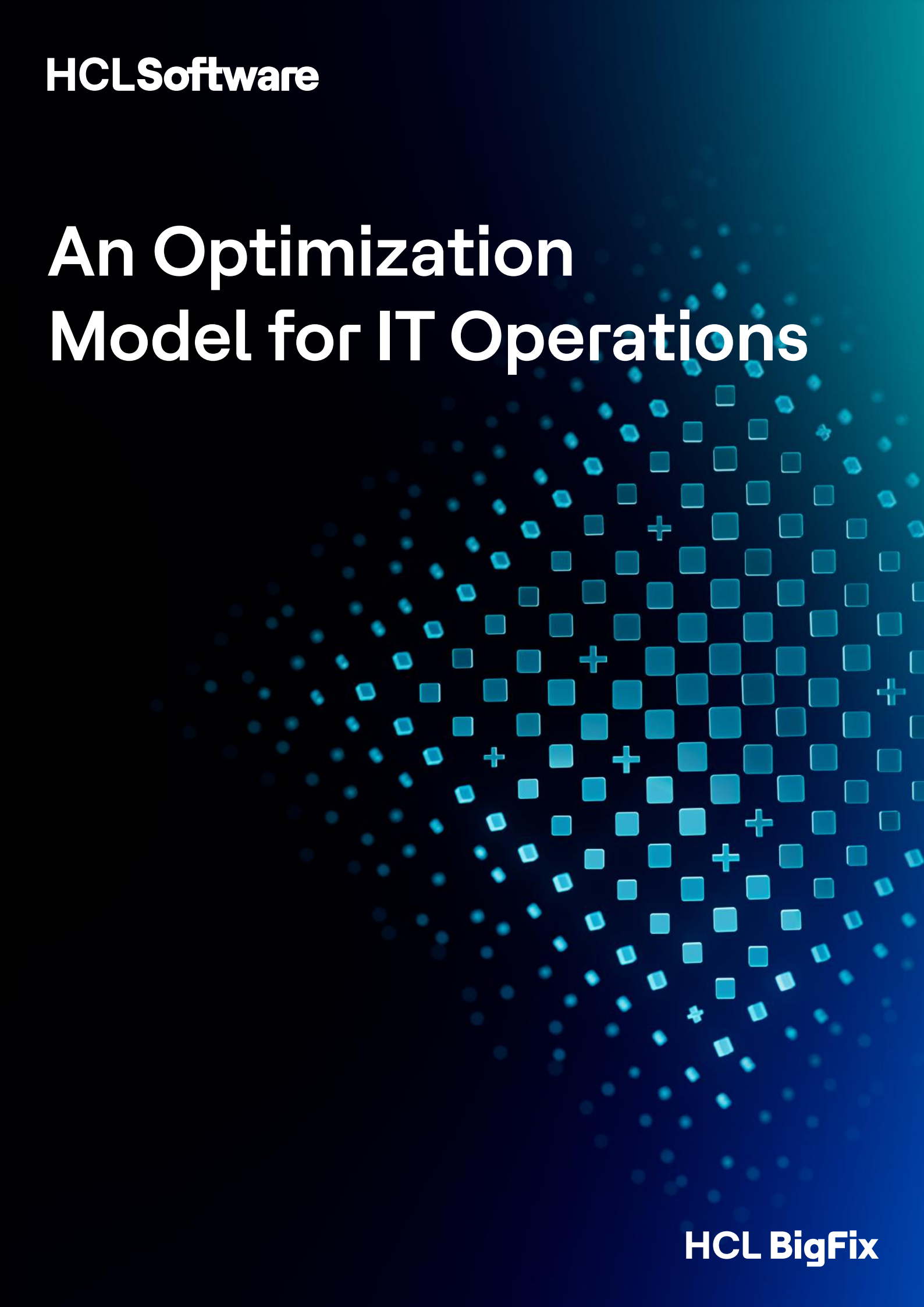
HCLSoftware

An Optimization Model for IT Operations



HCL BigFix

Overview

Optimizing IT Operations can be a challenging and complex area for organizations to manage. There is a constant need to ensure systems are up-to-date and fully secure, but it can be a difficult task to meet these demands. As organizations grow and their IT infrastructure becomes complex, it can be problematic to maintain visibility and control over all systems and devices. There is also a skills shortage in the cybersecurity industry. Compliance mandates cost millions for large organizations. And there is often a long remediation time to detect vulnerabilities.

New Challenge of 2023: Blocking Threats Before the Attack

60%

of breaches occur because a patch was available for known vulnerability but not applied

60 days

for an organization to remediate critical vulnerabilities

<15 days

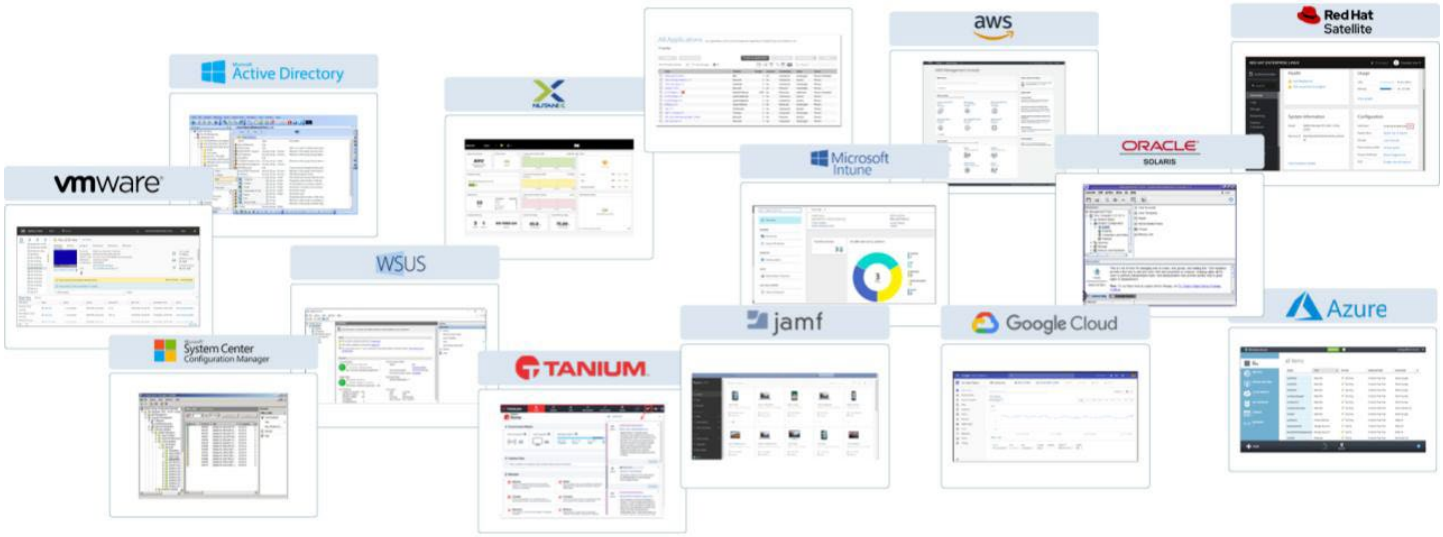
for attackers to exploit a discovered vulnerability

Mapping your place on the road to optimize IT operations:

Each enterprise is at a different place in their efficiency of their IT operations department. This could be due to organizational complexity, geographic distribution of teams, multiple acquisitions each with their own IT infrastructure, regulatory compliance requirements and more.

This paper proposes a working optimization model intended to provide operations team with a roadmap to greater efficiency, better security and lower costs.

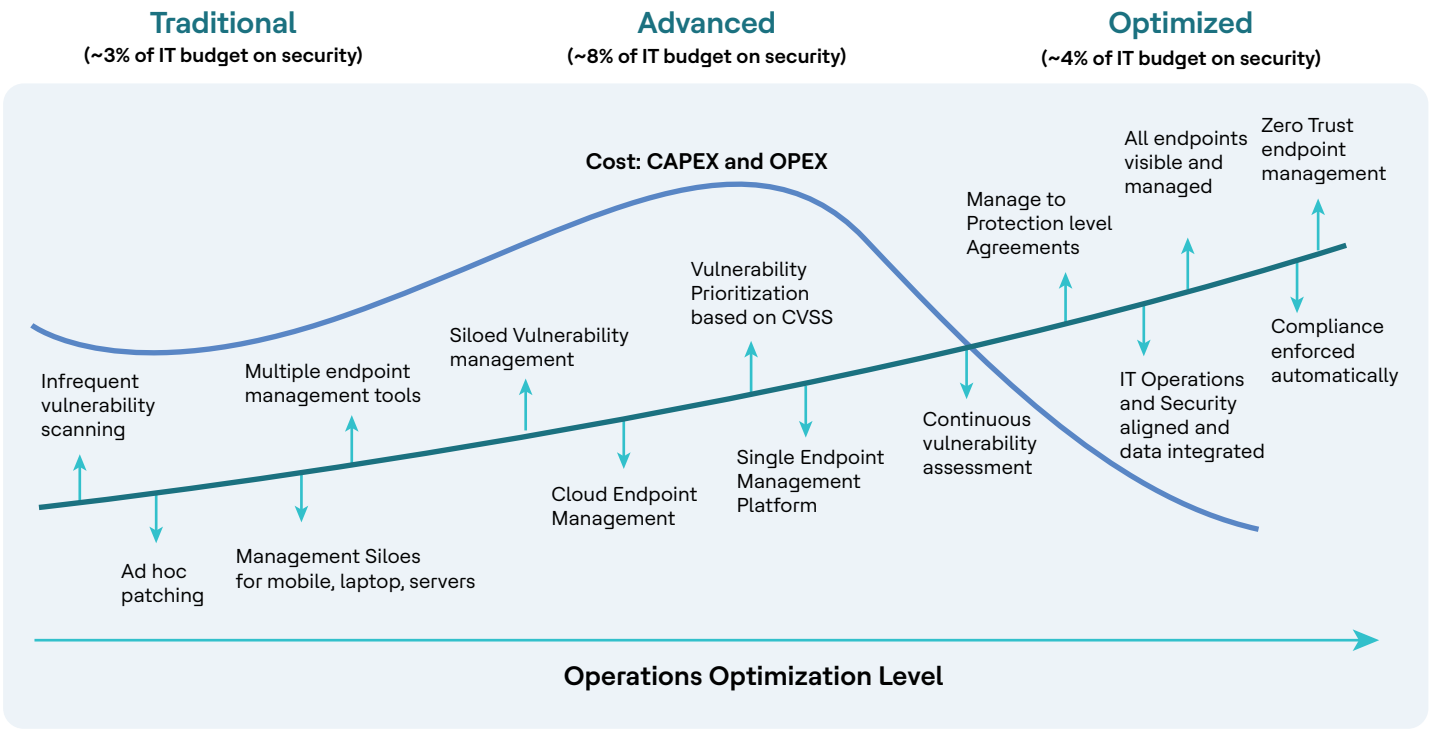
Technology Explosion Creates Complexity



- Every solution has an agent
- Every agent has a console
- Every console requires a server or cloud instance
- Every tool requires staff, training, maintenance, and support
- Where does it end? At what cost?

This is why an organization can greatly benefit from a structured approach to assessing their current level of maturity and identify areas of improvement that optimize IT endpoint security. The maturity model below describes three levels of maturity for managing endpoint security: Traditional, Advanced and Optimized.

Optimize Your **IT/Security Operations With Bigfix**



IT Operations Optimization Model depicts specific endpoint security processes that are typically associated with increasing levels of maturity. As organizations optimize endpoint security, their maturity level increases as shown in the chart above. Let's look at each level more closely.

Traditional: A traditional maturity level is characterized by the existence of many teams, many different tools, disparate processes, and limited – if any – coordination. IT teams are often using free or low-cost tools that only manage one OS and provide very basic security functions such as patching. In general, endpoint security is frequently viewed as an unavoidable but necessary IT process.

Advanced: The second level of maturity level is characterized by the recognition that endpoint security is a necessary task to protect the organization's assets and to ensure business continuity. It rises in importance from a "necessary evil" to an important IT function on which business operations depend. Related costs increase dramatically as more tools and processes are acquired and implemented to fill the gaps and deficiencies of basic tools initially deployed. An advancing organization focuses on improving patch hygiene and often struggles to remediate critical vulnerabilities quickly.

Optimized: The final phase of maturity is characterized by the implementation of best practices across the IT organization. IT moves beyond reacting to security issues to anticipating issues by automating patch and vulnerability remediation and ensuring that endpoints are continuously compliant. Organizations at this maturity level are also characterized by their recognition that endpoint security management is foundational to their success and to business continuity. By consolidating tools, reducing IT complexity, automating processes, and optimizing staff and IT processes, an organization can dramatically reduce the total cost of ownership. With optimized endpoint security, organizations can safely move workloads to the cloud, support employees working from home or traveling, and leverage modern and mobile devices.

TCO: There is a potential to reduce redundant tools and streamline processes while making IT operations team more efficient, hence reducing the total cost of ownership that your enterprise will experience.

Let's look at the model in a more granular way

In the chart below, the three broad maturity levels can be seen as six levels of maturity or steps toward optimization.

Optimized IT **Operations with HCL BigFix**

Traditional		Advanced		Optimized	
Level 0 **Non-existent**	**Level 1** **Scanning**	**Level 2** **Assessment and compliance**	**Level 3** **Analysis and prioritization**	**Level 4** **Attack management**	**Level 5** **Business risk management**
Visibility Many Endpoints are undiscovered	**Visibility** Vulnerability assessment performed by external party annually	**Visibility** Regulatory reporting requirements	**Visibility** • Emerging metrics and trends • Vulnerability scan data provided in spreadsheets to IT	**Visibility** • Attacker and threat focused • Multiple threat-vectors scanned and prioritized • Threat-triven metrics and trends	**Visibility** Visibility of all endpoints
Management • Ad hoc patching • No vulnerability scanning • Manual vulnerability assessments • No outbreak action plan	**Management** • Multiple endpoint management tools • Siloed processes for mobile, laptop and server	**Management** • Vulnerability management solution in place • Scheduled vulnerability scanning • Basic outbreak action plan	**Management** • Remediation with a risk prioritization model • Scan data prioritized through analytics • Measurable processes	**Management** • Patching based on risk to critical assets • Direct integration with vulnerability scanners and ITSM systems • Single tool and processes for user workspace and data center operations	**Management** • Every device and OS managed via single tool • Threat and risk aligned with business goals • Create and Manage to Protection level agreement • All threat-vectors scanned and prioritized
Standard support • No cloud security assessment • No Zero Trust endpoint management	**Standard support** No Zero Trust endpoint management	**Standard support** • Assessing Zero Trust endpoint management • Implement Microsoft Autopatch	**Standard support** Implementing some elements of Zero Trust endpoint management	**Standard support** Implementing Zero Trust endpoint management	**Standard support** • Automated, real time audit reports • Continuous compliance • Zero Trust endpoint management implemented

The model above decomposes the three levels of maturity (Traditional, Advanced and Optimized) into six more detailed levels (levels 0-5). These six levels will help you identify and assess your current IT operations more precisely and create a roadmap for advancing toward an optimized level of maturing and endpoint security. Within each of the six levels, the following three elements that characterize that maturity level:

Visibility refers to an organization's ability to monitor and understand the performance of their IT infrastructure, applications, and services in real-time, enabling quick and proactive identification and diagnosis of issues. For example, at level 0, an organization may lack any sort of monitoring tools or practices in place. As a result, they may be completely unaware of performance issues until they are reported by end-users or cause a major outage, while at level 5, the organization has achieved complete visibility and proactivity. They have fully automated monitoring and alerting systems that are integrated with their IT service management processes.

Management Controls refers to an organization's processes and procedures for incident, change and problem management. Effective management controls enable quick and efficient management of IT incidents and problems, minimization of their impact on business operations, and prevention of future incidents. For example, at level 0, an organization may have no formalized incident, change, or problem management processes in place. Issues are handled on an ad-hoc basis, and there is little to no documentation of incidents or problems, while at level 5, the organization has achieved complete management control maturity. They have well-documented, automated, and repeatable processes in place for incident, change, and problem management.

Measurement refers to an organization's ability to establish KPIs and other metrics to monitor and analyze the performance and effectiveness of their IT operations. For example, at level 0, an organization may have no established KPIs or other metrics in place to monitor IT operations. There is no way to measure the performance of IT operations, and there is no visibility into how well IT is supporting the business, while at level 5, the organization has a comprehensive set of KPIs and metrics that are aligned with business goals and objectives. They have established baselines for each metric and are continuously monitoring and analyzing performance to identify areas for improvement.

With this deeper and more granular understanding about the different maturity levels that IT Operations can exhibit along the continuum of IT Operations Optimization, specific steps can be identified to move toward the Optimized state at levels 4 and 5.

Map your own level of optimization

Add up your score and divide by 9 to know your level of optimization

Pillar	Security Posture	Score (1-5)
Visibility	Endpoint visibility (1=10% or more endpoints are not visible, 5= all endpoints visible and managed)	☐
	Vulnerability awareness: (1=assessment performed by external party annually, 3 = assessment done monthly or longer, 5= weekly assessment)	☐
Management	Number of endpoint management tools (1= 4 or more, 3= 2-4 tools , 5 = 1 tool)	☐
	Patching Program (1=ad hoc, 5 = risk based patching)	☐
	Vulnerability Management (1= no vulnerability scanning, 3= manual, 5 = integrated vulnerability with remediation	☐
	IT Operations SLA; (1= no SLA, 5= create and manage to protection level agreements)	☐
	Continuous Compliance (1= endpoints allowed to drift, 5= compliance enforced automatically)	☐
Compliance Support	Compliance: (1= ad hoc reports, 5= automated reporting for PCI, CIS, etc)	☐
	Zero Trust Architecture (1= no zero trust, 3= basic access control, 5= zero trust endpoint management)	☐

Summary

The Endpoint Security Maturity Model describes six levels of maturity from traditional to optimized. With this model, organizations can identify where they are on the continuum and identify areas of improvement that optimize IT operations. The model provides a roadmap that improves visibility, security, and the management of endpoints while enabling the measuring of endpoint compliance across all endpoints.

Analyze

Insights: Open Data Analytics Platform
Historical & Trend Reporting, Analytics

Discover Inventory

- Discovery and Enrollment
- Hardware and Software Inventory for over 100k titles

Compliance

Continuous Compliance and Patch

- PCI-DSS, DISA-Stig, CIS Compliance
- Eliminate Configuration Drift
- Software Lic Compliance Reporting

Vulnerability Remediation

Correlates vulnerabilities from Tenable and Qualysto bridge the Sec/Ops gap and reduce attack surface

Intelligent Automation

Fully automate operations for any endpoint

- Distribution
- Hardening
- Patch
- Compliance

Manage

- Desktop, Server, Cloud and Mobile
- End User Self-Service
- Remote Desktop Control
- Power Management

Integrate

- Integrations with 12+ Market Leading Products including
- ServiceNow, Tenable, Qualys,QRadar and more

With its breath of product offerings, HCL BigFix delivers an industry-leading unified endpoint management solution. BigFix allows IT security and operations teams to collaborate more effectively, reduces security risks, cuts operational costs, compresses endpoint management cycles, continuously enforces compliance, and improves staff productivity. With its broad range of capabilities, HCL BigFix can propel IT Operations to greater levels of efficiency and effectiveness optimizing all endpoint management functions.

Ready to advance endpoint security and management to the next level? We'll be happy to help you score yourself and get in touch with our experts to learn more about how HCL BigFix can help you optimize IT Operations and secure every endpoint. See where you stand on your journey to optimized IT operations. Contact us at info@hclfederal.com today.

HCLSoftware