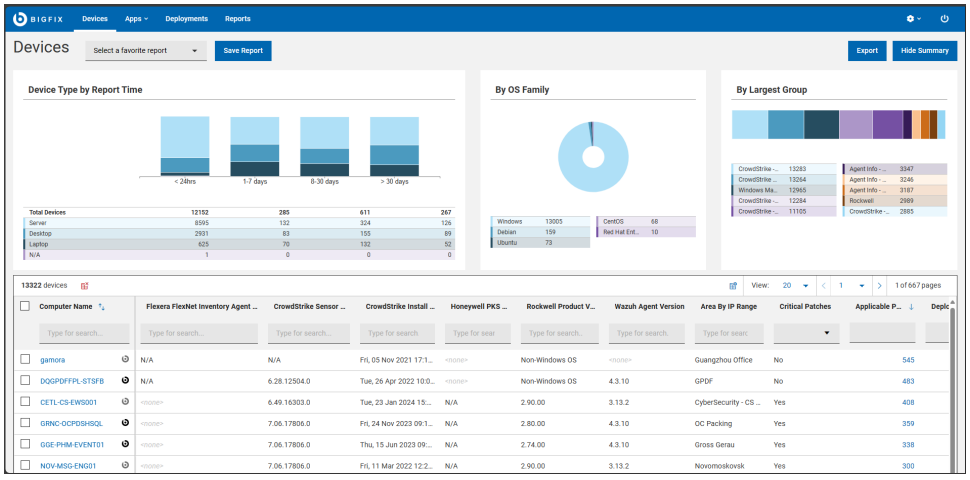
5. BANDWIDTH OPTIMIZATION

BigFix includes bandwidth optimization features, essential for OT environments where network resources are often limited. You can define exactly how much bandwidth to allow for any action. The relays also serve as a cache location for content intended to be distributed inside the OT network. Again, the relay architecture allows an administrator to control all inbound and outbound traffic while keeping Wide Area Network (WAN) traffic minimized. All traffic is on a single port to specified locations. You can distribute actions over a specified period of time to prevent network saturation, and you can designate exactly when a client will wake up, process patch content, and when that activity will stop. This control is critical in manufacturing operations.

WSUS is designed to use BITS, but otherwise offers limited bandwidth optimization features. Enabling the network load balancing requires the addition of a SQL server, adding expense and complexity. This feature also requires all WSUS replica and branch office servers to be at the same OS and cumulative update level. When you distribute content, you are relying on the hierarchy built on the WSUS server for priority, which could lead to unexpected outcomes and network congestion during critical operations.

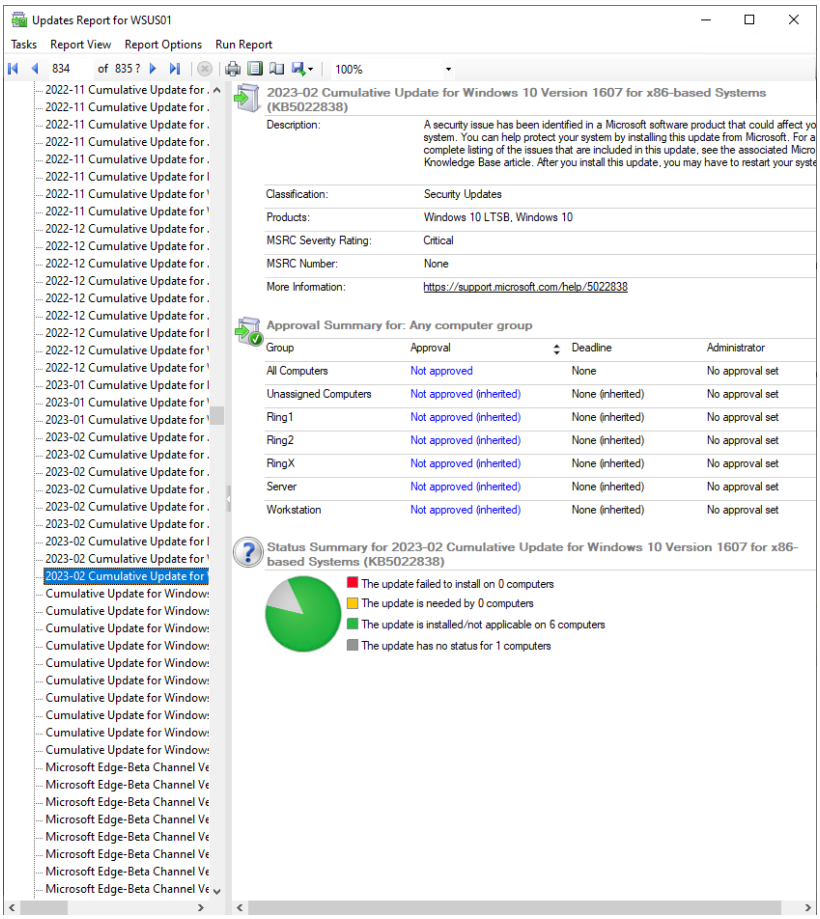
6. COMPREHENSIVE REPORTING

BigFix offers robust reporting and analytics capabilities to provide administrators with a panoramic view of the system status, compliance levels, and vulnerability assessments. BigFix offers tools to scan the network and discover other devices like printers, switches, even PLCs (programmable logic controllers) to gather details like IP addresses and serial numbers which provide significant additional reporting value. WebReports brings the ability to build custom interactive reporting pages. Our analytics teams have learned the BigFix database schema and have built many custom client-centric reports using PowerBI and other visualization and analytical tools based on the “near-time” data available.



Example of a BigFix reporting dashboard

WSUS is limited in this aspect, offering basic reporting features limited to the WSUS results on the Microsoft products you’ve added to the catalog. This may not meet the requirements of complex OT systems. There is no endpoint agent gathering data for hardware or software analysis. There is no way to get a broad understanding of your security posture nor accurate up-to-date visibility. Lacks the ability to collect hardware or software inventory, missing key details like BIOS and firmware information. There is no way to query other devices around the network. Reporting is focused on Microsoft patches for Microsoft products.



Example of a WSUS reporting dashboard
Reference: https://bit.ly/3SSaAL9

7. SECURITY FEATURES

BigFix is equipped with advanced security features like role-based access control, 384-bit encryption, and secure communications to protect sensitive OT data. It allows for industry standard Lightweight Directory Access Protocol (LDAP) integration for authentication. All communication is on a single port on specified protocols which allows for very tight firewall and network traffic control. The console has the capability to implement "four-eyes" authentication requiring multiple operators to issue and then approve actions on designated endpoints.

WSUS uses Active Directory authentication and allows for the groups and permissions features included. However, it lacks advanced security measures, making it less ideal for protecting complex OT systems. This could result in distribution of unwanted content and potential safety issues if the wrong systems were to be brought down unexpectedly.

8. UNIFIED ENDPOINT MANAGEMENT

BigFix goes beyond patch management to offer a unified endpoint management solution. It consolidates various tasks such as software distribution, security configuration management, and asset inventory into a single platform. The ability to see your physical, virtual, and even your mobile assets and their security exposure provides a complete view of your endpoint environment. Providing operating system patches is just one of the many endpoint management capabilities.

WSUS is limited to Microsoft operating systems and specified Microsoft application patch management. The tool does not have the capability to manage other operating systems or devices. It requires additional tools like SCCM for any inventory management capabilities. WSUS offers less comprehensive endpoint management.

9. INTEGRATION CAPABILITIES

BigFix is designed for seamless integration with other security tools and IT management solutions, which enhances the opportunity to improve the overall security posture of the entire organization. Partnerships with multiple large vendors like ServiceNOW, Tenable, Qualys, VMware, etc. bring many added capabilities and data analytics as well as the potential for visibility into both the IT and OT devices in your environment. You can ingest from and feed data to multiple other tools.

WSUS is designed to allow integration with other Microsoft tools like SCCM. It's limited in terms of integration capabilities with external vendors, which could result in a more fragmented security approach. WSUS is designed to deploy Microsoft patches to Microsoft devices.

10. SUPPORT

BigFix provides strong vendor support as well as an active user community continuously developing and sharing new features. This provides a dynamic support ecosystem. End users and developers answer questions to support each other and assist with creating custom solutions. BigFix User Group meetings are held as live events in major cities around the world with support from the vendor and partners. When a new exploit is announced there is usually a collaboration between the software developers and user communities to create new analysis and deployment content. This allows customers to begin testing quickly and have predictable outcomes.

WSUS support from Microsoft for the free tool may not be as comprehensive or dynamic, which could be a limiting factor for complex OT settings. Microsoft products have a strong online user community, but there is less detailed participation or engagement in those forums. Users just don't have as much flexibility to develop or share customized solutions and content. The community is not working to discover new capabilities or features or to develop solutions for new exploits as they are released.

Recommendations

For organizations with complex OT environments, BigFix offers a comprehensive framework that not only enhances security but also improves operational efficiency. The robust features and adaptability make it a smart choice for effectively managing all the OS, software updates, and other patching described above. It provides hardware and software inventory and then allows you to automate grouping or actions based on the content of your endpoints. It's a great tool for vulnerability remediation and automating server lifecycle management. The design fits in to the OT network architecture extremely well and the security features allow you to keep the environment safe from unwanted actions.

Some OT customers believe that because WSUS is agentless, it is a preferable solution over the BigFix agent-based solution. It can be true that installing additional software can have unintended consequences, especially in older OT environments with legacy systems operating at or near capacity for processor, memory, network, or disk. However, over decades of experience, the BigFix agent has proven to be stable, reliable, and non-disruptive. We see BigFix running on 25-year-old hardware performing high-speed precision manufacturing operations in the real world. Having the agent in place provides substantial and meaningful insight and benefit with very minimal risk.

You should carefully evaluate the specific requirements and constraints of your OT environment before making a choice between BigFix and WSUS. Generally, the only facilities where WSUS will win out are those with a predominantly Windows OS environment, a relatively simple, small deployment, or where there are significant budget constraints.

Implementing BigFix

Here are a few recommendations for implementing BigFix in your environment:

- Plan your deployment architecture for efficient relay and network communications to ensure you take advantage of the capabilities and control the flow of data
- Think about how you want to organize your administrative console groups for both users and computers as this will impact future patching automation capability as well as reporting operations
- Consider a phased approach to implementation, rolling out in stages allows you to adapt to the site-specific environments that you encounter
- Once you are comfortable using BigFix, leverage the tool's customization and real-time monitoring capabilities to enhance security and operational efficiency at your plant

In conclusion, BigFix offers a superior, flexible, and secure solution for patch management in OT environments. The critical advantage of BigFix is its ability to adapt to any OT environment and provide targeted, effective solutions for various challenges, from security to operation uptime. Its range of features—from cross-platform support and unified endpoint management to near-time monitoring and advanced security options—make it a compelling choice over WSUS for industrial OT operators and owners.

The Interstates Endpoint Security Team delivers a focused offering that provides comprehensive endpoint management for clients seeking better control over their OT environment. Our solutions for patch management, software distribution, inventory, vulnerability remediation and incident response keep our customers' machines safe, secure, and available for production without any unplanned downtime. Leveraging our partnerships with controls software vendors like Rockwell, Honeywell, Aveva Wonderware, and Siemens, we deliver vendor-qualified patch solutions from trained experts knowledgeable in OT environments.

AVEVA Honeywell

Rockwell Automation SIEMENS

Other Interstates teams focus on areas such as networking, virtualization, backup and recovery, server support, automation, HMI and PLC programming, data analytics, electrical engineering, and much more. This vast array of in-house manufacturing knowledge and expertise provides an exceptional and valuable support network for our Endpoint Security service and support team. The flexibility of our organization allows for cross-team training and custom solution development spanning multiple disciplines.

If you're interested in learning what Interstates can do for you, please visit our website www.interstates.com.

About the Author

Tom Dietrich is an OT Architect at Interstates. He has been working in Operational Technology for over 25 years and holds certifications from vendors like Microsoft, VMware, Intel, IBM, and HP in their cloud systems, administration tools, networking, virtualization, server, and endpoint security products. Reach him at tom.dietrich@interstates.com, or visit www.interstates.com for more information.