



# Reduce Complexity while Protecting Your IT Environment with Hitachi IT Operations Director

Choose the Right Systems Management Solution  
for Your Business

*By Hitachi Data Systems*

August 2011

## Table of Contents

<b>Introduction</b>	<b>3</b>
<b>How Complexity Impedes Your Business</b>	<b>3</b>
<b>Lower Complexity and Simplify Information Management</b>	<b>4</b>
<b>Enhance and Extend Security Policy Enforcement</b>	<b>4</b>
<b>Intelligently Audit and Manage Information Flow</b>	<b>6</b>
<b>Take Charge of Your IT Environment with Hitachi IT Operations Director</b>	<b>7</b>
<b>Summary</b>	<b>8</b>

---

## Introduction

Information technology is the engine that powers your business. To help that engine run efficiently, it needs to be secure, reliable and well managed. One way to get there is to reduce the complexity of your IT environment. Unfortunately, IT departments in many businesses today find themselves in a reactive mode: they tackle issues that arise with somewhat disjointed and ad hoc software tools. This burdens the company with uncertainty, wastes precious time and resources, and actually increases complexity.

The most successful businesses constantly look for ways to reduce this complexity and remove the uncertainty from their IT environments, while ensuring a positive experience for their end users. To accomplish this, these companies look for integrated lifecycle management solutions that simplify IT tasks, such as security management, asset management and software distribution. The result is a more effective engine running your business and a proactive IT team that has the time to focus on business-enhancing opportunities rather than dealing with unnecessary complexity.

## How Complexity Impedes Your Business

In today's typical IT environment, it is easy for administrators to find themselves forced into a "swivel chair" approach to managing their IT infrastructure. They may use one tool to manage security policies and virus scans, another for Microsoft Windows updates and yet another to deploy software. They may need to move between different dashboards to address issues as they arise. Multiple tools, custom scripts and ad hoc monitoring processes all contribute to complexity. This takes attention away from 2 of IT's biggest challenges: ensuring infrastructure consistency through policy enforcement, and auditing and managing the flow of information.

When it comes to ensuring infrastructure consistency, strict corporate policies over PC and infrastructure usage are not enough. There is always the risk of an employee downloading unauthorized software, using applications from home or installing pirated software. Instead, IT must be able to monitor everything within the infrastructure to maintain a secure, consistent and compliant environment. They need to know that everyone in the environment uses the latest antivirus definition file, and that virus scans run per requirements. They must be able to review and report on the status of security measures and access actionable information so they can make necessary adjustments.

Beyond security management, IT must be capable of determining which PCs or servers have the latest Windows operating system (OS) patches, and which do not, along with the status of each patch. They need proof, in real time, of which software applications are currently installed on users' machines. They must also prove that the applications are compliant with their license agreement. Finally, they need to preempt anyone who tries to bring unauthorized software into the environment.

Another major concern impacted by complexity is managing and auditing the flow of information inside and outside of the organization. Effective security management extends beyond locking down policies, deploying antivirus software and running scans. IT must limit and control which applications users install and run, determine which USB devices are authorized for use, and decide if there is a need to conduct file-level audits. While your environment may be secure, IT remains saddled with the task of determining what is happening at the file level. Managing this information is vital to protecting the business from theft of intellectual property, and reducing the risk of "data leaks."

A reality today is that data leaks can occur in any company. What happens when an employee copies a sensitive file, such as a financial report, then moves it to an insecure location? What if he or she emails it to someone outside the company? Also, consider USB device usage: even with authorized USB devices and authorized file access, employees are moving information in and out of the company, often beyond the control of IT. Preventing these incidents is a critical first step. Being able to track and audit the flow of information is even better. This is where systems management software comes into play.

## Lower Complexity and Simplify Information Management

According to a 2010 report by Gartner, management of desktop PCs is "the most critical factor in reducing total cost of ownership (TCO)."<sup>\*</sup> A locked and well-managed desktop PC can cost 43% less to maintain than an unmanaged one.

*\*Source: Federica Troni, Mark A. Margevicius, Michael A. Silver. "Desktop Total Cost of Ownership: 2011 Update," Gartner Report, November 16, 2010.*

What companies need to reduce the complexity within their IT environments is a fully integrated systems management software solution that simply and cost-effectively administers assets, security and software distribution. Integrating these key functions into a single solution can create a powerful tool for managing the entire IT environment. This means the IT staff can finally replace multiple tools with a single, easy-to-learn and simple-to-use solution. This provides tight integration of security, software distribution and assets, allowing these components to work together to help businesses stay focused on getting the most from their infrastructure.

Staying competitive requires that businesses lock down their most valuable asset: their intellectual property. The right systems management tool helps minimize the risk of information disclosure by monitoring all client computers and servers automatically. And this extends to automated monitoring of antivirus software and update status, allowing IT to proactively identify risks through a wide array of reports and alerts. Businesses can track the flow of information and specify policies for scenarios that trigger an error or violation, such as compliance with software license agreements.

To help reduce the time and labor required to discover, record and maintain IT asset inventories, a systems management solution can quickly discover and track all assets. This capability enables managers to make sure that the assets are correctly managed and supports budget planning by aggregating total asset-related costs, both hardware and software. It should provide the information and necessary control so that the IT manager can intelligently manage assets. When IT can efficiently manage assets, software distribution and provisioning, the result is information consistency throughout the business.

## Enhance and Extend Security Policy Enforcement

Many businesses are learning the hard way that internal security leaks, both unintentional and malicious, are becoming increasingly common and costly. Protecting your business calls for a way to monitor, analyze and trace the activity of every user, and ensure that IT security policies meet compliance requirements. To stay ahead of emerging threats, IT and business managers require timely, intuitive reports to help staff proactively make security adjustments as needed.

The right systems management solution delivers unmatched policy management tools so IT can define policies based on device type, organization, location and network segment. Delivering a

comprehensive security solution will help relieve the pressure on your IT staff, enabling them to focus on critical business initiatives. Look for a solution that reduces risks and helps you maintain a secure environment by:

- Driving consistency through defining which software is mandatory, required patch levels and which software is not allowed on devices in the IT environment
- Ensuring antivirus software recognizes the latest threats and reports current status
- Locking down security by monitoring firewall settings, controlling user access to services and printers, and controlling the use of shared folders
- Defining what types of external media, such as USB devices and SD memory cards, employees can use to access ports within the IT environment

Policies set within the solution should trigger software and patch updates, making software distribution as easy as possible. This means staff can monitor items based on policies from within the dashboard, simplifying IT management tasks even further. Agentless security and inventory monitoring should enable seamless integration with end-point security software. And the close coupling with 3rd-party security software should ensure consistency, verifying that all security applications are up to date. The right systems management tool should:

- **Manage Windows update tasks.** PCs require frequent patches to stay productive and secure. A robust solution should monitor patch status on client PCs and servers across the entire IT environment, and verify automatic Windows update status. This helps ensure that software is always in a working state, and end users have the required Windows OS patches with the latest updates.
- **Ensure antivirus software usage.** Stale virus definitions open the business to risk. With software management, IT can control antivirus software installation and settings, including scan engine versions, definition of file time stamps, auto-protect status and last scanned dates.
- **Restrict software use.** Not all users can be trusted to adhere to IT infrastructure terms of use. Software management gives IT control over which software is mandatory and which is prohibited. Administrators can automatically install mandatory software and block or uninstall prohibited software.
- **Limit Windows services.** Not all users should have access to sensitive Windows services. Systems management monitors which Windows services are running in the environment and automatically stops any unauthorized service before a threat arises.
- **Boost OS security.** Security does not stop at the user application level. A rich set of security policies enable IT to easily manage OS settings such as passwords, auto logon and firewall protection.
- **Manage device access.** Unauthorized device usage opens the business to potential threats. From 1 console, IT should prohibit or restrict access to devices such as printers and other external devices.

Look for a systems management solution that delivers deep visibility across multiple platforms and different product families, and presents the results in 1 dashboard. This means IT saves time by visualizing the entire environment from 1 tool, allowing them to answer difficult security-related questions rapidly. The dashboard should provide a view of assigned policy status, displaying the

violation level for each computer and category. For example, IT can quickly determine if all the PCs in the environment have similar Windows OS settings, like guest account login status.

In addition, the dashboard should provide IT with the flexibility to assign and enforce unique policies to a selected computer, locking down security at a granular level. And it should allow the consolidation and automation of critical tasks and reporting to enable the most efficient use of time and resources. The solution should administer all of your key lifecycle management functions, so you can spend less time managing your IT environment and more time growing your business.

## Intelligently Audit and Manage Information Flow

When it comes to managing security, it is not only about preventing intrusions and data leaks, but also about tracking the entire information flow lifecycle. Consider the case of a user who copies a file with sensitive financial information. Then, the same user emails the file to another user, who then uses the information for a quarterly report. While not considered a direct breach of security, there are a number of reasons why management may want to audit this information trail. The right systems management solution provides the insight management needs to track and trace file activities to achieve their compliance and security mandates.

A robust systems management solution takes information flow management to the next level while saving IT precious time. Administrators gain fast, intuitive, file-level auditing throughout the environment, giving them deep visibility into the flow of information as it moves from file creation to copy, further movement and email usage. Through user operation logs, this solution should display and audit the movement of all files. IT gains actionable intelligence into when someone copies a file to a USB device, or emails the file outside of the company. This tracing can range all the way back to the point where the leak occurred. A systems management solution helps to keep your PCs and confidential information secure by logging several critical operations, including:

- **Program execution or termination.** The solution tracks when a program launches and stops running, as well as what the program touched, such as files.
- **Internet Explorer and Firefox web access.** The solution maintains security policies for external network access; every file download and upload related to an information leak is logged and stored.
- **File access.** The solution tracks all files, including user actions (create, delete, open, copy rename, move, print) on the files and folders and preserves them as part of information flow auditing.
- **OS operation.** The solution controls every computer and logs PC-specific events, such as boot and shutdown times, who a user is and when a user logs on or off.
- **External media attach and detach.** The solution logs precise time, date and type of hardware any user attaches to a PC, including USB, SD memory and other direct-attach devices.

The time and resource savings that a systems management solution delivers add up quickly. From 1 console, administrators can audit and trace the log based on the particular file. It should automatically back up all logs so IT can roll back history to audit past events; this is a major requirement for achieving compliance mandates. Instead of manually pouring through audits, now your IT staff can focus on ways to optimize further, and provide a better return on investment (ROI) in the IT infrastructure.

# Take Charge of Your IT Environment with Hitachi IT Operations Director

Hitachi IT Operations Director helps you reduce the complexity of your IT environment with industry-leading systems management software that provides IT lifecycle management. An integrated solution, IT Operations Director solves the challenges presented by complex IT environments by simply and cost-effectively administering assets, security and software distribution. It helps keep your client computers and confidential information secure, provides the information you need to effectively manage your IT environment and automates critical tasks to save time and money.

## Hitachi IT Operations Director: Key Benefits

- **Protection:** helps keep your client computers, servers and confidential information secure
- **Control:** provides the information and control you need to effectively manage the user's IT environment
- **Efficiency:** consolidates and automates critical tasks, and displays information in a single, intuitive user interface to help you use your time and resources more efficiently

To reduce complexity, it is essential to control all of the assets in your IT environment. Hitachi IT Operations Director enables complete management of hardware assets (server, desktop, storage, switch, etc.), software license assets and asset contracts. It manages and stores contracts (type, start and end date, etc.) with related hardware and software, giving you the control you need to manage your assets in less time. With IT Operations Director, you can ensure license agreement compliance and reduce the headaches often associated with asset management.

Hitachi IT Operations Director offers several asset management benefits, such as tight integration with Microsoft Active Directory to discover computers and automatically store and organize asset details. IT Operations Director also assists system administrators by easily importing information about assets that are not connected to the network and providing software licensing information on a single screen.

System administrators are challenged by malicious and unintentional security leaks, which are becoming increasingly common and costly. Hitachi IT Operations Director provides a comprehensive security solution that provides both security policy management and PC auditing. Combined with a powerful set of security services like automatic corrections, proactive alerts, user operation logs and thorough reporting, IT Operations Director relieves pressure on IT staff and helps to keep your valuable data secure. For example, automatic corrections allows system administrators to automatically correct a computer's inappropriate or risky settings by simply applying a security policy. The software issues proactive alerts to identify potential information disclosure and external device alerts when unauthorized external devices, such as USB drives are used.

To protect your business, you need to monitor, analyze and trace the activity of every user and ensure that your company's IT security policies are adhered to and monitored. Hitachi IT Operations Director user operation logs trace all user activity and record only information that violates security policies to reduce the volume of logged data. IT Operations Director also enables file-level auditing, which instantly tells administrators if a file has been copied, moved, emailed, modified or deleted. To further boost administrative efficiency, the software offers mass distribution and installation of any software application or file, including antivirus software and updates, as well as automatic removal of prohibited software. Reporting capabilities of IT Operations Director provide focused security reports, including "top offender" reports that make it easy for system administrators to prioritize actions.

Efficiently managing software distribution and provisioning is a challenge in many IT environments, especially where software must be installed 1 computer at a time. To make software distribution as fast, easy and efficient as possible for your end users, IT Operations Director enables easy distribu-

tion for delivery of software packages, including executables (MSI, EXE), compressed packages (ZIP) and scripts (BAT). In addition, the software offers 1-step installation of software on multiple computers in 1 simple task, scheduled deployments to set up software and patches, and quality assurance that software is consistently deployed with the latest updates.

If you are overwhelmed by an IT environment that is challenging to manage, take back control with Hitachi IT Operations Director. Designed for medium-to-large businesses, IT Operations Director is an integrated solution that is easy to install, configure and learn. It is a powerful tool for efficiently protecting and controlling your entire IT environment.

## Summary

As IT environments grow larger and more complex, they become more challenging to manage. However, this does not need to be the case. Systems management solutions can help you reduce the complexity and give valuable time back to your IT team to help them focus on more business enhancing activities. Hitachi IT Operations Director helps you reduce complexity by automating processes for greater efficiency. It gives IT managers a fully integrated solution to manage key functions, including security management, asset management and software distribution. The integration of these 3 management functions helps eliminate the reliance on multiple tools, enabling consistency across the organization.

By bringing all of your IT management functions into sharp focus, IT Operations Director helps you take charge of your IT environment. It delivers deep information protection that helps keep your client computers, servers and confidential information secure. You gain the information and control you need to effectively manage and simplify even the most complex chores. And, you can finally consolidate and automate critical tasks by displaying information in a single, intuitive user interface to help you use your time and resources more efficiently.

Keep the engine that drives your business running at top efficiency. Get answers, quickly and accurately, to the vital questions about your infrastructure, including the OS, applications, antivirus protection and the files requiring audits. And gain the power to shift from reactive mode, such as fighting virus problems or finding out if PCs have the right software, to a proactive mode that frees your best people to deliver a better end user experience for employees and customers. Hitachi IT Operations Director can get you there.

### More Information

For more information about how Hitachi IT Operations Director can help you take charge of your IT environment, please visit our website: [www.itoperations.com](http://www.itoperations.com).

### About Hitachi Data Systems

Hitachi Data Systems provides best-in-class information technologies, services and solutions that deliver compelling customer ROI, unmatched return on assets (ROA) and demonstrable business impact. With a vision that IT must be virtualized, automated, cloud-ready and sustainable, Hitachi Data Systems offers solutions that improve IT costs and agility.

With more than 4,300 employees worldwide, Hitachi Data Systems does business in more than 100 countries and regions. Hitachi Data Systems products, services and solutions are trusted by the

world's leading enterprises, including more than 70% of the Fortune 100 and more than 80% of the Fortune Global 100. Hitachi Data Systems believes that data drives our world — and information is the new currency. To learn more, visit: [www.hds.com](http://www.hds.com).

## Hitachi Data Systems Corporation

---

### Corporate Headquarters

750 Central Expressway  
Santa Clara, California 95050-2627 USA  
[www.HDS.com](http://www.HDS.com)

### Regional Contact Information

**Americas:** +1 408 970 1000 or [info@hds.com](mailto:info@hds.com)  
**Europe, Middle East and Africa:** +44 (0) 1753 618000 or [info.emea@hds.com](mailto:info.emea@hds.com)  
**Asia Pacific:** +852 3189 7900 or [hds.marketing.apac@hds.com](mailto:hds.marketing.apac@hds.com)

Hitachi is a registered trademark of Hitachi, Ltd., in the United States and other countries. Hitachi Data Systems is a registered trademark and service mark of Hitachi, Ltd., in the United States and other countries.

All other trademarks, service marks and company names in this document or website are properties of their respective owners.

Notice: This document is for informational purposes only, and does not set forth any warranty, expressed or implied, concerning any equipment or service offered or to be offered by Hitachi Data Systems Corporation.

© Hitachi Data Systems Corporation 2011. All Rights Reserved. WP-407-A DG August 2011