HCL SOFTWARE

HCL

# Select the Best Endpoint Management Solution

Real-time visibility and control for hundreds of thousands of distributed endpoints

## Securing and Managing Thousands of Endpoints

Managing workstations, servers, and roaming devices presents IT organizations with a formidable challenge. With conventional management methods, even simple questions such as, “How many laptops do we have?”, “What operating system versions are our desktop systems running?” or “Are our patches up to date?” can take days to weeks to obtain and can generate inaccurate, incomplete responses. Days or weeks is not usually acceptable when board members and high-value supply chain partners want to know that all systems are patched and compliant. They understand business risk and the cost of disruption and data loss. When critical patches are released, time is of the essence. Vulnerable machines must be quickly identified and remediated as quickly as possible. The business impacts and disruption can be enormous and long term, as the WannaCry attack demonstrated in May 2017.

That is why organizations seek to enhance security and compliance as they attempt to consolidate and eliminate redundant and non-performing management tools, reduce costs, and improve staff productivity. Many are looking for ways to meet today's complex environment of heterogenous servers and workstations by implementing a comprehensive, endpoint management platform that addresses security, compliance, inventory and lifecycle management.

Organizations need better visibility into their endpoint infrastructure so they can understand needs, gaps and opportunities for improvement. They are looking for ways to speed and simplify the deployment of new software, software updates and critical security patches, maintain and prove compliance with evolving industry and government regulations, and protect an ever-expanding and often porous perimeter that is vulnerable to attack and security risk.

In a world accustomed to multiple, fragmented technologies and point solutions, organizations need a unified approach that supports endpoint security and management across heterogeneous devices and operating systems. They need fast deployment and rapid time to value, both in multi-cloud and on-premise implementations. They need an open architecture that delivers company-specific policies without extensive programming and scripting. And when the environment faces threats, they need agile, real-time endpoint visibility, protection, rapid remediation and reporting capabilities.

An effective endpoint security and management platform can meet all these goals as it simplifies management processes, enhances endpoint control and centralizes views with a single, easy-to-use graphical user interface. It can deliver these capabilities for any number of physical and virtual endpoints including servers, desktops, laptops, point-of-sale devices, ATMs and self-service kiosks.

More effective endpoint security and management can play a key role in delivering swift, secure, stable IT services 24×7 to customers, employees, business partners, regulators, investors and other constituents. The highly exposed nature of today's IT infrastructures is changing how organizations manage and secure endpoints, processes and data. An automated endpoint management platform is fundamental to the transformation of IT functions from back-end operations to key services that are closely integrated with business success, compliance with internal security policies, and effective process execution.

## Getting Started with Endpoint Management

This buyer's guide lists the features and capabilities that comprise an effective endpoint management platform:

- Device Discovery
- Inventory and Software Usage Analysis
- Patch Management
- Operating System Deployment and Software Distribution
- Server Automation
- Power Management
- Security and Compliance
- Remote Desktop Control
- Lightweight, Scalable Architecture

This guide discusses the benefits of each capability and provides checklists to help you evaluate whether or not a particular vendor's solution addresses each of these areas effectively. You will also find a list of attributes and capabilities you should look for in selecting a provider that can support the full breadth of your endpoint security and management requirements.

## Device Discovery

Device discovery is a key capability in most IT environments. Identification of devices including computers that are either unmanaged or potentially rogue is key to a secure and properly managed environment.

Gathering information about devices should be more than a number-counting, "snapshot" exercise conducted periodically. It should create dynamic, near real-time awareness about changing conditions in the infrastructure—with pervasive visibility and control to quickly identify all IP-addressable devices in the organization and the applications installed on them.

The optimal solution will distribute scanning to the endpoints. Distributed scanning conserves WAN bandwidth produces results faster since scanning can be done in parallel and can work in complex network configurations including isolated subnets. Once discovered, supported devices can be brought into the managed environment automatically, and then interrogated to identify installed applications and application usage data.

| **Device Discovery** | | |
|---|---|---|
| Look for a solution that: | **BigFix** | **Other** |
| Dynamic, near real-time identification all IP-addressable devices | √ | |
| Distributes scanning to the endpoints | √ | |

## Inventory and Software Usage Analysis

Creating a comprehensive software asset inventory for license reconciliation and compliance purposes is a highly valuable asset in any organization. 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. It supports better planning, budgeting and vendor license compliance. Current asset information can also provide invaluable information to help desk and support staff to speed problem diagnosis and resolution.

Unauthorized software on company-owned devices present a security risk that must be mitigated. Software asset inventories allow organizations to identify and then delete software that poses a clear and present security risk.

The optimal solution can drill-down to uncover details across vast infrastructures with hundreds of thousands of endpoints, rapidly delivering aggregated statistics and usage information. It helps maintain visibility into all endpoints, including devices that roam outside the organization's network. Newly discovered endpoints are brought under management with minimal impact on network operations. And it should do all of this as close to real-time as possible.

| **Inventory and Software Usage Analysis** | | |
|---|---|---|
| Look for a solution that: | **BigFix** | **Other** |
| Provides accurate, in-depth and detailed inventory data that includes all hardware, configuration, and software properties | √ | |
| Provides discovery and inventory management capabilities from a single console | √ | |
| Supports searching, browsing, and editing of a software identification catalog containing more than 100,000 signatures out of the box, and is kept current based on changes in the software industry | √ | |

| | | |
|---|---|---|
| Allows easy, wizard-based customization of the software identification catalog to include tracking of homegrown and proprietary applications | √ | |
| Provides drill-down information about the software publishers, titles and applications found on endpoints, as well as the CVEs available for identified titles | √ | |
| Includes software metering that aggregates historical statistics and usage information | √ | |
| Tracks software usage patterns and trends across Microsoft Windows, UNIX and Linux endpoints for applications from SAP, Oracle, Microsoft, IBM and other software vendors | √ | |
| Tracks End of Support (EOS) dates for titles from IBM and Microsoft | √ | |
| Provides rich asset data for reporting and integrating with other enterprise systems that need accurate, up-to-date inventory (for example, service desk, asset management system, inventory warehouse, configuration management databases) | √ | |
| Supports out-of-the-box service desk integration to deliver advanced functions, such as implementing an automated, self-service enterprise application ("app") store | √ | |
| Enables seamless integration with other service desk and asset management tools via Representational State Transfer (REST) application programming interfaces (APIs) | √ | |
| Enables ease of implementation and use, providing entry-level software asset management features while enabling adoption of more sophisticated solutions | √ | |
| Provides tight integration with endpoint security and compliance management | √ | |
| Includes both agent-based and agentless distributed scanning architecture for low-impact, low-latency device detection as well as deep inspection and reporting | √ | |
| Quickly identifies all IP-addressable devices including network devices and peripherals, such as printers, scanners, routers and switches, in addition to computer endpoints | √ | |
| Discovers undocumented endpoints within the environment and identifies suspicious "rogue" devices* | √ | |
| Provides near real-time reporting of open ports and services in use* | √ | |
| Supports ad hoc queries to endpoints—for example: "Get me the serial numbers of all computer monitors"—and delivers results in minutes with minimal impact at scale* | √ | |
| Reaches endpoints regardless of their location, on or off-network, and keeps inventory data current, even for endpoints not constantly connected to the network | √ | |

* These capabilities may be provided by the platform itself or a Query app.

## Patch Management

Increasing infrastructure complexity, proliferation of management tools, and overloaded IT personnel can overwhelm efforts to manage a rapidly growing base of endpoint devices and platforms. Organizations need a comprehensive, unified management platform that reduces the clutter, inefficiency, and expense of multiple tools as it delivers real-time visibility and control. Such a platform should optimize patch operations across all OS platforms by bringing them together under a single management umbrella.

The optimal solution provides an automated, simplified patching process that is administered from a single console and provides real-time visibility and enforcement to deploy and manage patches to endpoints — on and off the corporate network. It must provide a high first pass success rate, reducing manual remediation and repeated deployments. Besides increasing the effectiveness of the patch process, the solution should reduce operational effort and patch cycle times to keep your endpoints secure.

| **Patch management** | | |
|---|---|---|
| Look for a solution that: | **BigFix** | **Other** |
| Provides automatic patch management from a single management console | √ | |
| Automatically manages patches for multiple operating systems, including Microsoft Windows, UNIX, Linux and Mac OS, from the same console and server | √ | |
| Automatically manage patches for multiple operating systems including Windows, macOS, IBM AIX, HP-UX, Solaris, VMWare ESX Server, RHEL, SUSE, CentOS, Debian, and Ubuntu | √ | |
| Reduces remediation cycles from weeks to minutes or hours, minimizing security and compliance risk | √ | |
| Enables patch management for endpoints on or off the network, including roaming, Internet-connected devices | √ | |
| Provides consistent functionality over low-bandwidth and globally distributed networks | √ | |
| Increases patch success rates to over 98 percent (from a typical 60 to 75 percent)—and confirms remediation | √ | |
| Removes patch management overhead by providing pre-tested patch policies for administrators | √ | |
| Allows grouping of patches into a single deployment task to simplify management, automatically resolving any dependencies | √ | |
| Downloads and applies only the patches relevant to each endpoint | √ | |
| Allows system administrators to rapidly create and deploy custom patches to remediate zero-day vulnerabilities | √ | |
| Enables patching of online virtual machines to improve security in virtual environments | √ | |
| Provides offline virtual machine patching, so dormant virtual machines are not exploited when they are brought back into service | √ | |
| Coordinates operating system patching for complex multi-tier server applications in both physical and virtual environments | √ | |
| Supports task sequencing that can be used for critical tasks like server builds (for example, deploying operating systems, configuring settings, deploying software, patching, changing the host name and restarting computers) | √ | |
| Enhances visibility into patch compliance with flexible, real-time graphical monitoring and reporting | √ | |
| Displays patch status—Needs patch, patch is pending or running, patch was installed successfully, patch installation failed | √ | |
| Delivers information on which patches were deployed, when they were deployed and who deployed them | √ | |
| Automatically assesses endpoint compliance against defined policies, such as mandatory patch levels | √ | |
| Detects and remediates issues where a previously installed patch has been rolled back or overwritten, and allows automatic reapplication of uninstalled patches | √ | |

| | | |
|---|---|---|
| Allows making patches available as “offers” to users, with or without mandatory implementation dates, to minimize disruptions | √ | |
| Allows patches to be grouped and rapidly installed during defined change windows | √ | |
| Allows optional patch dialog window suppression and delayed/ scheduled reboots | √ | |

## Operating System Provisioning and Software Distribution

The ultimate goal is to simplify deployment of new workstations, laptops, and servers. This process not only includes the OS deployment; but also, all necessary applications.

Deploying and configurating operating systems on bare metal or upgrading operating systems is a frequent and time-consuming activity. The endpoint management platform should speed operating system deployment and user profile migration; and it should enforce standardized and approved images to reduce risks associated with non-compliant or insecure configurations. Additionally, operating system upgrades should minimize the impact on end users.

Organizations are more widely distributed today than ever, making IT management tasks such as distributing and managing endpoint software extremely challenging. These organizations need robust capabilities for quickly and reliably delivering and managing business-critical applications on a full spectrum of endpoints. An endpoint management platform should allow IT organizations to deploy key business applications and allow end users to select and install approved software from an enterprise catalog.

| **Operating System Provisioning and Software Distribution** | | |
|---|---|---|
| Look for a solution that: | **BigFix** | **Other** |
| Provides management of software distribution across multiple platforms from a single, unified point of control | √ | |
| Distributes large software updates across low-bandwidth and globally distributed networks | √ | |
| Supports policy- and computer group-based installation of new and updated software packages across distributed environments | √ | |
| Delivers closed-loop verification of software installation/de-installation | √ | |
| Supports user self-provisioning and de-provisioning of authorized applications and software packages | √ | |
| Supports local pre-caching of software packages to improve installation reliability | √ | |
| Eliminates the need to duplicate files for software distribution | √ | |
| Provides simple yet powerful customization capabilities for accurate targeting and deployment of software packages | √ | |
| Minimizes network impact via policy-driven bandwidth throttling, static and dynamic, across all operating system platforms, including the ability to throttle against actual available network link bandwidth | √ | |
| Maintains configuration files such as Microsoft Software Transform (MST) and Microsoft Software Patch (MSP) files separately from core software components to efficiently handle multiple package configurations | √ | |

| | | |
|---|---|---|
| Is compatible with incumbent software distribution tools and package formats | √ | |
| Supports fully integrated "bare metal" operating system deployment for new workstations, laptops and servers throughout the network as well as operating system migration for existing endpoints | √ | |
| Utilizes the endpoint management core infrastructure for operating system migration, eliminating the costs associated with maintaining a standalone operating system deployment infrastructure | √ | |
| Shrinks deployment and migration time with fully automated operations including remote wake-up support and deployment scheduling | √ | |
| Deploys hardware-independent images to machines from multiple hardware vendors, injecting appropriate device drivers as needed | √ | |
| Enables in-place upgrades from Win 7 to Win 10 as well as migration of user profiles and data | √ | |
| Integrates operating system deployment with security baselines and configuration provisioning requirements, including "top off" patching so that systems are ready to use immediately | √ | |
| Puts real-time endpoint information at administrators' fingertips with remote diagnostics capabilities that can simplify and streamline help-desk calls and problem resolution | √ | |
| Targets specific actions to an exact type of endpoint configuration or user type | √ | |
| Provides remote discovery and analysis of applications installed on endpoints | √ | |
| Allows administrators to establish role-based access to support different user responsibilities and line of business requirements | √ | |
| Simplifies and operationalizes security by embedding security practices and compliance initiatives as part of the IT operations process | √ | |

## Server Automation

Not all servers are created equal and it is imperative a endpoint management platform help manage physical, virtual and remote servers while lowering operational costs with real-time, policy-based management. A seamless physical and virtual server management from the same, single interface greatly can help improve visibility and control of all endpoints. This enables users to easily deploy and manage servers across heterogeneous platforms using either pre-built or custom automation.

Additionally, automated task sequencing capabilities should be a key consideration in order to establish critical tasks like server builds (ex. deploying operating systems, configuring settings, deploying simple software, changing the host name, and restarting the endpoint) in addition to other common system administrator tasks that need to be carefully sequenced. It is also important to select an endpoint management platform that provides advanced automated patching for physical, virtual and clustered servers as well as integration with other automation engines.

| **Server Automation** | | |
|---|---|---|
| Look for a solution that: | **BigFix** | **Other** |
| Delivers real-time visibility and control for all servers (physical and virtual) with policy-based management designed to lower costs. | √ | |
| Provides seamless physical and virtual server management – including clustered server OS patching – from a simple interface. | √ | |

| | | |
|---|---|---|
| Supports task sequencing with common tooling that can be used for critical tasks like server builds (ex. deploying operating systems, configuring settings, deploying software, patching, changing host names and restarting computers). | √ | |
| Supports fully integrated “bare metal” operating system deployment for new servers as well as operating system migration and refresh for existing servers. | √ | |
| Automates clustered OS and middleware patching, minimizing labor costs while ensuring that all servers are patched and configured according to security policies. | √ | |
| Coordinates operating system patching for complex multi-tier server applications in both physical and virtual environments | √ | |
| Integrates with other server automation engines such as Chef | √ | |

## Power Management

Most endpoints have built-in power management features, and many end users are familiar with their controls. But relying on end users to manage an organization’s power consumption is seldom enough to achieve measurable results. A more effective approach is centralized management. An ideal solution can reduce electricity usage while avoiding disruptions in systems management, with controls provided through a single, unified console.

The IT organization should be able to apply conservation policies infrastructure-wide while providing the necessary granularity to apply power management policies to a single computer if necessary. Combine power management with remote wake-up capabilities, and the result can satisfy the sometimes conflicting needs of management, which typically prefers that machines be powered down frequently to maximize energy savings, and the needs of IT, which requires machines to be on during non-working hours, when it is easiest to apply patches and update software.

| **Power Management** | | |
|---|---|---|
| Look for a solution that: | **BigFix** | **Other** |
| Enables management of power settings from the same centralized server and console for all endpoints running Windows and Mac operating systems | √ | |
| Provides out-of-the-box capabilities to deal with common power management issues, such as PC insomnia and PC narcolepsy | √ | |
| Provides the granularity necessary to apply policies to a single computer when necessary | √ | |
| Enables administrators to assign different power usage metrics to systems based on detected characteristics | √ | |
| Provides fine-grained controls for hibernation, standby and “save work before shutdown” options | √ | |
| Empowers end users with an opt-in approach that allows them to select their power profile from a menu of administrator-defined power configuration options | √ | |
| Engages end users in conservation initiatives through a client-side dashboard view into their individual power consumption and savings | √ | |
| Enables the creation of “what if” energy usage scenarios and provides green impact reports to encourage participation in conservation initiatives | √ | |
| Identifies and automatically fixes power profile misconfigurations | √ | |

| | | |
|---|---|---|
| Schedules computer sleep and hibernation states to keep a limited number of computers functional enough to receive and distribute wake-up alarms to other computers in deeper states of sleep | √ | |
| Preserves user data by automatically saving documents prior to beginning a shutdown or sleep/standby procedure | √ | |
| Schedules Wake-on-LAN to enable endpoint wake-up before the start of the workday or for scheduled maintenance, including support for remote user wake-up | √ | |
| Provides graphical reporting on aggregate power usage and savings, with the ability to export report data to Microsoft Excel for further analysis | √ | |

## Security and Compliance

Security teams can be overwhelmed by a sea of vulnerabilities–without the contextual data to help them focus their efforts on the weaknesses that are most likely to be exploited. Cyberthreats need to be stopped before they cause significant financial and reputational damages to an organization. Organizations need to detect vulnerabilities, prioritize risks, remediate and report compliance in near real time. The business disruption and financial impact can be enormous and long term, as the WannaCry attack demonstrated.

The WannaCry attack began in Asia on May 12, 2017. Within a day, the ransomware cryptoworm which targeted computers running the Microsoft Windows, was reported to have infected more than 230,000 computers worldwide. It encrypted data and demanded ransom payments. On May 16, BigFix released fixlets immediately after Microsoft released emergency patches and security bulletin MS17-010. BigFix clients were best prepared, allowing the patch to be deployed and installed within hours. However, business impact was enormous. WannaCry affected an estimated 400,000 computers in 150 countries, causing an estimated cost of up to $4 billion. Many organizations lost valuable data and infected machines were wiped and rebuilt — a remediation task that lasted for months. Consider a endpoint management platform that can keep devices continuously complaint and patched while allowing staff to respond with quickly when a cyber attack occurs.

Continuous compliance across an organization must include both connected (on-network) and disconnected (off-network) endpoints. An effective endpoint management platform should include out-of-the-box support for the most popular security benchmarks published by CIS, DISA STIG, USGCB and PCI-DSS. Agents on endpoints should monitor, enforce and report on the security configuration status of the endpoints in real-time regardless of OS type or location. Any compliance drifts should be reported instantly and quickly remediated to reduce the overall security risks and potential compliance fines and penalties.

An effective endpoint management platform not only must address the risks associated with security threats but also control cost, complexity and staff burden while meeting compliance mandates. It should help the organization protect endpoints and assure that compliance with internal security policies.

| **Security and Compliance** | | |
|---|---|---|
| Look for a solution that: | **BigFix** | **Other** |
| Manages the configuration of physical and virtual endpoints regardless of location, operating system, applications installed or connection (including wired computers or intermittently connected roaming devices) | √ | |

| | | |
|---|---|---|
| Remediates endpoints to a compliance baseline and then continuously enforces configuration policies on or off the network | √ | |
| Automates endpoint remediation without human interaction—a critical factor in quickly responding to cyber breaches before widespread damage occurs | √ | |
| Provides accurate, up-to-the minute visibility and continuous enforcement of security configurations and patches from a single management console | √ | |
| Integrates with IBM QRadar to expedite the remediation of the vulnerabilities QRadar finds and prioritizes | √ | |
| From QRadar, pushes the prioritized list of vulnerabilities directly to the management console, for timely, automated endpoint remediation (quarantine/patch/reconfigure) | √ | |
| Contains a comprehensive library of technical controls based on well-known best practices that help achieve security compliance by detecting and enforcing security configurations | √ | |
| Supports the Security Content Automation Protocol (SCAP) | √ | |
| Provides out-of-the-box checklists containing over 5,000 standard configuration settings mapped to industry standards for Windows, UNIX and Linux | √ | |
| Provides out-of-the-box checklists for PCI-DSS, the Payment Card Industry Data Security Standard, administered by the Payment Card Industry Security Standards Council | √ | |
| Provides out-of-the-box best practices that meet US Federal Desktop Core Configuration (FDCC) and United States Government Configuration Baseline (USGCB) regulations | √ | |
| Provides out-of-the-box best practices that meet Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs) | √ | |
| Provides out-of-the-box best practices based on Center for Internet Security (CIS) security benchmarks | √ | |
| Identifies and eliminates known vulnerabilities using automated policy enforcement or manual deployment | √ | |
| Can quickly identify rogue or misconfigured endpoints and takes steps to locate them for remediation or removal | √ | |
| Provides wizards for custom policy formulation, reporting and enforcement | √ | |
| Is certified by the National Institute of Standards and Technology (NIST) for both assessment and remediation | √ | |
| Enables quick customization through an easy to use API that supports multiple platforms using the same language | √ | |
| Supports administrator skill levels from beginner (with a wizard to create scripts without having to know the tool's language) to expert (with extreme flexibility in customization) | √ | |
| Provides tight integration with Lifecycle management tools (e.g. BigFix Lifecycle) | √ | |

It is common for an organization to need compliance information on a particular platform or type of endpoint, on a particular organizational or geographical segment, or on a specific regulatory or governance objective across all endpoints. Comprehensive reporting capabilities including ensure rapid, timely and easy-to-use reports and views are needed.

| **Compliance Reporting** | | |
|---|---|---|

| Look for a solution that: | **BigFix** | **Other** |
|---|---|---|
| Collects and archives automated security check results to help identify configuration issues and report levels of IT security-related compliance | √ | |
| Provides analytics capabilities that support enforcement of the organization's technical and configuration policies by monitoring, reporting, and tracking progress, and determining the success of security initiatives | √ | |
| Provide reports to board members and high-value supply chain partners that all systems are continuously patched and compliant, and provide historical reports to determine progress being made toward compliance goals | √ | |
| Delivers historical reports on the health and security of endpoints for use in the remediation of non-compliant endpoints and confirmation of remediation | √ | |
| Provides overview dashboards and executive rollups showing historical security compliance and hot spots, with the ability to drill down for detailed information | √ | |
| Provides actionable reports consolidated by remediation technique (such as a specific patch), not just a "laundry list" of overlapping, often redundant vulnerabilities | √ | |
| Identifies, manages and reports on policy exceptions and deviations | √ | |
| Provides a full range of reports for managing IT policy checks, including compliance status and history, reports by computer and computer group, and exception reports | √ | |
| Enables the creation of flexible, on-demand, ad hoc custom queries and reports | √ | |
| Provides report flexibility, including report filters (for example, historical compliance, computer metadata, checklist metadata, and so on), report column management, actual measured versus desired values, report exports, saved reports and more | √ | |
| Enables users to easily create custom checklists within minutes by combining included best-practice checks with custom checks | √ | |
| Shows trending and analysis of historical configuration compliance and security changes through advanced reporting | √ | |
| Bases analysis on infrastructure views that can be defined in multiple ways, from an individual device to groups of devices to the entire infrastructure | √ | |
| Includes a separate security analytics data warehouse to store historical compliance data | √ | |
| Supports audit requests by providing a historical state versus current state view | √ | |
| Supports a reporting server for auditors, with read-only access and access to selected information | √ | |
| Restricts access to endpoints and reports through user permissions and roles | √ | |
| Uses the same console, architecture and agent as IT operations uses to manage endpoints | √ | |

Recent data breaches highlight the urgency of protecting sensitive data from accidental or intentional misuse and loss. Faced with these challenges, organizations need a robust endpoint protection and data loss prevention (DLP) solution that integrates easily into the existing endpoint management infrastructure, effectively addressing the obstacles to deploying effective data protection. Deploying an endpoint management platform can help reduce complexity and save administrative time and costs.

| Endpoint Protection | | |
|---|---|---|
| Look for a solution that: | **BigFix** | **Other** |
| Provides a consolidated, unified approach to delivering and managing antivirus, anti-spyware, firewall and encryption services for leading products from multiple vendors, such as Symantec, McAfee, Trend Micro, Microsoft and Sophos | √ | |
| Monitors system health to ensure that endpoint protection clients are always running and that virus signatures are updated | √ | |
| Facilitates migrating endpoints from one security solution to another with one-click software removal and reinstall | √ | |
| Includes granular device control to restrict USB removable storage device access by vendor, model and serial number | √ | |

The ability to query and interrogate endpoints is a powerful and useful capability for IT Operators, Security Analysts, Help Desk Staff and other IT personnel. Having current endpoint configuration information can be critical to diagnosing and resolving issues that will invariably occur. The ability to run queries, quickly obtain results, deploy content, or take action is useful to anyone responsible for endpoint management and security. For example, Security Analysts must interrogate endpoints to research security threats and vulnerabilities. Analysts could wait for hours or days for ad hoc requests for information. They need the ability to interrogate all endpoint devices and receive instantaneous results. And if remediation is needed, authorized users should be able to deploy content and take other corrective actions - quickly and easily.

| Query and Interrogate Endpoints | | |
|---|---|---|
| Look for a solution that: | **BigFix** | **Other** |
| Queries individual computers, manual computer groups and dynamic computer groups, and receives results back within seconds. | √ | |
| Provides the same user interface to Security Analysts as used by IT Operations, strengthening enterprise security and bridging the gap between IT operations and Security. Control rights to query and manage endpoints. | √ | |
| Provides sample queries for applications, files, devices, networks, processes, registry, policies, and users. | √ | |
| Identifies which applications and services are installed on endpoints. | √ | |
| Examines files and system configuration settings to identify additional security threats. | √ | |
| Verifies target selection criteria, on a few sample endpoints, as content is developed, ensuring the correct endpoints are targeted before production use. | √ | |
| Exports query results to comma-separated value (.csv) file. | √ | |
| Creates a library of custom queries and keeps collections of queries private, or allows controlled sharing of libraries. | √ | |
| Search available queries by keyword. | √ | |

## Remote Desktop Control

Remote desktop control is a necessary capability of any endpoint management platform. Help desks and support personnel depend upon the ability to assume control of keyboard and screen of workstations and servers in a data center downstairs or half way around the world.

The ability to remote control Windows, Linux, and MacOS endpoints using a single tool streamlines staff efficiency and reduces training requirements. Remote diagnostics capabilities put real-time endpoint data at administrator's fingertips with capabilities to help end users resolve IT issues, which helps ensure that endpoint configurations remain current and compliant with organizational policies.

| **Remote Desktop Control** | | |
|---|---|---|
| Look for a solution that: | **BigFix** | **Other** |
| Provides functionality across Windows, Linux and MacOS endpoints. Optionally, remote desktop capabilities may be provided through built-in Microsoft components for endpoints running Windows. | √ | |
| Offers multiple actions to the controller user, such as remote control, guidance, chat, file transfer, collaboration | √ | |
| Can be configured to synchronize and authenticate user and group data from an LDAPv3 server, like Active Directory | √ | |
| Provides a method of centralized, and finer, policy control, where targets can have different policies that are determined by the user who is trying to start the remote-control session | √ | |
| Supports configuration of targets to be strictly managed, to fail back to peer-to-peer mode when the server is not reachable, and to accept both peer-to-peer and managed remote-control sessions | √ | |

## Lightweight Architecture

In most environments, the numbers and types of endpoints are rising, and networks are growing more complex. Visibility and control of endpoints are often poor and service levels are difficult to maintain. The resulting challenge is how to achieve an accurate and comprehensive "single source of truth" for the environment—and then use that truth for managing those vast numbers of endpoints. The key lies with an endpoint management platform that can consolidate and simplify key management services organization-wide.

By placing an intelligent agent on each endpoint, continuous self-assessment and policy enforcement significantly reduces staff workload. In contrast to traditional client-server architectures that wait for instructions from a central control point, an intelligent agent initiates actions in an autonomous manner, sending messages upstream to the central management server and pulling patches, configurations or other information to the endpoint when necessary to comply with a relevant policy.

The single-agent approach enables organizations to get the most from their current assets. Since the endpoint management server is always kept up-to-date by the agent, there is no need to run lengthy scans, execute queries or worry about systems that are shut down or roaming off the corporate network. The agent's autonomous operation, coupled with the visibility provided by a single console, enables administrators to see events taking place across the entire network. This single-infrastructure approach distributes decision making to the endpoints to shorten update cycles, improve success rates for provisioning, boost end-user productivity, and reduce the workload of IT and help-desk staff.

The many organizations need the flexibility of deploying solution components into public or private clouds (i.e. cloud-ready.) In fact, capacity planning should include specifications in terms of cloud virtual CPUs and operations per second. Tuning options should also work well in the cloud and on-premise implementations. And virtual environments should be supported.

| Solution Architecture | | |
|---|---|---|
| Look for a solution that: | **BigFix** | **Other** |
| Consolidates IT operations and IT security functions in a single view, delivery model and software offering | √ | |
| Assesses and remediates issues using a single, multipurpose, intelligent agent | √ | |
| Provides continuous endpoint self-assessment and policy enforcement in real time | √ | |
| Typically utilizes 10 MB of endpoint memory depending on platform, content and usage | √ | |
| Requires on average less than two percent of CPU utilization, ensuring endpoint performance is not impacted | √ | |
| Autonomously assesses and enforces policies whether the endpoint is connected to the corporate network or not | √ | |
| Employs a published command language to enable customers, business partners and developers to create custom policies and services for managed endpoints | √ | |
| Delivers real-time visibility into all endpoints including desktops, laptops, servers, point-of-sale systems, ATMs and self-service kiosks | √ | |
| Provides an easy-to-use graphical user interface as well as an advanced command line interface (CLI) and API | √ | |
| Query/Collect information from client workstations without impacting performance | √ | |
| Supports up to 250,000 endpoints from a single management server | √ | |
| Manages roaming endpoints whether connected to the network or not | √ | |
| Manages heterogeneous platforms (Microsoft Windows, UNIX, Linux and Mac operating systems running on physical or virtual machines) | √ | |
| Uses the same infrastructure and resources to provide integrated remote control to simplify and streamline help-desk calls and problem resolution | √ | |
| Utilizes existing servers or workstations to stage content such as software installers and patches, reducing the need for management servers, ensuring speed of package delivery and minimizing network traffic | √ | |
| Permits cloud integration through custom extenders (e.g. VMware). | √ | |
| Permits all infrastructure to be deployed in public or private clouds with cloud specific tuning capability. | √ | |
| Allows any agent to be configured as a relay, or staging agent, between other agents and the centralized management console, optionally storing policies and content to reduce network load | √ | |
| Provides a vendor software solution that is certified using EAL 3 Common Criteria | √ | |
| Controls access through user permissions and roles to restrict access to endpoints, reports and the management console | √ | |
| Installs rapidly, with full deployments completed in hours or days, compared to weeks or months, even for the largest of organizations | √ | |
| Brings newly discovered endpoints under management in minutes with a local deployment of the intelligent agent | √ | |

| | | |
|---|---|---|
| Utilizes the same infrastructure across endpoint management capabilities, making it easy to solve today's challenges and seamlessly add other endpoint management capabilities as organizational requirements grow | √ | |
| Upgrades itself using its own infrastructure, enabling major product upgrades and updates in minutes or hours rather than weeks or months | √ | |
| Authenticates client reports to protect against spoofing | | |
| Provides built-in encryption capabilities for securing sensitive information in transit to endpoints | √ | |
| Minimizes the effort to keep implementations current using integrated product and content updates | √ | |
| Integrates with a comprehensive management portfolio to help ensure real-time visibility, centralized control and enhanced functionality for the entire IT infrastructure | √ | |
| Provides native language support for Italian, German, French, Spanish, Japanese, simplified Chinese, Traditional Chinese, Portuguese, Korean and English | √ | |

## Selecting the Best Solution Provider

The provider you choose should be able to support the full breadth of your endpoint management requirements. Ideally, you will also want a provider that can support you throughout the process of implementing the solution. Before you select a provider, be sure to ask these questions:

**Does your provider support your organizational goals through their technology?**
Look for providers whose solutions align with your organization's objectives. Do their solutions promote efficiencies, reduce business service deployment time, reduce both operating and capital expenses, enhance compliance and speed time to market?

**Does your provider offer part of the total solution or the complete solution?**
When you select a solution that addresses only a particular environment or endpoint requirement, you create "islands of management" which are more expensive to acquire, maintain, and support. A single endpoint management platform that provides a breath of functionality across multiple operating system platforms lowers the total cost of ownership.

**What type of global presence does your provider have?**
If your organization has international offices, a provider with a global presence and proven international experience.is important. Make sure the provider can adequately support your offices abroad.

**How sure are you of your provider's stability and staying power in today's economy?**
A big issue in a challenging economy is provider stability and viability. You should consider a provider who has a long history in the industry, a solid, forward-looking strategy, and the resources to withstand adverse economic times.

**What type of product support does your provider offer?**
It is important to have a solution provider who offers software technical support in time zones which match your operations. Additionally, look for providers whose solutions are embraced by communities of users who host user group meetings and contribute to a community website where user-generated content is hosted in order to grow the solution outside of official channels.

**Can your provider provide a flexible licensing and deployment options?**
When comparing various solutions and providers, business priorities and needs

change over time. Business agility is critically important in today's fast paced environment. Can your solution provider deliver endpoint management in the cloud, on-premise, or software-as-a-service? Are term and perpetual licensing available from the provider? Do they have proven experience as a managed service provider should you decide to outsource the some or all endpoint management activities?

| **Solution Provider** | | |
|---|---|---|
| Look for a provider that: | **HCL** | **Other** |
| Provides solutions which align with your organization's objectives | √ | |
| Offers a complete endpoint management solution that eliminates 'islands of management' problems | √ | |
| Has a global presence and proven international experience | √ | |
| Has a long history in the industry, forward-looking strategy and the resources to withstand adverse economic times | √ | |
| Offers software technical support when you need it | √ | |
| Provide solutions which are enthusiastically embraced by a community of users who share content and knowledge | √ | |
| Provides a flexible licensing and deployment options to meet ever changing business needs, now and in the future | √ | |

## For more information

To learn more about HCL BigFix, contact your HCL Client Partner, 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.'



**HCL Corporation Pvt. Ltd.**
Corporate Towers, HCL Technology Hub,
Plot No 3A, Sector 126, Noida - 201303. UP (India)

Produced in the United States of America. June 2019.



WX-10486 V1.1