HCL SOFTWARE

HCL

Is Free Really Free?

What is the true value of ‘free’ when selecting an endpoint management platform for today’s enterprise?

Highlights

- Free software is really not free when you consider the total cost of the hardware, software, maintenance, engineering support, and operations for multiple, disparate solutions.
- Although effective patching is critical, software distribution, OS deployment, task automation, hardware and software inventory, remote control of endpoints, and continuous security compliance are also necessary for a comprehensive, endpoint management platform.
- Organizations who need to reduce IT costs and complexity are opting for an integrated, cross-platform solution supporting Windows, UNIX, Linux and MacOS while substantially reducing the total cost per managed endpoint.

Can free software really provide the value necessary to perform full lifecycle operations management across the enterprise. A famous catch phrase coined during the Great Depression of the 1920s and 1930s was “there ain’t no such thing as a free lunch.” the implication, of course, there is always a hidden cost to anything free—and software is no exception.

Most times ‘free’ software be it open sourced based or commercial generally has gaps in capabilities that require, or maybe better stated, force customers to acquire additional software to fill those gaps which in turn increases the cost and complexity of the infrastructure. A good analogy is the ‘free puppy.’ Take a deep breath and think about it. Initially, the puppy could be free, but the ongoing vet care, walking, feeding and pickup up after the puppy certainly aren’t.

Microsoft System Center Configuration Manager (SCCM) thought to be free when included in various licensing models; yet when the TCO (Total Cost of Ownership) is evaluated it becomes obvious it is far from free.

What are the costs associated to fully design, architect, implement and provide ongoing management of SCCM?

Consider not only your current topology; but what it might look like in the future and then think about how SCCM maps to the topography including how to implement all the SCCM roles or components (Site Servers, Management Points, Distribution Points, Software Update Points, etc.), backend databases, and additional required software. Does your current staff have the cycles to keep SCCM up and running? Could their time be better spent on higher value projects and activities?

How much time does your operations staff spend distributing content through the SCCM infrastructure? How much network bandwidth is consumed while patching? Consider that BigFIx automatically delivers content through its ecosystem automatically so your staff does not have to spend time cleaning up stale content or making sure it is on the correct distribution point. BigFix also has bandwidth throttling so management actions can be performed without negatively impacting the network or users.

How complex is the underlying infrastructure? Is it time consuming to manage?

The larger and more complex the infrastructure, the more difficult it becomes to manage and the longer it takes to detect and remediate problems. There are numerous software components in a typical SCCM implementation which increases complexity and requires ongoing maintenance and support. Think about the time necessary for SCCM clients to report back the data through the SCCM hierarchy. If IT staff have to continuously remediate agent failures, or the failure of any other component, the ability to quickly respond to attacks is compromised.

There are vendors who provide tools for SCCM to help administrators reduce the complexity of deploying and managing the infrastructure. Indeed, it seems apparent that Sysadmins need help. Consider that any additional tools or add-ons contribute to more complexity and higher management costs.

Many solutions require multiple agents which burden end user systems and add cost. How many agents are running on each endpoint today? How much of the CPU is required when endpoint management actions are being run? Do you need to schedule patching afterhours or weekends to prevent loss of productivity?

Is your IT environment heterogenous? Are UNIX, Linux and Macintosh operating systems in your network?

There are few enterprises that only use Microsoft Windows. Most enterprises are heterogenous and most IT organizations need to manage endpoints that run Windows and non-Windows operating systems.

In March 2018 Microsoft began notifying clients that certain features, products, and operating systems, including Linux and UNIX, were removed, or will be removed from SCCM support. This forces organizations to find a disparate tool or tools to management non-Windows operating systems. Consider ramifications – each tool will require additional hardware, software, expertise, etc. Does the current staff have the time and resources to manage additional tools in addition to SCCM, or will you need to hire additional Linux, UNIX and Mac expertise and create additional management silos?

For Microsoft Azure cloud environments, Azure Update Management is a service provided to patch Windows and Linux servers in the cloud. Although Azure Update Management is included in the Azure subscription, why not choose a single, comprehensive endpoint management platform that manages endpoints both in the cloud and on-premises? Why add complexity and cost just for devices in the cloud?

SCCM may integrate with other solutions in order to extend capabilities it doesn't natively provide. What is the initial integration and/or software license cost? How much time will be required of the IT staff to maintain these other solutions or integrations? Will these tools capture all the data to update the enterprise CMDB? How often is the data exchanged or used to update the enterprise CMDB? Is there a single view of all servers and workstations in the enterprise? If not, what is the cost of aggregating data on so that everyone has the same information?

Do you need information about the current status of the environment quickly? Is stale or inaccurate data a problem?

Speed is important, especially if there is a potential security threat. The ability to respond quickly is often key to mitigating threats. Scanning solutions, like SCCM, are often not fast enough when IT staff need immediate answers to make informed decisions and take decisive actions.

SCCM has a default check-in period for clients, which can potentially introduce stale data. If this check-in period is reduced in an attempt improve data currency, what will be the impact on the network of more frequent polling?

Do you have workstations who are seldom or never on the enterprise network? How long will it take to deploy a zero day vulnerability patch to all endpoints?

Does your organization have workstations that are internet facing or disconnected from the corporate network? If so, do these present management challenges? Are you able to effectively patch these endpoints quickly should a zero-day threat need remediation?

Consider what happens if Microsoft releases a patch for a zero day vulnerability that is all over the news. How quickly can you gather information about patch status across the organization? If your CEO asks if this vulnerability will this affect the organization, can you provide an accurate answer within minutes? How long will it take to patch all your endpoints and be 100% compliant? Is it measured in minutes and hours, or days and weeks?

Is your organization spending a lot of time scripting and building out tools?

Typically, there is a lot of scripting in IT organizations, and most likely there is a lot of duplicated effort. Community driven content and asset sharing increases productivity and promotes a sense of community. The community may also be extremely helpful when fixing common IT issues when they inevitably occur. An open, sharing community can be huge benefit to an organization. Does your endpoint management solution have an open community of members who share assets and expertise? Does the vendor promote and support the community?

Additionally, is your IT organization creating and maintaining different scripts for multiple operating systems? How much time would be saved if a single script was consumable by various OS platforms? How much time would be saved and how much simpler would management be?

How do you patch 3rd party software? How much time is spent each month manually creating Adobe flash patches or a new version of Google Chrome? With BigFIx, 3rd party patching is provided for vendors like Apple, Adobe, Google, Java, etc. This content is provided out of the box and does not require you to purchase additional tools.

Is speed important in your organization when remediating security threats?

Once a threat has been identified, the time to respond is critical to mitigating substantial business impacts. Many organizations have been severely impacted due to exploited vulnerabilities and resultant data breaches. *The 2018 Cost of a Data Breach* Study, released by IBM and the Ponemon Institute, estimated the average cost of a data breach is $3.86M. If you cannot patch quickly after a vendor releases a fix, the risk exposure for substantial business loss grows rapidly. Effective patching is still, and will continue to be, one of the most effective ways to prevent and mitigate security incidents. In a worst-case scenario when reacting to a propagating threat, the ability to manage and perform remediation actions against your managed systems within a constrained time frame can prevent a major incident.

Do you have security standards and patch policies mandated by an internal security team or by a regulatory agency?

Although ineffective patching can present a security risk, configuration drift on workstations and servers can also create problems for IT organizations. Monitoring compliance is a growing challenge for many IT organizations. The Payment Card Industry Data Security Standard (PCI DSS) applies to all companies that accept, process, store or transmit credit card information and dictates that a secure environment be maintained. Regulatory fines for non-compliance can be substantial and range from $5,000 to $100,000 a month, depending on company size and the length and degree of non-compliance.

How often is your IT organization identifying and remediating non-compliance endpoints? Is your compliance process automated or manual? Is it a part of your endpoint management platform or is another tool/process required? Has your organization been fined or penalized for non-compliance? How much time does it take to aggregate information to report on endpoint compliance with mandated standards or benchmarks?

Can IT quickly respond to mergers and acquisitions?

With the changing corporate landscape, are you able to easily manage upcoming mergers and acquisitions with your current endpoint management software? Are you able to gather information about the newly acquired company using your current solution? Consider that BigFix is domain independent, and therefore could be used to develop your integration plan. With BigFix, information such as installed applications, application usage, hardware inventory, and patch compliance can all be gathered ahead of the migration so these assets can be quickly brought into compliance with the organization's security policy and standards.

What is your Total Cost of Ownership of endpoint management?

Have you computed the total cost of ownership (TCO) of managing your Windows, UNIX, Linux and MacOS endpoints? Have you included the direct and indirect costs of each tool including hardware, software, network, maintenance, engineering support and operations staff? How many disparate tools are you using today for patching, software distribution, inventory, OS deployment, remote control and security compliance? Have you computed the average, annual cost per managed endpoint?

Let HCL show you how to lower costs and improve operational efficiently by using a single, comprehensive, integrated, endpoint management platform – HCL BigFix.

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.

WX-10486 V1.0 White Paper