IBM Endpoint Manager: Reaping the Benefits of a Unified Approach to Security and IT Operations Management

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for IBM

January 2012

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

IBM Endpoint Manager: Reaping the Benefits of a Unified Approach to Security and IT Operations Management

Table of Contents

Executive Summary 1

Security and IT Operations Management Depend on Each Other 1

The Reality: Divided by a Common Language 2

The Risks of Silos 3

Inadequate "Solution" Flexibility 3

The New World of Endpoints 4

The Limits of Scalability and Performance 5

Closing the Gaps: IBM Endpoint Manager 5

Flexible Endpoint Capability + Adaptability = Management at Scale 5

Benefits 6

"Future-Proofing" Endpoint Management 7

Success Stories 7

Optimizing Security Management for a Global Retailer 7

IBM Takes a Page from Its Own Playbook 8

EMA Perspective 9

About IBM 9

©2012 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

IBM Endpoint Manager: Reaping the Benefits of a Unified Approach to Security and IT Operations Management

Executive Summary

Today's endpoint management challenges have rarely been greater. Enterprise IT is undergoing a generational transformation as mobile devices – those owned by the business as well as personal devices brought into the enterprise – are overhauling long-held understandings of what "personal system" means. With the rise of virtualization and Cloud Computing, the notion of where the endpoint may be found now includes not only "classic" endpoints like workstations and laptops, but mobile devices and the data center as well – on-premises as well as environments hosted by third parties.

IT innovation is not the only challenge facing endpoint management. Attackers recognize that the endpoint is often the weakest link in security strategy, where the challenges of highly distributed management coupled with often inadequate security coverage increase risk. The sheer growth in the volume and sophistication of threats amplifies the need for more effective security, at the point where IT intersects with human factors most directly.

Never before has there been such a need for a unified approach to the shared concerns of security and IT operations management. Endpoint management systems are often the first line of defense when it comes to vulnerability remediation – yet this process itself requires the participation of both security *and* IT operations management, to match vulnerability intelligence with needed endpoint change. Sadly, far too many organizations fail in answering this challenge. The silos that keep security and IT operations technologies from responding effectively to security threats make it difficult for organizations to mount a proactive defense. They also create needless redundancies in systems that do fundamentally the same thing, and introduce gaps in mismatched coverage. Paradoxically, some of those who have the greatest resources for tackling the problem often suffer the worst, stymied by the inability to scale an effective approach.

In this report, ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) analysts examine IBM Endpoint Manager as an answer to these problems, which merits the label of "solution" far better than many others on the market do. IBM Endpoint Manager's combination of strong endpoint capabilities coupled with the flexibility of a highly adaptable, distributed processing architecture unifies the common objectives of security and IT operations management. Two successful customer use cases demonstrate the efficiency of IBM Endpoint Manager that enables a striking degree of scalability for some of the world's largest, most complex IT environments, while also successfully scaling down to small and medium-sized organizations. Businesses will gain an appreciation for the benefits of an approach that offers both greater efficiency and effective control over one of the most dynamic landscapes in IT: where the changing nature of the IT endpoint meets today's security challenges head on.

Security and IT Operations Management Depend on Each Other

Security often depends directly on the disciplines of IT operations management. Attackers directly exploit software and configuration exposures in order to gain access to high-value information assets. Remediating these exposures means more than software update or system reconfiguration. Organizations must have a consistent and reliable approach to IT operations management to assure that exposures are consistently controlled and, where possible, eliminated. They must also have the agility to react swiftly to emerging or previously unseen threats such as zero-day attacks. This class of threat may require organizations to respond with any number of remediation techniques – from rapid

©2012 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

deployment of workarounds to quarantine of affected systems – as fast and reliably as possible. When minutes count, typical patching or reconfiguration processes may not be up to the task.

Likewise, IT operations management benefits from the disciplines of security. A consistent, proactive and reliable approach to threat prevention and control over unauthorized or malicious change does more than strengthen IT against adversaries. It also introduces a discipline in IT management that constrains a key contributor to system instability, promoting greater reliability and better performance. It also limits support requirements and helps keep IT operations out of perpetual "firefighting" mode.

When organizations can take advantage of management disciplines that benefit both security and IT operations priorities, the rewards may go beyond increased efficiency alone. For example, in one EMA study of more than 200 respondents worldwide,[1] those who achieved these four IT change management milestones:

- Defining their change control processes
- Actually implementing those processes in practice
- Monitoring their environment for unexpected or unauthorized change, and
- Responding when deviations were detected

also reported half the median incidence of security events requiring an unplanned response compared to all others in the study – but that's not all.

This group also reported:

- A lower median incidence of unplanned IT work
- Generally higher server-to-system-administrator ratios
- A higher median rate of IT projects completed on time, within budget, and with expected features

than other respondents in this research.

Sadly, these high performers – who practice a number of other management disciplines that support both better security and improved IT operations management – represented only a fourth (23%) of all those studied. What does this say about those who make up the majority – not only of respondents in this research, but also of organizations generally?

Security and IT operations teams alike often share the same goals for system control, and may look to the same or similar tools to achieve those goals. Far too often, however, they find themselves confounded by the limitations of many current approaches.

The Reality: Divided by a Common Language

Those who fail to capitalize on techniques that benefit both security and IT operations management sometimes reflect G. B. Shaw's impression of the world of English speakers: "divided by a common language." Security and IT operations teams alike often share the same goals for system control, and may look to the same or similar tools to achieve those goals. Far too often, however, they find themselves confounded by the limitations of many current approaches. For example:

[1] *IT Risk Management: Five Aspects of High Performers that Set Them Apart*, EMA Advisory Note, July 2011.

The Risks of Silos

One of the most common limitations is the "siloing" of management tools that serve essentially the same function, but exist in different domains (such as operations and security). Often, organizations fail to question these redundancies. They may have legacy solutions in place that have grown up from different backgrounds or serve different purposes. Antivirus systems have produced their own tools for deploying signatures throughout an enterprise, while systems management platforms have long been used to distribute application or OS updates and configuration changes across a wide range of endpoints.

But does a longstanding legacy mean that the redundancy of these silos is actually necessary? More significantly still: Can maintaining these silos actually cause harm?

It may not take much to realize that these overlaps may duplicate costs – in terms of management processes as well as technologies – for what is essentially the same thing, as in the case of software distribution, regardless whether for antivirus signatures or software updates. Also consider the *gaps* that silos introduce. For example, when an emerging security threat first becomes known, it may take far too long for IT operations management tools to prepare a software update to remediate an exploited vulnerability.

In the meantime, organizations may be able to limit or eliminate their exposure through system reconfiguration or the deployment of updated threat signatures to security tools – if their tools can support the needed change quickly and efficiently. In reality, one system may cover endpoint security; another may address system change or software distribution, with mismatches in coverage producing overlaps as well as gaps. Not only may these tools be redundant, they may also fail to work effectively in sync, or add significantly to support costs when processes must be devised to compensate each and every time. The net result is that organizations subject to the risks of siloed management tools may too often be left with no consistent, centralized idea of just how effective their response to an emerging threat may be, particularly if it requires a coordinated response from both security and IT operations management.

Consider, for example, the case of a zero-day attack that exploits a specific Dynamic Link Library (DLL) file. DLLs are often targeted, since an operating system will load a DLL on demand to meet a specific functional need. When exploited, the OS may not be able to distinguish a malicious DLL from the legitimate file it replaces, and may execute an attack as a result. If an organization can rapidly determine which endpoints have a targeted DLL, it could quickly determine how long remediation will take, what will be involved, and help determine the overall risk to the business.

Inadequate "Solution" Flexibility

The problem is exacerbated by the fact that many management tools do not make it easy – or in some cases even possible – to break down these silos. Security tools are not typically well purposed to manage system configuration or the challenges of software distribution beyond signature update, for example. Conversely, IT operations management tools may not be designed to manage security technologies or distribute security updates in ways directly consumable by security tools. In addition, many security tools are designed primarily for scanning or monitoring, but not for remediation. IT operations tools may be better suited for remediative tactics such as system change or software distribution, but are not as well purposed for vulnerability assessment or reporting.

> The problem is exacerbated by the fact that many management tools do not make it easy – or in some cases even possible – to break down these silos.

©2012 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

These inflexibilities call into question the very use of the term “solution” when used to describe siloed tools, given their inability to address a wider range of concerns shared across security and IT operations management. If these difficulties exist today, imagine what they mean for IT tomorrow.

Consider, for example, that among government agencies as well as many forward-thinking enterprises, compliance with the Security Content Automation Protocol (SCAP)[2] is becoming a requirement for IT management tools used in vulnerability remediation. This means the integration of security awareness with IT operations capabilities for remediating exposures in every affected system quickly, across an entire organization. In other words, SCAP is an initiative that seeks to break down many of the very silos and gaps described earlier. Legacy tools, however, may require considerable adaptation to become SCAP-ready (if they can be adapted at all), and will require ongoing updates to maintain currency as technology changes are reflected in SCAP specifications. These factors may complicate efforts to respond to requirements for consuming and integrating SCAP-compliant content and add to their overall cost.

The New World of Endpoints

The emergence of a new class of endpoints in the enterprise poses even greater challenges for tools that seek to unify the common objectives of IT operations and security management. The growing capabilities of today’s personal devices have gone well beyond the concept of the “smartphone.” But many tools for managing both security and IT operations demands are not yet well prepared to embrace these new endpoints, despite the majority of enterprises that prefer Mobile Device Management (MDM) capabilities to be either included with an enterprise IT management platform or integrated with third-party management tools, as documented in recent EMA research.[3]

The emergence of a new class of endpoints in the enterprise poses even greater challenges for tools that seek to unify the common objectives of IT operations and security management.

The issue is further exacerbated when personnel are allowed to use their own personal devices in a “bring your own” environment. According to the EMA research cited above, 37% of mobile devices in enterprises of more than 10,000 employees are Apple or Android systems – a figure that increases to 50% in businesses of 500 to 10,000 employees, and 70% among smaller organizations. Across all organizations surveyed, approximately half of these Apple and Android devices are personally owned by individuals rather than by the business.[4] Clearly, “BYO” is becoming a reality for personal business computing.

These factors raise the bar considerably for the capabilities enterprises will expect from their IT operations management platforms – particularly when it comes to security. When EMA asked more than 200 organizations about the MDM capabilities considered most important, data security and device security were rated “extremely important” by 72% and 60% of respondents, respectively.[5] This suggests that the comprehensive IT management systems businesses will prefer tomorrow will not only require significant MDM capability, but the ability to define and enforce security measures as well.

Even more daunting for the future may be the increased penetration of intelligence into systems and assets not typically considered part of “enterprise IT” today. This includes a growing number of

[2] http://scap.nist.gov/

[3] Enterprise Mobile Device Management: How Smartphone and Tables are Changing Workforce IT Requirements, EMA Research Report, October 2011, p. 22.

[4] Ibid., pp. 5-7.

[5] Ibid., p. 26.

smart monitoring, metering and control systems for environments from public utilities to healthcare, manufacturing, transportation, and many more. The extent to which these environments intersect with more conventional IT may define the requirements for both IT operations and security management systems of the future.

The Limits of Scalability and Performance

As it is today, many current solutions have more than enough difficulty navigating the terrain of "now." The truly distributed enterprise must often deal with networks throughout the world that may vary widely in performance and response, from high-bandwidth site-to-site links to constrained – and perhaps uncertain – connections for remote or field offices or personnel. The inability of management tools to "four-wheel" safely over these challenging environments, or the public Internet, can have significant consequences for the business. Delay in response to emerging security threats, or gaps that leave organizations uncertain if endpoints are protected, can leave significant parts of the enterprise vulnerable to damage or loss. Regulatory mandates often require "continuous" compliance, in part because of such concerns. Businesses unable to respond quickly and consistently throughout their operations may find themselves more exposed than they realize.

The distribution and diversity of enterprise IT is often a consequence of scale. Larger enterprises typically face the need to manage hundreds or thousands of endpoints, regardless of where they are located or how diverse they may be. (Indeed, the automation of swift and effective response to complex security management demands at scale is one of the manifest intentions of SCAP.) But organizational size can cause significant problems when response to emerging issues must be swift – or even timely. Management tools that do not scale well may choke network bandwidth or system resources required for business priorities, while driving the total cost of ownership for those tools very high. Those that do not embrace real diversity can cause as many problems as they solve if they are incompatible with the range of systems actually found throughout the organization. The overlaps and gaps created by siloed security and IT operations management tools can exacerbate these problems, inhibiting the ability of the large, complex or diverse enterprise to consistently meet its IT operations and security management demands.

> Organizational size can cause significant problems when response to emerging issues must be swift – or even timely. Management tools that do not scale well may choke network bandwidth or system resources required for business priorities, while driving the total cost of ownership for those tools very high.

Closing the Gaps: IBM Endpoint Manager

With a distinctive approach to flexibility that breaks down these longstanding barriers, IBM Endpoint Manager offers businesses a way out of these confines of the past.

Flexible Endpoint Capability + Adaptability = Management at Scale

IBM Endpoint Manager is differentiated by its combination of a wide range of functionality at the endpoint and "Fixlets" that direct actions and tasks from a centralized management server. Fixlets are discrete, authenticated policy messages that can be adapted to virtually any management need – from software distribution to change management, policy enforcement, or highly granular monitoring and data collection, meeting both security and IT operations demands. IBM Endpoint Manager also has a highly distributed content distribution mechanism that utilizes "relays" installed on existing

IT resources such as messaging or directory servers. Relays enable the distribution of relevant content (such as patches) closer to the endpoints, increasing scalability while decreasing network overhead.

The combination of extensive endpoint functionality and the flexibility of the Fixlet concept enables a much more distributed and simplified architecture – and this means scalability. Large enterprises report more economical and efficient management of hundreds of thousands of endpoints with IBM Endpoint Manager: up to 240,000 in the case of one global retailer. At IBM itself, the company deployed IBM Endpoint Manager on more than 500,000 endpoints within six months, with plans to manage hundreds of thousands more. (These deployments are described in more detail below.)

With IBM Endpoint Manager, the combination of extensive endpoint functionality and the flexibility of the Fixlet concept enables a much more distributed and simplified architecture – and this means scalability.

Benefits

For security requirements that depend on timely and efficient IT operations management, IBM Endpoint Manager delivers an end-to-end approach. A single unified console enables visibility throughout the environment that correlates vulnerability intelligence to the detailed configuration of each endpoint. This gives organizations an immediate, up-to-date and accurate view throughout their operations essential to assuring continuous compliance demands.

This same system also enables the remediation of security exposures, as well as the ongoing maintenance of security and compliance requirements. Role-based access to IBM Endpoint Manager functionality enables organizations to maintain separations of duties in security and IT operations management processes, giving security teams the monitoring, oversight and advisory capability they require while protecting IT operations from unauthorized control.

The adaptability of IBM Endpoint Manager suits it well to meeting fast-changing security demands. For example, when an emerging threat requires immediate insight into the exposure of endpoints, individual IBM Endpoint Manager agents can be designated as relay or discovery points within minutes. This enables local collection of critical data from surrounding endpoints, and the staging of information relay toward management centers. This not only supports scalability and faster response, but also increases efficiency by leveraging existing infrastructure. It also provides built-in redundancy that helps assure coverage where many other systems fail – systems that cannot call on such adaptability on demand.

A truly unified solution breaks down the silos of past approaches, enabling organizations to reap the benefits of greater efficiency. IBM Endpoint Manager delivers these benefits by not only enabling typical endpoint operations relevant to security such as software distribution or configuration management, but also the direct management of endpoint security functionality. IBM Endpoint Manager can be used as the management console for endpoint antivirus and host intrusion prevention systems, as it is for many organizations worldwide. It can distribute antivirus signatures as well as patches and system updates required for security. It can enforce change controls that help prevent malicious changes due to malware or other security threats. These capabilities reduce costs by eliminating redundancies that create overlaps as well as gaps in siloed legacy tools, and assure consistency of coverage across a broad spectrum of security and IT operations requirements.

"Future-Proofing" Endpoint Management

Because IBM Endpoint Manager is so adaptable, it is well positioned for meeting the demands raised by the rapidly changing nature of the endpoint in the enterprise.

The flexibility of Fixlets enables IBM Endpoint Manager to perform any function supported by the endpoint agent. For mobile devices, this means expanded capability for tracking device inventory, setting security policy, managing the application complement, placing constraints on unauthorized applications, and assuring protection for sensitive data in the event of the loss, theft or other compromise of mobile endpoints.

The adaptability to any supported endpoint also means that IBM Endpoint Manager is also well suited to help enterprises capitalize on Cloud Computing opportunities such as the promise of Infrastructure-as-a-Service (IaaS). One of the greatest barriers to Cloud adoption is the lack of visibility and control over hosted or third-party environments such as the public Cloud. Instrumenting endpoints in the Cloud with IBM Endpoint Manager can help overcome these concerns, giving organizations needed visibility and control for Cloud environments and centralizing management with on-premises IT.

These examples suggest how the flexible adaptability of IBM Endpoint Manager can help organizations better prepare for what may come next for IT, regardless what it may be. As "smart" systems such as utilities, transportation, logistics, or supply chain technologies continue to advance, the adaptability of IBM Endpoint Manager may well become a valuable asset as enterprises seek ways to leverage their existing management investment and increase efficiencies through a unified platform.

Success Stories

The advantages of IBM Endpoint Manager are best illustrated by examples that highlight the efficiencies of this comprehensive, adaptable and highly scalable management system.

Optimizing Security Management for a Global Retailer

In one such case, a global retailer's IT security organization recognized that current methods for distributing patches and security updates were inadequate. In particular, visibility into which systems had successfully been updated and which had not was inconsistent or absent in some cases, posing compliance as well as a security risks if the organization could not be certain about its exposure. Existing tools could only inform the organization when an update had been distributed – but not if it had been successfully deployed.

The adaptability of IBM Endpoint Manager enabled the security organization to introduce the platform to serve its requirements for greater visibility into endpoint security. Since its adoption, it has also become a tool to assure comprehensive delivery of systems updates and authorized changes, with divisions of responsibilities between security and IT operations defined in the deployment.

This retailer has realized a savings of approximately $1.2 million per year from the ability to manage endpoint security requirements that previous tools were unable to meet. Because IBM Endpoint Manager is, as this organization describes it, "client-driven" ("That's where all the intelligence is," says one representative), the company is able to

IBM Endpoint Manager has enabled one global retailer to realize a savings of a savings of approximately $1.2 million per year from the ability to manage endpoint security requirements that previous tools were unable to meet.

©2012 Enterprise Management Associates, Inc. All Rights Reserved. | www.enterprisemanagement.com

manage more than 240,000 diverse endpoints with only a single IBM Endpoint Manager server. Better management of software licenses is another advantage enabled by the IBM platform, which provides the visibility needed to know when and where licenses are in use, where they are not, and where licensing costs can be reduced accordingly.

IBM Endpoint Manager has also helped this organization to meet compliance demands, such as the need to deploy specific applications to meet compliance requirements. In one such case, the company's previous system was only able to deploy a certain application to no more than 70% of target endpoints, and was unable to get beyond that limit. Once IBM Endpoint Manager was in place, the company was able to deliver this application to 95% of targets within three weeks, after trying for "months" with the previous solution, according to project personnel.

IBM Endpoint Manager also enables this organization to build, customize, deploy and enforce security policies based on widely accepted guidance such as that arising from the Federal Desktop Core Configuration (FDCC) mandate or Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). The flexibility of IBM Endpoint Manager is particularly called out by this company, who also points to the ability to re-use existing content in adapting Fixlets to the requirements of a specific organization.

IBM Takes a Page from Its Own Playbook

Among the large organizations who value these capabilities of IBM Endpoint Manager is a hundred-year-old Fortune 50 enterprise that is one of the largest, most complex and distributed corporations in the world: IBM itself.

IBM faced a serious issue in assuring control of vulnerabilities throughout its global IT environment. Issues such as patch latency (the time it takes to deploy security patches once a vulnerability is known) were increasing exposure to security threats. The need to assure continuous compliance with internal security policy (as opposed to periodic "snapshots" that could mask exposures in between assessments) was also a factor motivating investigation of alternatives.

Within six months, IBM had deployed IBM Endpoint Manager on more than 550,000 endpoints worldwide – "the largest and fastest internal client deployment within IBM's history," according to the company's own documentation of the effort.

In making an objective assessment, IBM explored third-party alternatives as well as IBM Endpoint Manager. When a pilot study demonstrated an estimated 50% savings in endpoint support, the company determined to deploy IBM Endpoint Manager on its own systems. Within six months, IBM had deployed IBM Endpoint Manager on more than 550,000 endpoints worldwide – "the largest and fastest internal client deployment within IBM's history," according to the company's own documentation of the effort.[6]

While the deployment has served primarily to optimize patch management for the company's widely distributed endpoints, IBM has also used IBM Endpoint Manager to gather detailed and highly granular intelligence on changes to vital system components such as Dynamic Link Libraries (DLLs) and registry entries that can directly indicate an attack. With previous solutions, IBM had to gather each condition individually and correlate results manually. With IBM Endpoint Manager, complex endpoint

[6] IBM deploys Tivoli Endpoint Manager internally, IBM white paper, November 2011.

intelligence queries can be gathered within minutes to determine which, if any, endpoints may be at risk for a new security threat. Says David Merrill of the company's Chief Information Security Office, "IBM Endpoint Manager is flexible enough that we can use it to deliver control technology for just about any problem."

EMA Perspective

High-performing organizations have demonstrated the value of a unified approach to security and IT operations management. They recognize not only the value but also the need for an integrated approach, when IT operations management is required for essential security measures such as vulnerability remediation, environmental monitoring, and safeguards against malicious IT change. Those who succeed reap benefits beyond security or IT operations management alone. EMA research demonstrates that a truly unified approach pays off in benefits to the business, through increased efficiency, lower rates of unplanned work, and reduced support costs.

In recent years, the need for a unified approach has gone from an advantage for forward-thinking organizations to a necessity for all. Growth in the sheer volume and sophistication of threats demonstrates the need for constant vigilance over the distributed endpoint environment; regulatory requirements increasingly demand it. Attackers know the endpoint is the weakest link in many enterprises, given the challenges of distributed management, human interaction, and the growing diversity of endpoint devices. Organizations can no longer afford to tolerate significant gaps in their endpoint security strategy.

With the availability of platforms such as IBM Endpoint Manager, businesses have a richer set of capability for answering today's more challenging demands, from traditional desktops to a growing number and diversity of mobile devices and non-traditional "smart" endpoints. IBM Endpoint Manager is a strong example of a management platform that better integrates security and IT operations processes across this variety of endpoints while preserving the integrity of each. IBM Endpoint Manager's combination of wide capability coupled with the highly adaptable Fixlet concept enables more than high scalability. It also gives enterprises a powerful set of tools to perform virtually any function at the endpoint necessary for managing a fast-changing landscape of endpoint systems as well as threats. As businesses contemplate a future for IT that may be significantly different from the past, those that rely on IBM Endpoint Manager may find themselves well prepared for unifying the challenges of today with a toolset that gives them an excellent footing for what may come tomorrow.

About IBM

Tivoli software from IBM helps organizations efficiently and effectively manage IT resources, tasks and processes to meet every-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce cost. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT lifecycle management, and is backed by world-class IBM services, support and research. For more information on Tivoli software from IBM, visit: ibm.com/tivoli. For more information on IBM Endpoint Manager, visit: ibm.com/tivoli/endpoint.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter or Facebook.

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2012 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com
2402.012412