The 7 Best Practices for Resolving Emerging Challenges in Unified Endpoint Management

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

April 2017

EMA™
IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Executive Summary

Information technology (IT) advances and evolving enterprise requirements are changing the businesses utilization of computing resources. Lifecycle management processes needs to evolve as well to meet rising adoption of business-critical IT requirements for workforce mobility, virtualization, reliable software delivery, and increased infrastructure complexity. In order to face these emerging challenges, organizations must be armed with processes and automation solutions that will deliver the agility and extensibility to maintain performance and reliability without sacrificing cost-effectiveness in IT investments.

The New Lifecycle Management Paradigm

The history of IT is segmented by periods of fundamental transition when processes and technologies evolve to meet rapidly expanding enterprise productivity requirements. This was certainly the case in the past with such dramatic advances as the introduction of the mainframe and the advent of the PC revolution. Fundamental changes in technology are inevitable as development breakthroughs occur and organizations that rise to embrace IT advances are better positioned to compete against those that do not. A recent convergence of new technology introductions has ushered in a new period of transition that will fundamentally change the way we utilize and manage IT resources.

A recent convergence of new technology introductions has ushered in a new period of transition that will fundamentally change the way we utilize and manage IT resources.

Today's businesses require greater agility, high-availability, and customization of supported IT services. Enterprise personnel expect services to be eminently available "on-demand" and, indeed, require prompt access to critical applications and data in order to respond to rapidly changing market conditions. Modern users also have developed very specialized requirements for their IT resources to address the unique challenges of each of their particular business roles. This, in turn, requires more customizable IT implementations with a focus on meeting end-user needs and preferences. Rising to the challenge of delivering a wide variety of reliable IT services on-request has led to the development of new technology concepts such as virtualization, mobilization, and cloud solutions. As these emerging technologies grow in adoption methods for delivering, monitoring and managing them must also evolve to meet expanding requirements.

Traditional methods for managing IT resources, including servers, desktops, and laptops, are the core precepts of lifecycle management. Put simply, lifecycle management encompasses all the endpoint management processes necessary to ensure systems meet business requirements from their initial deployment through their final retirement. A number of disparate management services comprise lifecycle management. The most critical of these include: system deployment, application provisioning, patching, change and configuration management, security and compliance, problem and incident management, and backup and disaster recovery. Because of the breadth of administrative tasks required for these individual services and the extensive number of endpoints managed by typical medium and large-sized organizations, support for lifecycle management cannot be achieved by manual process alone. Automation is essential to the successful delivery of lifecycle management support. Fortunately, a number of automated management solutions are available in the market today. Many of these are point solutions only designed to address one or a few endpoint management challenges. More effective, however, are automated suites that provide a broad range of automation service to achieve the breadth of lifecycle management requirements.

Until recently, traditional lifecycle management practices and automation solution suites were adequate to achieving enterprise IT support goals. However, the evolution of IT processes to providing more dynamic resources has outpaced the ability of traditional solutions to support them. Traversing the gap between traditional practices and emerging challenges requires the adoption of new concepts for enhancing lifecycle management processes.

Evolving IT Management Challenges

Increased complexity lies at the heart of emerging IT management challenges. As organizations increase the breadth of their services, infrastructures become proportionally more difficult to manage. Applications and other IT resources, for example, are not just delivered from physical servers, but can also be hosted on virtual or cloud environments. This creates multiple levels of abstraction for hosted services that may be difficult to monitor, maintain, and ensure ongoing performance on, and existing management tools may not directly provide support for these alternative environments. Here are some of the more significant emerging management challenges IT organizations are facing today:

Expanding Workforce Mobility

Increased complexity in IT infrastructures derives directly from expanding endpoint requirements. Nowhere is this more evident than with the increased reliance on IT support for workforce mobility. Enterprise employees are increasingly requiring remote access to business IT resources. Any critical data accessed outside the controlled environment of the office facilities by remote devices (such as laptops or home desktops) introduces risks to the business due to the release of sensitive information and may result in an inability to meet regulatory compliance objectives. Management of remote systems is also extremely challenging as IT support's connectivity to the endpoints is not persistent. Patch updates, for instance, are often only performed when target systems are network accessible, and the longer the delay for patch installations, the greater the chance of environment failures and security breaches. In addition, the inability to immediately update endpoints with configuration changes increases the chances the endpoints will drift from established baseline standards. When failures do occur, IT administrative staffs have no way of accessing the remote systems and often must resort to talking inexperienced users through resolving their own problems, significantly impacting user and administrator productivity.

Bring Your Own Device Programs

The increased adoption of "Bring Your Own Device" (BYOD) programs where organizations finance the purchase of employee-owned workstations (either in whole or in part) has only exasperated the challenges with supporting workforce mobility. Since organizations have limited control over employee-owned devices, the lines are blurred as to whether the business or the end user is responsible for management. Enterprise IT support, for instance, may not be able to enforce the use of software agents and monitoring tools on employee-owned endpoints – which even further increases security and compliance risks.

Increased Virtualization Adoption

Whether the endpoint is remote or local, increased adoption of virtualization technologies also introduces a host of new management challenges. Since each Virtual Machine (VM) is abstracted from the physical host server, both layers must be managed independently as well as the virtualization platform itself. For example, with the most popular form of desktop virtualization, Virtual Desktop Infrastructure (VDI), a separate VM is created for each end-user environment, but with common core operating system and/or licensing elements hosted on a single physical server. When a new patch or update needs to be installed, traditional methods would require the update to be provisioned to each individual VDI VM, which will significantly (and unnecessarily) hamper both CPU and I/O performance of the virtualization server since all the installs will be running simultaneously on the same physical system. Additionally, since provisioning of a virtual desktop is easier and less expensive than physical endpoints, it is not uncommon for multiple new VMs to be enabled and abandoned without deletion. This leads to "VM sprawl," dedicating valuable virtualization resources on unused VMs.

Endpoint Migration

Transitioning end users from one environment to another, such as between physical to virtual desktops or to new OS versions, offers additional difficulties. Applications need to be compatible in the new environment and all dependencies must be accommodated. A consistent user experience also needs to be maintained in order to prevent productivity loss. This is particularly true with OS changes, such as when migrating from Windows XP to Windows 7 or migrating to Windows 10, since configuration elements must be mapped to new locations and the environment will likely be unfamiliar to migrating users.

Lack of Software Standardization

Software delivery and updating can also be an arduous task as different and changing end user requirements often make standardization of applications difficult. When endpoint configurations lack consistency, the chances are increased for software conflicts and a reduction in application performance.

Management Tool Sprawl

Enterprise reaction to increased complexity from changing requirements is commonly to fill gaps in existing management services with point products specifically designed to address the missing support coverage. This "band-aid" may offer some temporary relief, but the use of multiple management solutions can significantly degrade administrative performance. The reliance on multiple management interfaces, for instance, can result in "swivel-chair management," where administrators must manually switch between a variety of windows to correlate events and perform management tasks. This significantly reduces IT support's ability to perform root cause analysis on environment problems. Additionally, the use of multiple management tools that are not fully integrated can themselves impact the performance of the endpoints they are supposed to be supporting. Multiple agents can reduce endpoint system performance, and the data transfer of monitoring and system information to multiple data collection points can adversely impact network performance. Instead, a more holistic approach should be adopted where integrated processes and automated tools unify endpoint visibility and administrative procedures.

Best Practices for Resolving Emerging Challenges

The path to reducing challenges from evolving IT requirements begins with the simplification of management processes. Included below are process improvements that will dramatically reduce management difficulties and increase enterprise productivity.

Consolidated Management

Multiple management platforms should be consolidated onto a single unified and fully integrated solution set that utilizes a single-pane-of-glass interface for supporting all physical and virtual endpoints. Continuous monitoring of the supported stack should be performed to identify new endpoints and changes to existing asset configurations. This asset and configuration information should be recorded in a centralized data repository or, ideally, in a federated Configuration Management Database (CMDB) to provide a single source of truth about the inventory and state of the support stack. A unified management interface will enable a holistic view of the infrastructure, simplifying administrative activities across multiple lifecycle management disciplines.

Standardize Processes and Monitor for Compliance

Management efforts are further eased with the standardization of processes and endpoint configurations. When managed systems utilize a common baseline configuration that is known to function optimally, it is easier to target potential problems by identifying any conditions that are not aligned with these standards. Additionally, by maintaining consistent administrative practices, supported systems are less likely to drift from established baselines. All endpoints should be monitored to determine if they have fallen out of alignment with configuration standards. This enables proactive problem identification so that incidents can be resolved before they become business impacting, breaking the cycle of systemic reactive "firefighting." When problems do occur, standardized configurations and holistic environment views provide the key resources that enable prompt and effective root cause analysis. Support stack reliability is further enhanced with continuous malware detection and regular data backups.

Introduce an End User Self-Service Portal

The use of an end-user self-service portal can significantly reduce IT support effort by allowing end users the ability to initiate application downloads and service requests with little or no administrator interaction. This also allows end users the ability to select which applications they require and avoid the provisioning of licenses they don't need. In this way, baseline endpoint configurations can be customized to meet unique user requirements without incurring excessive time and effort from operational support staff.

Enable Remote Management

Any difficulties with managing remote systems should also be addressed, beginning with the establishment of organizational policies necessitating any device used for business purposes to conform to specific enterprise IT management and security requirements. Put simply, if end users want to access business data, applications, and services, they must be willing to allow monitoring, maintenance, and security processes to operate on their systems, even if those endpoints are employee-owned. Automated management tools for patching, configuration, and security enforcement should be able to operate off-line, ensuring endpoints are properly secured and updated even when not directly connected to the office network. Any managed system that experiences failures or drifts from baseline standards should be automatically reported to IT operations for prompt remediation to minimize impacts and ensure continuous compliance.

Mobile endpoints should also be secured to prevent data loss and inappropriate access. When remote systems connect to the business network, any sensitive data accessed needs to be secured both in transit and on the remote endpoints with encryption. USB and other device ports also must be locked down to prevent unauthorized data duplication. Although it is essential to provide access points for remote users to connect with the business network and resources, these should all be hardened with strong, two-factor authentication.

Adopt Virtualization Aware Management Solutions

When managing desktop and application virtualization implementations, it is essential to utilize automation tools that are "virtualization aware" – that is, management resources that understand virtual license requirements as well as the parent/child dependency relationships of virtualization configurations. This will greatly simplify provisioning, patching and on-going administration of supported VMs. In addition, all VMs in an infrastructure should be automatically identified and tracked to determine their level of activity. Any unnecessary instances – those that have had little or no end user activity in a reasonable period of time – should be eliminated to prevent VM sprawl.

Utilize Automation for Migrations

Automation should also be employed when transitioning users to new environments. Automated deployment solutions begin the process by provisioning the endpoint (either physical or virtual). Application deployment and configuration processes propagate the new environment with settings consistent with adopted standards for optimum performance. To minimize impacts on the end user, "user state migration" must be used to automatically transition user data, preferences, and configurations to the new endpoint, mapping any settings appropriately to their location in the new environment.

Ensure Software Consistency

Processes should also be established that ensure software consistency across the support stack. Begin with the identification of application dependencies to accurately map which software installations, updates and patches should be installed to meet endpoint requirements. Software versions and dependency requirements will change over time as the platforms evolve, so it is important that standardized configuration be recorded and regularly updated to provide a common baseline for endpoints to be compared against. Installed software packages should be monitored throughout their lifecycle to ensure they are continually in compliance with the established baselines.

All of these processes will help reduce infrastructure complexity, allowing IT support to more proactively react to changing enterprise requirements. For additional evolving challenges not addressed here, the basic precepts of consolidating management, standardizing configurations, and monitoring for compliance still apply. But, of course, process alone cannot resolve complex problems – automation is essential to simplifying administrative tasks.

Enabling Dynamic Lifecycle Management with Automation

A common theme across all management process improvement is the need for automated solutions to simplify administrative tasks. Since a majority of lifecycle management activities are eminently repeatable, these procedures are ideal for automation. The more IT processes are automated, the more time support staffs regain to focus on IT improvements and business-focused projects. Additionally, automation increases the reliability of a support stack by monitoring for failures and reducing mean-time-to-repair of any incidents that are detected. This is essential to moving support environments from reactive to proactive problem management.

Ivanti offers a lifecycle management automation platform specifically designed to address challenges in both traditional and emerging endpoint management requirements. The Ivanti Destop and Server Management (Ivanti DSM) solution suite from Ivanti offers a unified management solution for supporting both physical and virtual Windows-based PCs, mobile devices, thin clients, and servers across the enterprise. With a Web-accessible interface and role-based access and authentication, the product set allows IT professionals easy access and customized views of the entire support stack from a centralized location. Wizard-based tasks and an end-user self-service portal are included to greatly simplify administrative tasks.

Ivanti offers a lifecycle management automation platform specifically designed to address challenges in both traditional and emerging endpoint management requirements.

Addressing core lifecycle management requirements, Ivanti DSM provides asset management, system provision services, Software and configuration management, remote control, patch management, security assurance, and backup automation. For asset and inventory management, the solution set discovers all IP-addressable hardware components and integrates with the vendor's own CMDB implementation for a consolidated and holistic enterprise view. Image-based and/or "pre-scripted unattended build" system deployment is also included to enable the bare-metal provisioning of physical and virtual endpoints. The solution's "Software Factory" provides integrated OS, application, patch and driver packaging with 170 pre-defined wizard driven commands included out-of-the-box to simplify software delivery. Security assurance reports and alarms ensure endpoints meet compliance objectives, and both vulnerability and malware scans prevent endpoints from being compromised. Backup and restoration features are also included to assist in data and configuration migrations and to facilitate disaster recovery.

Going beyond traditional lifecycle management processes, Ivanti DSM provides advanced capabilities specifically developed to address emerging management challenges. For instance, the platform includes virtualization aware monitoring and maintenance features. VMs are discovered and can be fully and easily provisioned with the same interface used for deployment to physical endpoints. Application virtualization packaging and provisioning capabilities are also included with full support available for Citrix XenApp implementations. Personality migration automation enables a smooth transition of user states to and from virtual and physical endpoint or between different operating environments. Additionally, a software lifecycle dashboard is provided, which achieves full software release monitoring and management functionality. Wizard-based queries identify software dependencies and appropriate package installation order prior to deployment, and individual release packages can be modified to meet unique endpoint requirements. Also, the status of software package delivery is tracked and clearly reported on the dashboard interface.

In order to address emerging requirements that have not yet been developed for the Ivanti solution set, easy-to-use integrations with third-party solutions have been established, greatly enhancing the extensibility of the platform. Taken as a whole, the Ivanti DSM solution suite from Ivanti offers a comprehensive and consolidated platform for achieving both traditional lifecycle management requirements and emerging technologies, allowing organizations to provide the management resources necessary for enterprises to succeed in meeting evolving IT requirements.

EMA Perspective

There can be no question that IT is evolving. Increased use of emerging technologies, particularly in regard to virtualization and mobilization of IT resources, are changing how enterprise services are hosted, provisioned, and employed. Business pressures to "do more with less" are driving this transition as consolidation initiatives improve cost-effectiveness, and increased IT accessibility is expected to enhance user productivity. To be effective in the adoption of these new capabilities, however, organizations must enable management solutions that keep pace with the expanding technology. Enterprises that are able to adapt to emerging requirements will have a competitive edge over businesses that continue to rely on antiquated IT processes.

Enterprises that are able to adapt to emerging requirements will have a competitive edge over businesses that continue to rely on antiquated IT processes.

Automation and integration are the two key elements in a management solution that enable agility in meeting these challenges. Comprehensive automation is essential to the simplification of disparate management requirements in a complex IT ecosystem, and integration is essential both for enabling consolidated management practices within a solution set and also for extending capabilities beyond the solution set. The use of multiple point solutions fails to provide either and is often adopted to fix immediate problems without concern for the long-term viability of the IT investments. Organizations are cautioned not to compromise business value for short-sightedness. Investment in an integrated, centralized IT management solutions suite, such as Ivanti DSM from Ivanti, will yield both immediate improvements and long-term value that will dynamically adjust to the changing condition of the marketplace and emerging IT requirements.

About Ivanti

Ivanti is IT *evolved*. By integrating and automating critical IT tasks, Ivanti helps IT organizations secure the digital workplace. For more than three decades, Ivanti has helped IT professionals address security threats, manage devices and optimize their user experience. From traditional PCs, to mobile devices, virtual machines and the data center, Ivanti helps discover and manage your IT assets wherever they are located, improving IT service delivery and reducing risk. Ivanti also ensures that supply chain and warehouse teams are effectively leveraging the most up-to-date technology to improve productivity throughout their operation. Ivanti is headquartered in Salt Lake City, Utah, and has offices all over the world. For more information, visit www.ivanti.com.

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 EMA's 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, Facebook or LinkedIn.

Corporate Headquarters:
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com

2367.040617