HCL SOFTWARE | BigFix

HCL

A Buyers Guide for Selecting the Best Endpoint Management Solution

A feature by feature guide to selecting the best tools for your environment

Table of Contents

Securing and Managing Thousands of Endpoints

This buyer's guide lists capabilities that characterize an effective endpoint management platform and provides a checklist of features and attributes to help you evaluate whether or not a particular vendor's solution effectively addresses each of these feature and capabilities.

Managing a diverse set of endpoints - 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; therefore, vulnerable machines must be 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.

Organizations want to enhance security and compliance while consolidating and eliminating redundant and non/under-performing management tools in order to reduce costs and improve staff productivity. Additionally, 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.

Remote workers are becoming increasingly more important to business continuity. Keeping the workstations of remote works continuously patched and compliant, without costly VPN infrastructures, is critically important to expediting a Digital Transformation and protecting against cyber-attacks.

An effective endpoint security and management platform can meet all these business goals and objectives as it simplifies management processes, enhances endpoint control, and provides executives with business insights that enable better decision making. It can deliver these capabilities for any number of physical and virtual endpoints, on premise, at home, in the cloud or elsewhere -including servers, desktops, laptops, point-of-sale devices, ATMs, self-service kiosks and the latest modern devices running Windows 10 and macOS..

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, in both the cloud and on-premise implementations. An open and secure architecture delivering company-specific policies without extensive programming and scripting is needed. And when the environment faces security threats, they need agile, real-time endpoint visibility, protection, rapid remediation and reporting capabilities.

Getting Started with Endpoint Management

IT organizations must effectively manage endpoints throughout their lifecycle from provisioning to retirement. Capabilities must include the ability to discover new endpoints, inventory endpoint hardware and software, identify and optionally remove risky software, deploy software and associated updates, keep security applications running, deploy patches, remediate vulnerabilities identified by the Security team, automate manual processes through task automation, ensure compliance to internal and regulatory standards, monitor configuration settings and remediate drift, remotely control desktops, and interrogate on endpoints on as-needed basis. Organizations must consider the cost and complexity of using multiple tools, understanding the potential savings of centralizing and automating endpoint management activities across all endpoints, regardless of device type, operating systems, connection or location.

This buyer's guide provides 17 categories and more than 175 functions and capabilities to consider when selecting an endpoint management solution.

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

Beyond network discovery, a solution should also utilize cloud credentials to discover endpoints through cloud native APIs on multiple clouds.

Look for a solution that:

- 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 distributed scanning to conserve WAN bandwidth and speed the process
- Scanning tasks can be scheduled and automated

Inventory and Software Use 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 presents a security risk that must be mitigated. Likewise, software that is end of life represents a security risk because it is no longer patched. Software asset inventories allow organizations to identify and then delete/update software that poses a clear and present security risk. Tracking this software can be done through "allowlists" that identify only allowed software, or "denylists" that explicitly identify disallowed software.

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.

Look for a solution that:

- Provides accurate, in-depth and detailed inventory data that includes all hardware, configuration, and software properties.
- Identify if discovered software is stand-alone or part of a packaged bundle.
- Provides discovery and inventory management capabilities from a single console.

- Discover and inventory software in Containers.
- Provides a broad range of discovery mechanisms including a software identification catalog, package installation registry, vendor specific discovery APIs, custom template signatures, ISO SWID tags, and hardware discovery.
- 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 flexible customization of the software identification catalog to include tracking of homegrown and proprietary applications, as well as customization for rapidly changing software.
- 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 Oracle, Microsoft, Adobe, Red Hat, SAP, HP, BMC, CA, Citrix, Corel, Symantec, TIBCO, VMware 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).

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 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.

Look for a solution that:

- Automatically provide curated and supported patch content for multiple operating systems you need to manage such as Microsoft Windows, UNIX, Linux distributions and Mac OSX, all from the same solution interface and server.
- Ensures devices remain patch compliant regardless of their location or connection to the network.
- Reduces remediation cycles from weeks to minutes, minimizing security and compliance risk, increasing patch success rates to over 98 percent in the first pass.
- Validates the patch was successfully installed using the original conditions that led to the identification that the patch was necessary.
- Allows system administrators to rapidly create and deploy custom patches to remediate zero-day vulnerabilities.

- Automatically assesses endpoint compliance against defined policies, such as mandatory patch levels.
- Profoundly efficient, downloading and applying only the needed patches for each device.
- 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.
- Allows letting the end user decide when to install and restart, with ability to control defer, delay, and force install timing.
- Allows optional patch dialog window suppression and delayed/ scheduled reboots
- Offers a complete patching approach to manage the load balancing, distribution, install/remediation, and reporting with remediation confirmation.
- Provides flexible patch methods out of the box such as set-and-forget policy-based, custom curated patch bundles, or via individual application.
- Allows patches to be grouped and rapidly installed during defined change windows
- Simplifies operating system patching for complex multi-tier server applications in both physical and virtual environments.

Operating System Provisioning and Software Distribution

The ultimate goal is to simplify deployment of new workstations, laptops, and servers; and 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.

Look for a solution that:

- 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 of endpoints running Windows 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.
- Takes advantage of existing LDAP without being dependent to function.
- Simplifies and operationalizes security by embedding security practices and compliance initiatives as part of the IT operations process.

Task Automation

Today's skills shortage has put pressure on IT staff to do more with less; and automation is the key tool in your arsenal to find and fix more issues while minimizing manual processes. Advanced automation technologies enable admins to easily deploy and manage endpoints across heterogeneous platforms using a variety of languages and provide either pre-built or custom automation content.

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, cloud and clustered servers as well as integration with other automation engines.

Look for a solution that:

- Supports multiple automation languages such as Powershell and Python
- Provides thousands of pre-built and supported scripts that are provided as part of your product subscription
- Supports new releases of critical new software releases, such as Windows 11, and responses to new threats that need immediate remediation within 24 hours of the release.

- Delivers real-time visibility and control automation for all endpoints (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 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.

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.

Look for a solution that:

- 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.
- Enables the creation of "what if" energy usage scenarios and provides green impact reports to encourage participation in conservation initiatives.
- 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.
- 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.

Compliance and Security Policy Enforcement

Continuous security policy 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 and 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.

Look for a solution that:

- Provide real-time visibility into the security configurations of physical and virtual endpoints, regardless of location, operating system, applications installed or connection (including wired computers or intermittently connected roaming devices) to continuously enforce security policies.
- Discovers any configuration drifts instantly and remediates endpoints to a compliance baseline / policy. Endpoint remediation can be automated without human interaction - a critical factor in quickly responding to cyber breaches before widespread damage occurs.
- Provides out-of-the-box security configuration checklists including 20,000+ checks for 60+ operating systems (Windows, Mac, Linux, Unix) and middleware / applications (database, Web server, browser), based on best-practice security benchmarks such as CIS, DISA STIG, USGCB, and PCI DSS.
- Refreshes checklists constantly to support the latest benchmark levels to provide the best protection against new intrusion techniques.
- Provides wizards to customize checklists and allows configuration parameters to be easily changed to support specific organization needs.
- Is certified to the latest SCAP specification to consume custom contents and generate packages for additional checks.
- Monitors and manages the deployment status and health of various third-party anti-virus tools from Microsoft, Symantec, McAfee, Trend Micro, and Sophos. Provides remediations to address out-of-policy issues such as virus definition outdated.
- Assesses Windows endpoints against standardized, OVAL based security vulnerability definitions and reports vulnerabilities in real time.
- Isolates out-of-compliance endpoints from the network to protects against zero-day malware and vulnerability attacks until remediation is complete.
- Integrated with IBM QRadar SIEM solution to enable greater insights to security posture and QRadar Vulnerability Manager (QVM) to remediate vulnerabilities more effectively.
- Integrated with Carbon Black EDR solution to deploy CB agents and monitor their health and remediate vulnerabilities at an enterprise scale
- Integrated with Forescout Network Access Control (NAC) solution to authorize a device's access to network based on the device's configuration status.

Compliance Analytics and Reporting

An organization has a need to know the compliance status of all endpoints, a specific group of endpoints, or individual endpoints against a specific regulatory or organization policy objective. Comprehensive reporting capabilities including timely data collection and easy-to-use reports in order to track the effectiveness of its compliance effort and quickly identify security exposures and risks.

Look for a solution that:

- Continuously collects and aggregates endpoint check results from all endpoints in a database optimized for analytics and reporting.
- Provides analytics and reports for various groups (security analyst, IT operators, compliance analysts) to expose the policy compliance posture, including the current status and historical trending, for the entire deployment, a specific group, or individual endpoints
- Deploys a single analytics engine and provides consistent compliance reports to cover three key security domains: Security Configuration, Patch, and Vulnerability, from a single UI with easy switch from one domain to another.
- Security Configuration Reporting: Provides various reports to show both the current status and the historic trends for individual endpoint, individual checklist, individual check. An aggregated compliance posture for the entire deployment is also available.
- Patch Reporting: Provides a comprehensive and historical view of patching activities across the entire deployment to assess the overall patching posture. It enables more efficient prioritization of vulnerability remediation by identifying the critical patches to be applied, and helps organizations demonstrate compliance and pass audits.
- Vulnerability Reporting: Tracks and reports endpoints' vulnerability posture as a result of patching actions, enabling organizations to assess the risk posture, prioritize remediation risks, and demonstrate compliance with vulnerability related policies.
- Provides specific PCI dashboards and reports to simplify the monitoring and reporting of PCI compliance, against each PCI requirement and milestone
- Customizes all data fields to be included in reports and saves customized reports for later use.

Endpoint Interrogation

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.

Look for a solution that:

- 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 halfway 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.

Look for a solution that:

- Provides remote desktop control functionality across Windows, Linux, and macOS endpoints.
- Enables multiple actions to the controller user, such as remote control, guidance, chat, file transfer, and collaboration.
- Can be configured to synchronize and authenticate user and group data from an LDAPv3 server, like Active Directory.
- Provides a method of centralized policy control allowing targets to have different policies determined by the user initiating the remote-control session.
- Supports configuration of remote, in-network targets to accept both peer-to-peer and managed remote-control sessions, or if the server is not reachable, allow failback to peer-to-peer mode.
- Supports remote control sessions of endpoints, located inside or outside the corporate network either in attended or unattended mode.
- Permits a user located outside the corporate network to initiate a remote control session.
- Maintains session history with the possibility to record session activity for auditing purposes.

Reporting and Integration

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

Look for a solution that:

- Imports and consolidates endpoint data into a single endpoint data repository for reporting or other integrations.
- Manages all data source import to the data repository as well as provides the ability to schedules imports for each data source.
- Leverages a Business Intelligence (BI) tool to provide out-of-the-box reports to provide executives with an elevated view of the endpoint posture in various areas that enables quick risk identification and decision making.
- Provides high level and insightful data summaries grouped by different properties, displayed with a rich set of visualizations. Filtering should be provided enabling quick drill-down to a specific data group or category within seconds.
- Provides historical trends should be available to provide a quick glance of the progress over time.
- Provides an overviews of how all patches have been deployed across all endpoints over time, an overview of the exact numbers of devices of various types that are discovered and managed over time, and the migration status of the devices running unsupported OS versions, which introduce significant security risks, to supported versions.
- Provides an overview of the progress of all deployments that have been issued and results of deployment on devices.
- Consolidates data in a data repository, allowing an organization to use a BI tool of its own choice to generate additional reports to meet specific business needs.
- Provides deeper insights through integrations with other third-party solutions and enriched data sets that can include additional business context (e.g., business units, locations) or other endpoint security data (e.g., vulnerability) into the data repository.

Vulnerability Remediation

Vulnerability remediation capabilities should inform IT and Security operations on how to apply the best patch and configuration settings to quickly remediate discovered vulnerabilities, reducing risk and improving security. The goal is to eliminate or significantly reduce the burden of manually looking up each vulnerability on a static spreadsheet and then trying to match the vulnerabilities and their affected hosts.

Look for a solution that:

- Seamlessly integrates with vulnerability scanners like Tenable or Qualys.
- Reduces the time required to move from vulnerability assessment to remediation, from days or weeks to hours or minutes.
- Provides graphical reports enabling users to drill-down into the underlying data.
- Identifies vulnerabilities with available patches and those without.
- Automates the creation of prioritized remediation workflows.

Managing Endpoints in the Cloud

Vulnerability remediation capabilities should inform IT and Security operations on how to apply the best patch and configuration settings to quickly remediate discovered vulnerabilities, reducing risk and improving security. The goal is to eliminate or significantly reduce the burden of manually looking up each vulnerability on a static spreadsheet and then trying to match the vulnerabilities and their affected hosts..

Look for a solution that:

- Provides the ability to discover endpoints in the cloud through cloud native APIs to rapidly find cloud endpoints that are not managed.
- Includes full visibility to cloud endpoints with endpoint properties retrieved using cloud native APIs.
- Permits speedy automated deployment of the management agent on cloud endpoints to enable continuous patching, inventory and compliance.
- Supports simultaneous endpoint management in multiple cloud environments including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform
- Leverages a single infrastructure and tool to consistently manage both on-premise endpoints and cloud endpoints.

Modern Client Management

Modern client management capabilities enable organization do effectively deploy and managed Windows 10, Windows 11 and macOS endpoints.

Look for a solution that:

- Provides visibility and control of MCM endpoints alongside traditional endpoints from a single view.
- Provides correlated reporting, preventing the need to use spreadsheets or multiple reporting interfaces.
- Enables organizations to assume operational control of macOS, preventing end user activation lockout.
- Permits management of Windows 10, Windows 11 and macOS endpoints with or without an installed management agent.
- Uses the industry standard, Mobile Device Management Application Programming Interface.
- Simplifies “onboarding” through remote, end-user-initiated enrollment.
- Deploys an initial security policy once enrolled.
- Provides security polices such as installing kernel extensions and configuring inactivity and passcode settings.
- Centralizes control of security and configuration settings.
- Provides detailed inventory of MDM-managed endpoints.
- Provides the MDM actions such as remote wipe, lock device, restart, shutdown, and remove policies.

Mobile Management

Many IT organizations have deployed smartphones and tablets to support mission critical applications. Additionally, employees want to use their own mobile devices for business purposes. As a result, IT needs to cost-effectively manage both corporate-owned and employee-owned mobile devices running Android, iOS and iPadOS.

Look for a solution that:

- Manage and control mobile devices running iOS, iPadOS and Android operating systems.
- Utilize the same management infrastructure for mobile device as other endpoints, minimizing infrastructure, support and management costs.
- Provide visibility and control of all managed mobile devices from one management interface/console, alongside managed laptops, desktops and servers.
- Provide zero-touch, over-the-air BYOD enrollment of moibile devices
- Provision applications from Google Playstore and Apple App store.
- Provide security and control of managed devices including set passcode policy, restrictions policies, application blacklist and whitelist, camera and print settings, remote lock, wipe and restart capability.
- Be certified to support the following Android Enterprise management sets: Work Profile Management, Full Device Management. and Dedicated Device Management.

Lightweight and Scalable 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 endpoint shortens update cycles, improves success rates for provisioning, boosts end-user productivity, and reduces 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 also supported.

.**Look for a solution that:**

- 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, mobile devices, 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 300,000 endpoints from a single management server.
- Manages roaming endpoints whether connected to the network or not.
- Manages heterogeneous platforms (Microsoft Windows, UNIX, Linux and Macintosh 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 most agents to be configured as a relay, or staging agent between other agents and the centralized management console, optionally storing policies and content and reducing network load.
- Provides a vendor software solution that is certified under 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.
- Enables and speeds product upgrades and updates

- 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.

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? Can your solution provider deliver endpoint management in the cloud, on-premise, and software-as-a-service? Do they have proven experience as a managed service provider should you decide to outsource the some or all endpoint management activities?
When comparing various solutions and providers, business priorities and needs change over time. Business agility is critically important in today's fast paced environment.

Look for a solution that:

- Provides solutions which align with your organization's objectives.
- Offers a complete endpoint management solution that eliminates islands of management and redundant functionality.

- 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.

Conclusion

As cyber threats continue to grow in both complexity and number it's more important than ever to have an effective endpoint management platform across the enterprise. It is important to have a solution that addresses the entire lifecycle of endpoint management, fosters collaboration between the various teams responsible for patching and endpoint management, improves staff efficiency, reduces IT costs and complexity, speeds patching, and automates remediation of non-compliant endpoints.

This guide will enable you to make an informed decision on the tools needed to serve your organization and maximize your protection against the threats and attacks of today and into the future. Thanks for the opportunity to assist you in finding the best way forward.

For more, please visit **www.bigfix.com**.

© Copyright 2021 HCL
HCL Corporation Pvt. Ltd.
Produced in the United States of America.
All trademarks are the property of their respective owners.

About HCL Software

HCL Software, a division of HCL Technologies (HCL) develops, markets, sells, and supports over 30 product families in the areas of Customer Experience, Digital Solutions, DevSecOps, and Security and Automation. HCL Software is the cloud native solution factory for enterprise software and powers millions of apps at more than 20,000 organizations, including over half of the Fortune 1000 and Global 2000 companies. HCL Software's mission is to drive ultimate customer success with its IT investments through relentless product innovation.

For more information

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