Solution Showcase

HCL BigFix

Seven Must-have Endpoint Management Capabilities

Date: September 2019 **Author:** Dave Gruber, Senior ESG Analyst

Abstract:

- When endpoint management systems are effectively integrated with security and IT operations tools, they play a major role in proving compliance, stopping threats, consolidating tools, and protecting brands.
- Since most cyber-attacks leverage known vulnerabilities, IT operations and security organizations need to collaborate to quickly address security risks that threaten the organization.
- Patch management, security configuration and compliance, software distribution, and inventory are core IT infrastructure capabilities that need to interoperate with the rest of the IT operations and security toolset. Organizations that want to tighten security should consider BigFix for its rich endpoint management capabilities and the ability to easily integrate with other IT and security tools, helping IT operations and security teams to collaborate more effectively.

Overview

Endpoints represent the operational engine that enables the modern knowledge worker to perform. Disruption to these systems impacts both individual productivity and the collaboration of teams, slowing overall business operations. A leading cause of systems disruption today comes from security-related attacks, which affect wholesale system function, and result in degradation in operational performance.

Modern attacks often leverage known vulnerabilities in software for which patches and remediation actions already exist. Misconfigured systems also provide a means of attack. Organizations can prevent cyber-attacks and costly data breaches by keeping current with operating system and application patches together with implementing configuration management to enforce compliance with standard security guidelines. IT teams therefore need a continuous, precise inventory of all endpoints, software, and configuration details across their environment. Using this inventory, IT teams can ensure these systems are: kept current with the latest OS and application patches; license- and regulatory-compliant; and securely configured.

Since security teams are typically responsible for the detection of vulnerabilities while IT operations teams are responsible for remediation, effective collaboration between these teams is imperative for business continuity. A properly implemented endpoint management system (EMS) can provide a collaborative platform for both IT operations and security

that enhances the overall security posture. To accomplish this, these solutions must be comprehensive, nimble, and integrated with IT and security infrastructure. They must enable rapid, consistent remediation of threats across all endpoints while continuously verifying that all endpoints are patched and compliant.

This paper will explore the challenges associated with endpoint management, the key capabilities needed, and a recommended solution.

Challenges

Perimeter defenses are no longer enough; endpoints themselves are now part of the attack surface. With a **continuously growing attack surface**—including new types of endpoints, servers, devices, and applications—**IT teams are struggling to keep up with configuration, patching, and compliance management**. This issue increases the risk of compromise due to exposed vulnerabilities in unpatched and misconfigured systems. Timely patching is critical to stay ahead of attackers. Without an effective endpoint management strategy and process, organizations will fail to secure their environment.

As security teams increase their use of threat detection and response tools, **the amount of work required to remediate identified threats overwhelms many IT organizations**. For example, when CVEs are released, security teams first need to assess the level of risk by identifying how many systems are impacted and prioritizing remediation actions based upon the severity of the vulnerability or threat. Threat remediation is "unplanned" work for most IT teams, often creating a growing backlog of unfinished IT expansion projects due to the distraction created by threat remediation. The question of "How do we fix what we find?" is all too common today.

Roaming endpoints and cloud-based endpoints are not seen by many endpoint management systems, creating a growing management challenge. While mobile device management solutions provide some needed capabilities, few have the scalability required to effectively manage endpoints, regardless of which operating system they are running, where they are located, or how they are connected.

Ensuring that security tools are installed, current, and active is critical to securing the infrastructure. However, continuous monitoring and automated remediation of rogue systems is challenging, especially with today's highly mobile workforce.

Compliance management requires visibility into endpoint configuration and software inventory. With the growing diversity in endpoints, this level of consolidated visibility is challenging at best.

> IT teams are struggling to keep up with configuration, patching, and compliance management.

Timely patching of security and configuration vulnerabilities can be the difference between a compromised system and an uncompromised one. When security tools identify issues, integration with EMS tools becomes critical to rapidly prioritize and remediate vulnerabilities. Yet few organizations have integrated these tools, leading to slower remediation times.

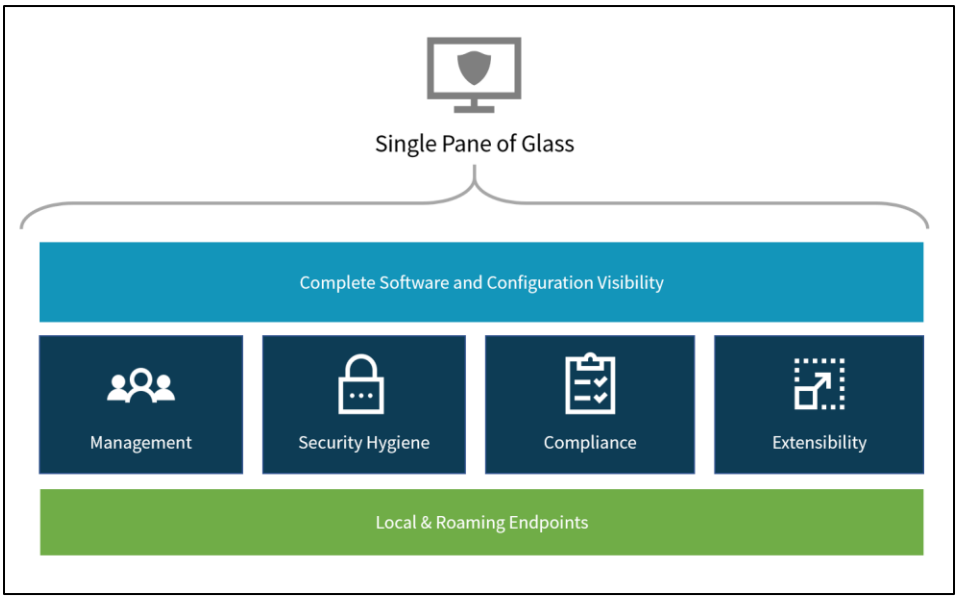
Supply chain vendors are progressively asking for **verification that systems and software are compliant with specific industry regulations**. Compliance is all too often thought of as an event. Organizations would be better served to verify compliance on an ongoing and continuous basis.

Reporting compliance verification to senior management and auditors can be challenging without continuous monitoring tools. Besides tracking, analyzing, and reporting on the current status of patching activities across all endpoints, IT organizations need to track compliance history as an overall percentage—a meaningful metric to gauge the progress of compliance efforts over time.

What's Needed

These **seven endpoint management capabilities** help operations and security teams to gain needed visibility, stop threats, and prove compliance, all while consolidating tools:

1. **Comprehensive visibility.**
   - Rapid, continuous endpoint discovery and precise software and configuration inventory.
   - Easy-to-visualize reporting with historical trending (compliance, inventory, and deviation).
   - Drift detection and alerting.
2. **Ease of management.**
   - Reliable, consistent software distribution.
   - Fast, reliable patching, with high first-pass success rates.
   - Configuration updates and verification.
   - Automated software provisioning.
3. **Continuous security hygiene.**
   - Continuous monitoring and patching.
   - Configuration drift detection and remediation.
   - Enforcement of security policies.



4. **Continuous compliance.**
   - Continuous monitoring and verification of software and configuration against policy and regulations.
   - Enforcement of regulatory policies.
5. **Roaming endpoint management.**
   - Precise configuration control of remote endpoints.
6. **Extensibility and integration with existing infrastructure.**
   - Out-of-the-box integrations with security tools, including endpoint protection platform (EPP) and security information and event management (SIEM) tools.
   - APIs that expose all aspects of endpoint management to drive automation.
7. **A single pane of glass across the endpoint fleet.**
   - Common view of all system assets, regardless of operating system, location, or connection type.

HCL BigFix: A Collaborative Endpoint Management and Security Platform

HCL BigFix is a full-feature endpoint management and security system currently deployed on and managing over 100M endpoints worldwide. It provides a turnkey approach to asset discovery, software distribution, and OS provisioning, leading to secure and compliant systems, regardless of operating system, location, or connectivity.

Discover assets rapidly (hardware and software inventory, software license and usage, and compliance reporting).

- Rapidly inventory endpoints across multiple operating systems, identifying all endpoints while providing accurate and current information about the installed software, software usage, and configuration.
- Gain near-real time visibility into endpoint information from an individual device or from groups of endpoints using BigFix Query.
- Identify unmanaged endpoints including potentially rouge devices connected to the network.

Manage easily (software patching, distribution, and provisioning).

- Quickly deploy and patch operating systems and third-party software with high first-pass success rates.
- Reduce annual software spend by assessing application usage and licensing.
- Manage secure configuration across all endpoints, including roaming remote systems.
- Share a common view of all hardware and software assets with both IT and security teams.

"BigFix is like an aircraft carrier. It is central to our solution and is the platform that we have built upon to rapidly deliver value to our customers. We chose BigFix because of its flexibility and its ability to easily integrate with all aspects of our solution."
John Livingston, CEO, Verve Industrial Protection

Secure continuously (continuous monitoring and patching, enforcement of security policies, and proper configuration).

- Continuously monitor, patch, and enforce security policies across all endpoints, regardless of operating system, location, or connection type.
- Keep cloud-based endpoints, remote servers, and roaming (internet-facing) endpoints updated, secure, and always properly configured.

Enforce compliance in real time.

- Improve compliance reporting by providing out-of-the-box support for security benchmarks published by CIS, DISA, STIG, USGCB, and PCI-DSS.
- Enable endpoint compliance across Windows, UNIX, Linux, and Macintosh operating systems.
- Continuously monitor and enforce endpoint security configurations to ensure compliance with regulatory or organizational security policies.

Manage remote endpoints.

- Get full visibility of your servers, desktops, and laptops, regardless of location, connection, type, or status.
- Manage and patch both on-prem and internet-facing endpoints.
- Discover unmanaged assets to quickly bring them under management.

Integrate seamlessly.

- Integrate with endpoint detection and response (EDR) tools to help security teams better identify threats and operations teams remediate endpoints at scale.

- Integrate with network access control software (VPN clients, firewalls, etc.) to quarantine endpoints and enforce compliance.
- Enable SOC teams to see endpoint data within their existing security information and event management (SIEM) and incident response tools. Accelerate and improve incident response through discovery, enrichment, and automated response.
- Use a rich set of APIs to customize and automate endpoint management activities.

"BigFix is an incredibly powerful and versatile tool and has huge power to be customized. The ease of integrating BigFix with other tools has proven to be one of its most powerful strengths."
Stacy Lee, Information Security Systems Specialist, Stanford University

Provide common view of assets.

- With BigFix's single console and single platform, IT operations and security organizations can collaborate more effectively to cut operational costs, compress endpoint management cycles, enforce compliance in real time, and improve productivity.

Using BigFix, security and infrastructure teams can see and act on the same endpoint data without switching between multiple applications, saving them time and accelerating decision making. IT operations and security teams can collaborate more effectively to cut operational costs, compress endpoint management cycles, and enforce compliance in real time while improving productivity.

The Bigger Truth

Endpoint management software plays a critical role in both security and compliance strategies. With an ever-changing attack surface in most organizations, securing endpoints is an almost impossible task without automating the inventory, patching, and configuration process.

EMS is a core component of IT infrastructure, and as such, must facilitate integration with the many other risk management systems that are operating in the security stack. This integration is paramount to enabling both IT and security teams to keep up with the rapidly expanding threat landscape.

While there are many patching solutions available today, organizations should closely evaluate options to ensure they offer robust capabilities supporting both security and compliance requirements, while offering the scalability, flexibility, and extensibility to support organizational growth and complexity.

HCL BigFix, widely recognized as a leading endpoint management software solution, meets or exceeds the seven endpoint management capabilities and should therefore be strongly considered when organizations are adding or upgrading their EMS.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.