CDW PEOPLE WHO GET IT

THE MYTHS OF SOFTWARE COMPLIANCE

Don't make software license compliance harder by falling victim to common misconceptions about tracking and managing software assets.

Executive Summary

Increasingly complex software licensing models, a fast-changing IT landscape and heightened risk of vendor-driven software audits are making software license and asset management a top-of-mind issue for IT and business organizations alike. IT shops are struggling to grasp the disposition of the software they own, to the point that they may inadvertently fall out of compliance with their contractual obligations to software vendors.

Software asset management (SAM) solutions promise to fix all that. They present a set of tools, practices and processes that take the uncertainty out of software licensing and enable organizations to fully optimize software inventories. But efforts to establish formal SAM programs are sometimes clouded by myths and misconceptions that result in avoidable setbacks.

From heightened expectations about the efficacy of SAM tools to a lack of understanding of audit risks, organizations too often fall prey to complacency. And there are significant risks to simply ignoring how software is licensed and used throughout the enterprise. This paper presents some of the top misconceptions and offers insight to help organizations steer around them.

Table of Contents

The Growing License Management Challenge

Software license compliance has emerged as a critical area of focus for organizations. Challenged by increasingly complex licensing models, a fast-changing IT landscape and the heightened risk of vendor-driven software audits, organizations are moving to deploy software license management systems and processes. But even as IT shops move to better discover, track, manage and remediate license compliance across the enterprise, they are falling victim to assumptions and misconceptions that can stymie their efforts and increase the risk of attracting an expensive software audit.

Gartner analyst Patricia Adams, in a MarketScope report on IT asset management (ITAM), wrote that Gartner expects market penetration of asset management solutions to increase from about 45 percent in 2011 to 70 percent in 2016. These investments reflect growing awareness of the challenges facing organizations as they struggle to manage an increasingly diverse and expansive software portfolio.

Unfortunately, organizations must contend with misconceptions about license management even as they work to address it. In a presentation at the fall 2013 conference of the International Association of IT Asset Managers (IAITAM), Christof Beaupoil, president and co-founder of Aspera Technologies, laid out what he called common myths of strategic license management.

He argued that entities are often overconfident about the effectiveness of automated tools, and that they fail to grasp the breadth of the asset management challenge as it crosses technical, functional and operational boundaries. The success of an asset management program, he says, depends on a blend of advanced tools, adapted processes and committed management.

Drawing Fire

Businesses can't afford to ignore the issue. According to BSA, an association of software vendors that promotes and enforces software compliance, the commercial value of pirated software deployed in the United States alone is nearly $10 billion. That figure has motivated software vendors to rigorously support efforts to curb software piracy and license noncompliance.

Software publishers are turning to audits to challenge customers they suspect of being out of compliance, and the pace of those audits is going up. In its *2012 Key Trends in Software Pricing and Licensing* survey, analyst firm IDC and Flexera Software found that 64 percent of enterprises reported undergoing an audit or license review over the past 18 to 24 months. More than one-third of respondents (36 percent) reported being audited at least twice in that time period, while 10 percent reported more than three audits.

New Challenges in Software Management

Shifting application delivery models pose a challenge to software license and asset management programs. Virtualized environments, cloud-based services — including software-as-a-service (SaaS) applications — and bring-your-own-device (BYOD) mobile application scenarios are forcing organizations to scramble to manage new license models.

On the virtualization side, organizations face complex licensing schemes based on physical resources allocated to virtual machines. But virtualized environments cloud the relationship between software and hardware. Audit solutions may fail to identify software installed on virtual machines or to uncover the relationship between a virtual machine and physical host. Because these relationships often must be measured manually, sometimes by expensive consultants, it simply never gets done.

The cost of failure can be high. Organizations that conduct inaccurate audits and put the wrong kind of license against a database can easily face costs that range into the hundreds of thousands of dollars.

Cloud-based services turn the virtualization challenge on its head. Here, compliance isn't the issue as much as cost optimization. Cloud vendor contracts prevent organizations from using more software than they've licensed, but do little to prevent organizations from owning more licenses than they use. Software tailored to monitoring cloud-based application activity can help determine if a company is overprovisioned.

Shelfware and overprovisioning are constant concerns with cloud-based software. To avoid carrying too many licenses, managers must be disciplined in deleting virtual machines that are spun up by individuals or departments. Failure to do so risks carrying large numbers of so-called "orphaned" virtual machines that consume licenses and inflate cost.

The outlook for BYOD mobile applications may be murkiest of all. Mobile device usage in the enterprise is exploding. A global survey of 1,700 senior IT decision-makers by Citrix Systems found that 74 percent allow or encourage use of personal mobile devices in the enterprise.

Yet, BYOD presents a compliance management challenge. In theory, employee-owned applications that connect to the corporate network may be subject to corporate licensing rules. For instance, if an employee uses a BYOD device to check work email while logged on to the corporate network, the organization needs to own a license for the app on that device, even if the employee has a personal license of his own.

Some organizations are considering enterprise app stores, modeled after consumer venues such as Apple's App Store or Google Play, as a solution to streamline software delivery and license management. However, these are not yet widely deployed.

Faced with increasingly diverse application ecosystems, growing license complexity and a greater risk of being audited, organizations are compelled to take action. But to do so effectively, they must avoid misconceptions and pitfalls that can hamper their efforts.

Myth 1: Discovery and Scanning Tools Alone Provide an Actionable Picture of Software Assets

Companies of all sizes struggle to gain visibility and control over software license management. However, it's not for lack of trying. In the *2012 Key Trends* survey, 82 percent of enterprises describe managing software licenses as either important or very important, up from 72 percent the year before. However, a common mistake that organizations make is to rely too much on automated software discovery and scanning tools.

While highly logical, the first thing companies often do when initiating a license management effort is to deploy a software discovery and scanning tool. Such tools can be highly effective; however, care must be taken to cover a number of nuances that can lead to shortfalls.

Companies that rely exclusively on scanning and discovery tools can find themselves missing crucial information needed to drive a proper assessment. Missing data can include:

- Hardware configuration data needed for management of server software licenses, including number of processor cores and hard or soft partitioning for virtualization
- Application-specific data that can be gleaned only from more comprehensive deep scans
- Changed registry keys
- Signatures and recognition rules used to identify stand-alone software (such as Microsoft Word) from suite-based products (such as Microsoft Office).

Another potential source of trouble comes from so-called "orphaned devices," which are not assigned to any cost center in the business. Orphaned devices include legacy systems or hardware that the organization has retired, but some of which remain in use because the hardware was never collected from users. As orphaned devices don't belong to a defined cost center, data gathered about them during a scan can go unassigned and essentially become lost in the system.

Organizations must grasp both the limitations and the role of discovery and scanning tools in the context of a license management program. These tools allow IT managers to see the applications installed on their systems, and offer some baseline intelligence for a software license management effort. But they will not provide insight into the actual licenses and entitlements associated with the software they detect.

The BSA and SIIA: Keeping an Eye on Software

BSA and the Software & Information Industry Association are industry trade groups broadly concerned with intellectual property ownership and anti-piracy efforts. While both organizations represent and advocate for software publishers, SIIA takes a broader focus, with a membership that includes media, content and software publishing firms.

Both organizations maintain whistleblower programs that offer cash rewards to employees who report verifiable instances of software piracy, and both conduct software audits of companies suspected of noncompliance. While larger enterprises undergo audits as part of their contractual agreements with software vendors, smaller companies typically don't draw audits unless they are reported by an employee or other party.

Peter Beruk, senior director of compliance marketing for BSA, says his organization fielded about 2,025 allegations of piracy in the United States in 2013, a number of which were formally investigated. Globally, BSA conducted about 12,000 piracy investigations, according to Beruk.

Figures for settlements are not available, but an August 2012 BSA report announced that the organization logged $2.5 million in audit settlements during the first half of 2012 — an amount described as a "record period of settlements."

In addition to enforcement activities, both BSA and the SIIA maintain programs to promote license compliance. The Verafirm program at BSA, for instance, offers software and resources to help organizations pull their programs into compliance.

Myth 2: An Organization's Software Procurement Data Typically Is Complete

An organization concerned with facing down an audit must possess a clear, accurate and complete understanding of the software it has purchased and the commitments made under those purchases. Unfortunately, most organizations don't.

Some IT departments assume that procurement systems contain all the data needed to drive a license management effort. While these systems may support a license management effort, they are not tailored to capture all the specific types of data needed for such a project.

Thus, organizations frequently struggle with procurement data that is incorrect, incomplete or out of date. Among the procurement data that may be at issue:

- **Product SKU (Stock Keeping Unit):** A unique manufacturer article number used to automate the license inventory process. Without the SKU, publishers have no way to record product use rights.

- **Pricing information:** Missing or incorrect price or currency information will foil financial evaluation.
- **Contract number:** Needed to verify inherited product use rights and maintenance as well as milestone checks.
- **Cost center information:** Required to assign ownership within the organization.
- **Invoice date:** Vital for determining maintenance timeframes.

Organizations must dig through procurement histories and match recorded purchases against installed software and available licensing data.

From a process standpoint, the enterprise must centralize software procurement or struggle to track meaningful data about purchases that occur at the departmental (or individual) level. Even for organizations that funnel software purchases through a central authority, challenges remain. For instance, cloud providers make it easy for elements to sidestep centralized procurement channels.

Ultimately, spending management and procurement software enables a well-managed process that feeds critical data into a license management effort. But these systems are not tailored for license management and the unique metrics and data associated with it. A SKU catalog, for instance, can fill the gap and ensure that vital information is captured and tracked.

Myth 3: Automated Software License Management Tools Invariably Yield Accurate Results

An effective license management program relies on advanced software, effective processes and proactive management to create data inventories that catalog information both about purchased software and the licensing terms and entitlements associated with it. Organizations that rely too heavily on tools to automate license management risk moving forward with poor or incomplete data.

For instance, relying on asset discovery tools to glean software technical data can yield large gaps in the resulting software inventory, including missing or incomplete data on these elements:

- Product names
- Product versions
- Software configuration
- Virtual machine to host relationships

Virtualized environments pose an ongoing challenge. Discovery tools may not be able to provide full visibility into these environments and the underlying hardware. Tools that link to the source management platform, such as VMware's vCenter Server, will provide more complete and reliable technical information about installed software.

Peter Beruk, senior director of compliance marketing at BSA, says administrators sometimes have significant expectations of their SAM tools. These tools depend on data drawn from IT management solutions used to install, configure and monitor the software on each platform in the organization.

If inputs from these data sources — such as Microsoft System Center Configuration Manager and Virtual Machine Manager, HP Asset Manager and Citrix Express Software Manager — are poor, the data going into the automated license management tool will be poor as well. Automated license management tools must be able to process different types of data coming from a variety of discovery and scanning tool sources.

Improving the performance of license management tools and yielding good data inventories takes a concerted effort that accounts for variables in software licensing and contracts. It's a process that requires the tool to be configured to match the proper license to each specific application or bundle.

Processes must also be adopted, with proper roles and responsibility established among staff, to ensure that data quality in the license management tool is tracked and monitored. Companies should avail themselves of consulting services offered by tool providers, as these can go a long way toward addressing holes that exist in the data flow. Consultants can also address the complexity of licenses, providing vital vendor- and application-specific insight that most organizations cannot afford to keep on staff.

Myth 4: Chances Are Good That an Organization Will Not Face a Software Audit

Year by year, an organization's risk of a vendor software audit goes up. Numerous surveys and reports indicate that as many as two-thirds of all companies face a software audit each year. Notably, software vendors are investing more resources into audit functions.

A KPMG survey of 31 software vendors (representing more the 50 percent of the total revenue in the software industry) found that nearly 90 percent of vendors have a customer license compliance program in place, up from 64 percent in 2007.

Behind this heightened activity is a drive by software vendors to capture lost revenue. The KPMG survey found that more than half the vendors say unlicensed software reduced company revenue by at least 10 percent. And 48 percent of those vendors report that license compliance efforts generated additional revenue equivalent to 4 percent or more of annual software sales.

In short, software publishers have many reasons to conduct audits. Industry surveys confirm that larger organizations are more likely to draw vendor scrutiny than smaller firms.

Risky Business: Software Compliance and Security

Organizations have many reasons to stay on top of software compliance, not the least of which is the risk that renegade software installations pose to systems and networks. Lax license management and out-of-compliance software represent a significant risk to IT operations and lend an urgency to any license management effort.

The SANS Institute, in its report *Top 20 Critical Security Controls,* identified keeping an inventory of authorized and unauthorized software as a key step in securing infrastructure against threats. As the report notes, poorly controlled machines are "more likely to be either running software that is unneeded for business purposes, introducing potential security flaws, or running malware introduced by a computer attacker after a system is compromised."

The report advises IT organizations to deploy an application white list to limit software allowed on managed systems, and to employ software inventory tools and systems to track, control and configure deployed software. These and other recommended steps in the report mirror activities in most software asset management programs.

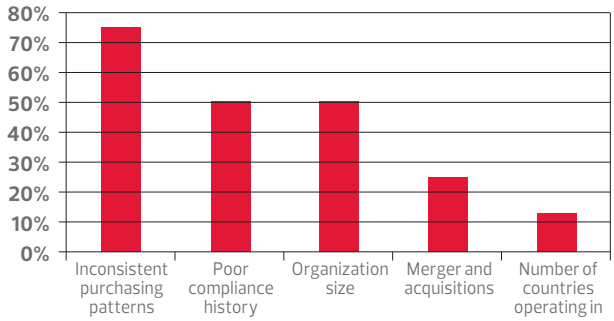
Many experts say the primary threat posed by unmanaged software is that of a Trojan horse infiltration, which open backdoors on the network that third parties can use to compromise systems and data.

In fact, enterprise size is a leading predictor of audit frequency, according to the *2012 Key Trends in Software Pricing and Licensing* survey by IDC and Flexera Software.

A variety of factors increase the chances of drawing an audit. Among the leading drivers:

- **Size of the organization:** Large enterprises generally hold more licenses from more vendors in more complex environments than smaller firms. These factors present audit triggers to an organization's vendor pool. The likelihood of a large settlement for a vendor is also higher.
- **Poor compliance history:** Organizations that are previously found to be out of compliance are at heightened risk of a review.
- **Changed behavior:** Vendors analyze customer purchase patterns and compare them against historical behavior, as well as against industry norms and the behavior of similar companies. Canceled maintenance agreements, reduced license purchase volume and other changes all raise red flags.
- **Organizational changes:** Mergers and acquisitions, growth or contraction, and other structural changes that can affect software usage increase the likelihood of an audit.

How vendors select a customer for audit



SOURCE: Ernst & Young, *Software Compliance Without Tears*, 2011

The smaller enterprise can generally elude scrutiny, in large part because they don't sign volume license agreements that include an audit clause. For smaller firms, something typically must happen to draw compliance into question — such as a disgruntled employee reporting a violation to the vendor or an association such as BSA.

Myth 5: A Large Team of Experts Is Required to Manage Software Licenses

Software license management may seem an overwhelming task, but in truth a small, cross-functional team can address the scope of activities around software license compliance, provided that team adequately represents stakeholders across the organization. Among the functional areas that should be represented on a software compliance team:

- **Executive-level sponsor:** An executive at the C-level, often the CIO, must be engaged with the team to provide umbrella authority and ensure compliance with team initiatives across the organization. This team member is also vital for informing top management of compliance activities.
- **IT management:** Depending on the size of the organization, multiple IT managers might serve on the team to represent users and data center administrators. Regardless, the IT representative should manage key operational details of the group's activities, including deployment of scanning, discovery and management software systems, and management of data-gathering activities. The IT representative is often assigned leadership of the cross-functional compliance team.
- **Procurement/finance:** Finance is another core stakeholder in the license management effort. This representative is responsible for reviewing, adapting and managing the software procurement processes to ensure license compliance and tracking of assets. This person also ensures

that procurement systems and software work effectively with asset management systems. Increasingly, compliance efforts are driven from the finance side of an organization, with the result that the procurement/finance team member is sometimes involved in a leadership role.

- **Compliance officer:** In larger organizations, a compliance officer may be needed to address team efforts within the broader context of corporate governance and best practices.

Matt Fisher, vice president of marketing and communication at SAM tools provider Snow Software adds that every compliance team needs "one person who actually knows what they are doing when it comes to specific vendors' licensing schemes." Many businesses don't have this expertise on staff, and hiring a full-time employee to obtain it often doesn't make financial sense. Snow suggests that organizations consider third-party consulting services to engage this expertise at a reasonable cost.

Ultimately, the success of a license management and remediation program hinges on executive support and effective interaction among organizational stakeholders. A select team of engaged experts can provide the support and oversight a software compliance effort needs to succeed.

Myth 6: Effective Software Management Is Always a Cost and Never an Asset

Discovery, management and remediation activities around software licensing can be expensive and disruptive. A company with 50,000 employees can expect to employ four full-time staff members in a license management effort, according to Aspera Technologies' Beaupoil. Businesses must also budget for software and consulting services.

Less well understood are the financial benefits an effective software license program can deliver.

According to the experts, a license management program can produce quick returns on investment, paying for itself within the span of one to two years. A *Software Efficiency Report* by IAITAM and Opinion Matters found that unused software costs organizations an average of $414.50 per PC. The survey also found that 83 percent of managers report having undeployed "shelfware" in the enterprise, with an average of 23 percent of all purchased software never having been installed.

Among the financial benefits of a software license management program:

- **Elimination of shelfware:** If a substantial portion of purchased software is never installed or deployed, eliminating shelfware from inventories could reduce software expenditures by as much as one-fifth.

Why Software License and Asset Management Projects Fail

Software license and asset management projects are a significant undertaking, requiring the active and sustained engagement of both business and technical/IT management. Unfortunately, these programs often struggle and fail to deliver the promise of rational, efficient and comprehensive oversight of software assets across the enterprise. Among the reasons:

- **Failure to scope:** Organizations that rush into a software asset management program without adequate planning can find themselves facing an unmanageable task. Snow Software's V.P. of Marketing and Communication, Matt Fisher, warns that many are surprised by the scope of their license management efforts. Be mindful of the scope and scale of the task ahead and budget time and money accordingly.
- **Failure to iterate:** Organizations that are just getting started should consider breaking the task into smaller portions, targeting first a specific geography, a well-defined hardware profile (only desktop PCs, for example) or a single vendor's installed products. This reduces the scope of mistakes and allows the team to apply lessons from these efforts as they move forward in successive phases of the project.
- **Failure to define success:** Goals are a foundational component of any successful license management effort. Organizations that are out of compliance should factor in the cost of retroactively paying for licenses into the success matrix and cast "planned cost" as a success metric against the unplanned cost of a software audit. An effective SAM program will establish metrics to recognize achievements such as reducing the number of unused or underutilized licenses, which can help sell SAM efforts to executive management.
- **Failure to gain executive sponsorship:** As a cross-functional effort that can impact and, at times, disrupt operations across the enterprise, a successful license management program requires executive-level support. The active engagement of a C-level executive is necessary to carry a top-down mandate to the organization, while also selling the effort to executive management.
- **Failure to engage stakeholders:** Projects that fail to engage key stakeholders often struggle. A large, dedicated team is not required, but a successful effort must get buy-in from the organization and all affected departments. A SAM program should recruit key representatives from affected units, including IT, finance, procurement, human resources and executive management. Larger organizations may add a data center IT representative, as well as a governance officer to ensure compliance with best practices.

- **Implementation of pooling:** Software maintenance accounts for 80 percent of license costs over the course of a contract. Yet as much as 30 percent of licenses are often no longer being used or are not being used correctly. For instance, a company that shrinks its workforce may develop a stockpile of available licenses, yet fail to recycle those assets (a practice called pooling) during deployments. Right-sizing software license inventories can significantly reduce the annual cost of software contracts.
- **Enhanced negotiation:** Improved visibility into software inventory, usage and trends allows companies to hammer out better terms with software vendors during contract negotiations.
- **Reduced risk:** Software audits routinely produce settlements in the hundreds of thousands (and sometimes even millions) of dollars, not counting costs associated with defending audits. The *Express Metrix 2013 Software Audit Industry Report* found that 24 percent of audits among those surveyed yielded costs between $50,000 and $250,000. License management programs swap an expensive, unplanned cost for more economical planned costs.

Companies that establish an effective software license optimization regime realize additional benefits. For instance, tools and data can help an organization determine software costs associated with changes such as adding personnel or updating data center assets.

Software Audits: The Best Defense Is a Good Defense

When it comes to experiencing a software audit, it's not a matter of if, but when. According to a report by CDW and CIO Custom Solutions Group, nearly two-thirds of all businesses in the United States will be audited by at least one software vendor over the next year. Yet, nearly half of respondents to an IDG Research Services survey reported feeling somewhat or not at all prepared to defend an audit. Only 10 percent of survey respondents said they felt extremely well prepared.

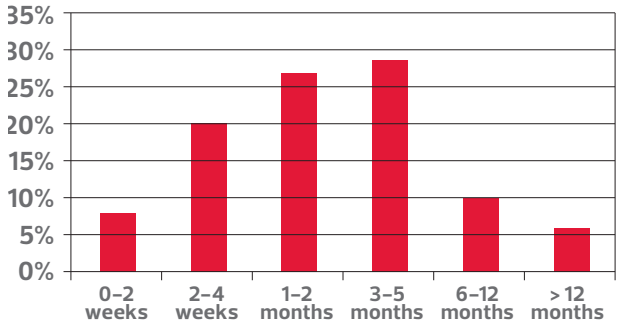
This lack of preparation is born out by Opinion Matters' *Software Efficiency Report*, which surveyed 500 companies and found that 52 percent of enterprises are using spreadsheets to record part or all of their software license data. Further, 12 percent have no process to track software licenses at all. For these organizations, facing down a software audit can be incredibly challenging.

BSA's Senior Director of Compliance Marketing, Peter Beruk, says the first rule of defending a software audit is not to ignore the software audit. "If you ignore the request, people are going to think you really have something to hide," he says, urging companies to get ahead of the problem. "Engage your management. Engage your legal counsel."

Audited companies must promptly gather key information and begin mounting a defense. An initial order of business will be forming an audit defense team, if one doesn't exist already as part of the company's license management program. That team will need to include executive-level sponsorship to ensure that business units comply with mandates and to apprise top-level management.

The audit process can be prolonged. The Express Metrix survey found that nearly half of organizations were given a month or more to prepare for an audit, while the entire process, from initial request to close of action, often stretches for months.

Length of Audit



SOURCE: *Express Metrix 2013 Software Audit Industry Report*

Organizations should use the available time to gather key information, including:

- Purchase records and proofs of purchase
- Invoices and sales receipts from vendors
- Manuals and certificates of authenticity
- Comparison of purchased licenses to installed software

Ultimately, the best defense against an audit is not to trigger one. And in this regard, the best protection could be to deploy IT asset management tools. The Express Metrix survey showed that organizations that had implemented IT asset management reported an audit rate of 46 percent over the previous two years, compared with a 68 percent rate for organizations without such tools. By deploying SAM tools, companies stand to significantly lower the chance of audit.

CDW: A SAM Partner That Gets It

CDW's trained and certified technology experts understand the intricacies of SAM and can help organizations take a comprehensive approach to deploying a solution that fits their unique environments. Our team of experts includes:

- **Software asset management specialists:** Our certified specialists can analyze your licenses in depth and provide reconciliation services to help you understand gaps between entitled and deployed licenses. They can help incorporate software asset management best practices into your regular systems management tasks.
- **Licensing account executives:** By attending onsite meetings and technology briefings, these specialists review your current environment.
- **Presales systems engineers:** The engineers are always available to answer in-depth software, licensing and technical questions.

For software licensing and asset management support services, CDW provides assessment, planning and design; assistance with evaluating software licensing program options; contract planning and management; configuration management; and onsite software installation and lifecycle support. Our step-by-step approach involves:

- An initial discovery session to understand goals, requirements and budget
- An assessment of the existing IT environment and definition of project requirements
- Detailed evaluations, recommendations, environment design and proof of concept
- Procurement, configuration and deployment of the chosen solution
- Telephone support and ongoing product lifecycle support

To learn more about CDW's software license management solutions, contact a CDW account manager, call 800.800.4239 or visit CDW.com/SAM

Microsoft

Microsoft Office 365 for large and small organizations is a subscription service that combines the familiar Microsoft Office Apps with a set of web-enabled tools that are easy to learn and use, that work with your existing hardware and that come backed by the robust security, reliability and control you need to run your organization.

CDW.com/microsoft

Adobe

Deploy Adobe Acrobat® XI to help your organization achieve mission objectives. With Adobe Acrobat XI software, users get reliable, easy-to-use tools to create, edit and sign PDF documents with enhanced security and simplified software management. Automate processes to improve responsiveness and protect documents wherever they go.

CDW.com/adobe

Symantec

Symantec Backup Exec protects virtual and physical environments, simplifies both backup and disaster recovery, reduces storage with integrated data deduplication and offers powerful recovery capabilities in a single solution. Backup Exec is licensed per agent and option or per front-end TB (capacity).

CDW.com/symantec

vmware

VMware vSphere with Operations Management combines a virtualization platform with management capabilities. This solution enables users to gain operational insight into vSphere while also optimizing capacity. As vSphere environments continue to grow, it is essential that users have proactive management that can deliver monitoring, performance and capacity information at a glance.

CDW.com/vmware

SHARE THIS WHITE PAPER

CDW PEOPLE WHO GET IT