LEARNING MADE EASY

Nlyte Special Edition

Software Asset Management

for dummies®
A Wiley Brand

Identify licensing and entitlement issues

Address software security risks

Optimize software usage and costs

Brought to you by

Nlyte®

Lawrence Miller

About Nlyte

Nlyte Software empowers organizations to increase the efficiency of application workload infrastructure management across their extended enterprise—from the desktop to data center, from colocation to edge to IoT devices. Using Nlyte's monitoring, management, workflow, and analytics capabilities, organizations can automate the management of their resources to reduce costs, improve uptime, and ensure compliance with organizational policies.

Software Asset Management

Software Asset Management

Nlyte Special Edition

by Lawrence Miller, CISSP

for dummies®
A Wiley Brand

Software Asset Management For Dummies®, Nlyte Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-56528-4 (pbk); ISBN 978-1-119-56530-7 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

For general information on our other products and services, or how to create a custom *For Dummies* book for your business or organization, please contact our Business Development Department in the U.S. at 877-409-4177, contact info@dummies.biz, or visit www.wiley.com/go/custompub. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Development Editor: Elizabeth Kuball
Copy Editor: Elizabeth Kuball
Executive Editor: Katie Mohr
Editorial Manager: Rev Mengle
Business Development Representative: Karen Hattan
Production Editor: Vasanth Koilraj

Table of Contents

Introduction

Managing software assets is not a new challenge for businesses. However, the risks of poor software asset management (SAM) have perhaps never been greater. In addition to greater enforcement of licensing compliance by software vendors, many regulatory compliance mandates now require strict control of business software. Sophisticated malware and other cybersecurity threats require organizations to have complete visibility of their computing environment to ensure all software is properly patched in a timely manner and does not introduce unknown vulnerabilities. Finally, overspending on software licensing, support, and maintenance continues to be an ever-growing problem for businesses.

In this book, you discover how a modern SAM solution can help you regain control of your software spending, ensure licensing and regulatory compliance, and reduce security risk for your organization.

About This Book

Software Asset Management For Dummies consists of six chapters that explore the following:

- The basics of SAM, including business drivers and tracking challenges (Chapter 1)
- Software licensing compliance challenges (Chapter 2)
- Software security risks in hybrid on-premises and cloud environments (Chapter 3)
- Software cost management issues (Chapter 4)
- Technical requirements, use cases, and benefits of a modern SAM solution (Chapter 5)
- Key considerations for implementing a SAM solution (Chapter 6)

Foolish Assumptions

It's been said that most assumptions have outlived their uselessness, but I assume a few things nonetheless!

Mainly, I assume that you work in a finance, technology, or compliance role, such as a chief financial officer (CFO), chief information officer (CIO), compliance officer, IT operations manager, or procurement manager. I assume that you understand some of the challenges of software licensing and asset management, but that you may not be aware of your options for a modern SAM solution. Finally, I don't assume any in-depth technical knowledge, so I'll be sure to explain any technical terms and concepts throughout this book and I'll spell out any TLAs — three-letter acronyms!

If any of these assumptions describes you, then this book is for you! If none of these assumptions describes you, keep reading anyway. It's a great book and when you finish reading it, you'll know quite a few things about SAM!

Icons Used in This Book

Throughout this book, I occasionally use special icons to call attention to important information. Here's what to expect:


REMEMBER

The Remember icon points out information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!


TECHNICAL STUFF

You won't find a map of the human genome here, but if you seek to attain the seventh level of NERD-vana, perk up! The Technical Stuff icon explains the jargon beneath the jargon!


TIP

Tips are appreciated, never expected — and I sure hope you'll appreciate these tips. The Tip icon points out useful nuggets of information.


WARNING

These alerts point out the stuff your mother warned you about (well, probably not), but anything marked with the Warning icon does offer practical advice to help you avoid potentially costly or frustrating mistakes.

Beyond the Book

There's only so much I can cover in 48 short pages, so if you find yourself at the end of this book, thinking, "Where can I learn more?," just go to `www.nlyte.com`.

Where to Go from Here

If you don't know where you're going, any chapter will get you there — but Chapter 1 is a good place to start! However, if you see a particular topic that piques your interest, feel free to jump ahead to that chapter. Each chapter is written to stand on its own, so you can read this book in any order that suits you (though I don't recommend upside down or backward).

IN THIS CHAPTER

- Understanding software asset management concepts
- Looking at important business drivers
- Tackling software asset management challenges
- Defining a software asset management process

Chapter 1
What Is Software Asset Management?

In this chapter, you learn the basics of software asset management (SAM) including business drivers and challenges, and how to get started with SAM in your organization.

Covering the Basics of Software Asset Management

The basic concept of SAM is familiar to most businesses, though the many reasons for it may not be fully understood. Many businesses track their software assets for no other reason than to know what they have and what they need. But effective SAM requires a comprehensive and uniform practice, supported by processes and technology, to ensure licensing compliance, manage software costs, improve security, and make better business decisions.

REMEMBER

SAM is a function of technology asset management (TAM). TAM focuses on providing input for managing the total cost of ownership (TCO) around all of an organization's technology assets throughout their life cycle.

SAM is about capturing a deep and wide view of all software assets across your entire organization. At its core, SAM technology discovers

- What software is being used and for what purposes
- Where software is installed
- Who is using the software
- How extensively the software is being used

With this information in hand, organizations are better able to track and manage the proliferation of software across distributed environments. Ideally, SAM technology is nonintrusive and discovers and quantifies software assets on an ongoing basis. SAM technology must provide an automated way for IT leaders to understand their software user base, IT services, and software versions in order to gain clarity about assets — whether in Windows, Linux, or Mac environments. In this way, they can reconcile system use against software licenses to help with external software vendor audits, as well as internal audits.

TIP

SAM technology can help you identify opportunities to save on software licensing, support, maintenance, and other costs.

SAM helps organizations

- Gain complete visibility of the software that is installed in their computing environment
- Understand who is entitled to use installed software and what services are being delivered

When a business uses SAM to perform software version control, it will be able to understand who the users of an application are and what entitlements have been applied, as well as what changes have been made over time. Having a user perspective on application usage also makes it possible to know whether new software licenses must be purchased.

Recognizing the Business Drivers

SAM is perhaps not as much of a priority as it should be for many businesses, given that executives don't necessarily perceive SAM as a strategic initiative. This perception is a bit ironic, given the

importance of software to practically every product or service that's provided by a business in any industry. Yet there is apparently little concern that as organizational investments in software grow, so too do risks and missed opportunities.

A recent survey by Deloitte, "Software Asset Management: Time for a Reset," notes that "SAM hasn't become a strategic priority because companies either aren't focused enough on the significant financial and operational benefits or they haven't felt the sting of a vendor audit." Research conducted by IDG for the survey found that 72 percent of CIOs and IT leaders have not yet created or implemented a formal SAM strategy. This laissez faire approach to SAM has repercussions downstream. When IT leaders don't emphasize the value of SAM, it's easier for the rest of the IT staff to dismiss the importance of SAM as well. Many experts believe that IT staff will have the attitude that they've got more important things to do, that SAM has no applicability to their workloads, and that moving forward with SAM will take too much time and effort away from their "real" jobs.

TIP

Executive leaders — in both IT and business functions — must visibly and proactively support SAM so that all employees realize how important it is to the organization.

A strategic long-term approach to SAM can help businesses reduce legal and financial risks and deliver significant cost savings. The most important potential benefits of implementing a SAM solution, according to respondents in the Deloitte survey, are as follows:

- **Improving systems security, data integrity, and data security:** 36 percent (see Chapter 3)
- **Controlling software costs:** 34 percent (see Chapter 4)
- **Avoiding compliance irregularities:** 33 percent (see Chapter 2)
- **Realizing cost savings:** 32 percent
- **Optimizing software deployment and usage:** 29 percent
- **Improving position to negotiate software licensing:** 27 percent
- **Increasing operational efficiency:** 26 percent
- **Improving ability to identify product rationalization opps:** 22 percent

- **Gaining/maintaining long-term control over software assets:** 21 percent
- **Improving software performance and scalability:** 19 percent
- **Improving data quality to enhance business decisions:** 19 percent
- **Improving budgeting process and financial controls:** 18 percent
- **Improving the management of vulnerability risk:** 16 percent
- **Enhancing user experience:** 14 percent

Understanding Software Tracking Challenges

Many challenges are associated with SAM. For starters, software licenses differ widely from one software vendor to another, and even within a single vendor's product suite. For example:

- Is a system's license based on the central processing unit (CPU) cores of the hardware on which it is installed?
- Is the license tied to additional services upon which the software's use cases depend?
- Does the license accommodate virtual, cloud, and mobile technologies?
- Will licenses be required for Internet of Things (IoT) devices and sensors reporting to a database?
- Does the license permit multiple concurrent users or installations?
- Are named users or instances required?
- Is the license subscription-based or perpetual?
- What maintenance and support options are available and/or required?

Another challenge is that many traditional SAM tools are agent-based and must be installed on every endpoint device in the environment to get a full software asset inventory. The agents themselves must then be managed, along with the enterprise

applications. The agents may interfere with other software applications or processes running on certain endpoints and can be problematic to deploy and install, for example, on the following:

- Non-Windows computers, such as Linux and Mac
- Mobile devices running Android OS or Apple iOS
- Specialized endpoints (such as retail point-of-sale systems, medical technology, and manufacturing equipment)
- IoT devices and sensors

If there are missed endpoints (such as failed installations or dormant virtual machines) or unknown endpoints in the environment, the agent will not be installed, any software on those endpoints will not be accounted for, and the SAM inventory will be incomplete and inaccurate.

WARNING

Some agents use network broadcasts to discover endpoints. These types of agents can introduce security risks and cause network performance issues.

Establishing a Software Asset Management Process

Effective SAM requires a combination of process and technology. The right technology can make the process part of SAM easier, which will help your IT staff better manage your software assets.

A SAM solution automates software discovery and normalizes the data. In this way, SAM tools support SAM processes and enable complete visibility into the following:

- What software is installed, including authorized/unauthorized and sanctioned/unsanctioned software
- Whether installed software is properly patched and kept up to date
- Who is licensed to use installed software and how often it is being used

WARNING

It isn't easy for organizations to understand their software entitlements because software vendors have different licensing requirements, even within their own product suites. For example, Microsoft doesn't license its SQL database the same way it licenses Office 365. Likewise, an SAP license can be individually negotiated but must then be manually entered and reconciled in the system.

At a high level, an effective SAM program requires the following steps:

1. **Build a baseline of licenses owned by the organization.**
2. **Obtain a trusted data source of all application and software assets.**
3. **Store information about discovered assets in a central repository.**
4. **Conduct asset management intelligence on an ongoing basis.**
5. **Reconcile assets and user entitlements against valid licenses.**
6. **Manage software license pools across asset life cycles.**
7. **Integrate with other IT and business systems, such as help desk ticketing systems, configuration management databases, and security dashboards.**

TIP

Read Chapter 5 to learn what to look for in a SAM technology solution to support your SAM program.

IN THIS CHAPTER

- Centralizing software asset management
- Deconstructing complex licensing models
- Managing entitlements
- Keeping track of applications
- Dealing with software audits
- Avoiding fines and negative publicity

Chapter 2
Understanding the Compliance Dilemma

In this chapter, you learn about software license compliance challenges that can be addressed by an effective software asset management (SAM) program.

Single Source of Truth

Data management — regardless of the sources, types, and uses of the data itself — is a challenge for practically every modern organization today. Managing the sheer volume of data is a challenge in itself, but this challenge is further compounded by data quality issues including:

- Accuracy
- Consistency
- Integrity
- Redundancy

A key to addressing many of these data quality issues is to maintain a single source of truth, or system of record. For example, in many organizations, an enterprise resource planning (ERP) system is the system of record for an organization's financial data.

Establishing a single source of truth for SAM can be challenging without a SAM solution. For example, many organizations, both large and small, maintain software asset information at a departmental or business unit level. This information may be manually stored in a variety of ways, such as in a Microsoft Excel spreadsheet or a Microsoft Access database. In some cases, the IT department may make a best effort attempt to manually maintain software asset information in a help desk ticketing system or in a software distribution and management solution, such as Microsoft System Center Configuration Manager (SCCM).

Finally, the asset information that different departments or business units maintain, and their business purposes, may be different. For example, IT may maintain asset information as part of a configuration management database, a help desk ticketing system, and/or a centralized anti-malware console, among others, with different information tracked in each system. The finance department may maintain asset information to track fixed assets throughout the organization, with different rules for classifying software as either a capital expenditure or operating expense.

Designating your SAM solution as the single source of truth for software asset information can help you automate data collection and ensure that complete and accurate information about your software assets is consistently maintained, thereby reducing or eliminating many data quality issues.

Licensing Models

Software vendors have a multitude of often confusing ways to structure their application and software licenses. As discussed in Chapter 1, software licensing models aren't necessarily consistent within a single vendor's software product suites, let alone across multiple vendors. Software terms and conditions (T&Cs) that define specific right-to-use requirements also differ among vendors and can be quite confusing.

REMEMBER

A *software license* provides the right to use a software application, including the terms and conditions under which its use is permitted. An *entitlement* specifies the user or device to which a software license has been applied.

When procuring new software, negotiating terms, or preparing for a software audit, organizations must carefully consider the following licensing questions:

- Are licenses defined by named or concurrent users, devices, revenue, system, processing power, consumption, or organizational business unit?
- Are subscription licenses for desktops, Software as a Service (SaaS), servers, Internet of Things (IoT) devices, and mobile devices available and portable between on-premises, data center, cloud, and SaaS environments for a particular entity or user base?
- Are perpetual licenses restricted in any way, such as being applicable only to on-premises deployments?
- Are database licenses optimized to private or public cloud environments, such as by specifying license applications to virtual machines?
- Are entitlements part of the application model, thus requiring the acquisition of entitlements for the maximum number of concurrent users?
- Are roaming license policies in place to enable mobile users to remain in compliance when their laptops are disconnected from the corporate network?
- Will your company potentially be restricted in terms of the software features it can use depending on licensing models?
- Are the licenses subject to changes upon notification?
- What are the terms of audit rights?

One way for organizations to deal with this challenge is to have licensing experts on staff who fully understand and can work through these SAM questions upfront. This approach works particularly well when these individuals are well versed in a certain vendor's technology. At a minimum, a corporate attorney or in-house counsel should review all software licenses, contracts, and terms and conditions. But backend concerns will still bedevil

many organizations, such as whether there's a way to match complex SAM license logistics to real-world knowledge of what software is in use across the organization.

Entitlement Management

Software licensing and software entitlements are two sides of the same coin. A software license authorizes you to use a software application, subject to its terms and conditions. An entitlement essentially assigns a valid software license to a user or device.

Entitlement management can be a tricky, and often overlooked, aspect of SAM. Like software licensing, there are many different options. For example, entitlements may be assigned

- On a per-user or per-device basis
- To a named user or concurrent users
- On a single device or multiple devices

Entitlements are often defined in the software terms and conditions. Manually managing entitlements can be challenging, if not impossible.


TIP

Properly managing software entitlements is important not only to ensure software licensing compliance, but also to ensure that organizations don't overspend on software licenses (discussed in Chapter 4).

Application Tracking

Application tracking provides an organization with an understanding of how its software is used, when it's used, and by whom. This information enables inefficiencies and low-performance areas to be identified and corrected, and more effective policies and procedures to be implemented to maximize the return on investment (ROI) of an organization's assets.


REMEMBER

Application tracking is a performance management and monitoring tool that provides key information about your organization's critical resources.

Legacy asset management and metering software is limited to reporting only basic properties of devices and applications. Modern application tracking bridges the gap between the device and the user to help you better understand how your device and application assets are used. With this information, organizations can identify which applications are required for the business and eliminate nonessential software packages and their associated costs.

TIP

Creating software standards throughout an organization reduces license, support, and training costs.

Managing the Audit

Organizations that implement a clearly defined SAM strategy will gain clarity on their software assets and user entitlements and will be able to reconcile these against valid licenses. This is critical for quick and accurate responses to a software audit from a vendor or a compliance request from internal or external auditors, including organizations such as the Business Software Alliance (BSA) and the Software and Information Industry Association (SIIA). When there is no clarity, the organization will scramble to pull together information about what software has been purchased and installed when auditors come knocking at the door.

Software audits and compliance requests are common when an organization's core software applications are up for renewal. As a starting point in the negotiation process, software vendors will often require the organization to "true up" its software license counts to prove that they currently own sufficient licenses that are correctly matched to their entitlements.

However, software renewals are not the only times that an organization may be required to audit its licenses and entitlements. Most software license contracts (and/or terms and conditions) require the purchasing or leasing organization to voluntarily participate in any vendor audits or compliance requests.

Additionally, organizations such as the BSA may audit a business to determine compliance. Such an audit can even be triggered by a current or former disgruntled employee, for example.

Finally, many organizations run their own internal audit programs. These programs are helpful to proactively prepare for possible external or third-party audits, as well as for various industry

certifications, to support regulatory mandates, or as part of the due diligence process in a pending merger or acquisition.

Fines and Negative Publicity

Of course, software license compliance would be difficult to enforce if there weren't any negative consequences associated with non-compliance.

Significant fines and other penalties for software licensing violations are legally enforceable. Often worse than the financial penalty itself is the negative publicity that follows. This can have a negative impact on brand image and customer loyalty that can significantly affect profitability far in excess of the actual fines and penalties.

Although many software vendors will often work with an organization to avoid punitive fines by allowing the organization to purchase the required licenses for compliance, this can certainly weaken (or destroy) the organization's negotiating position.

THE "MILE HIGH" CITY FACES THE LOWS OF SOFTWARE LICENSING NON-COMPLIANCE

The U.S. city of Denver, Colorado, recently found itself in the software license compliance crosshairs. In 2017, it was revealed that the city had violated its licensing agreements with Oracle. After an audit, Oracle concluded that the city's over-deployment of its software would require more than $10 million to license. The city was also facing a potential $10 million penalty for overuse.

The city wound up signing a new contract with Oracle that increased its fee for Oracle software and services to close to $4 million annually, up from about $1 million. Going forward, the city of Denver plans to tighten its controls by monitoring software usage for license compliance more frequently and closely.

IN THIS CHAPTER

- Getting complete visibility of your assets
- Managing software vulnerabilities
- Controlling malware infections
- Protecting software assets in hybrid on-premises and cloud environments

Chapter 3
Recognizing the Security Risk

In this chapter, you learn how a software asset management (SAM) solution can help your organization improve its security posture by addressing some common security risks and challenges.

Knowing What You're Protecting

Identifying your information technology assets — including hardware and software — is a critical first step in protecting your organization from cybersecurity threats. Asset management is so foundational to cybersecurity, in fact, that it's the first category identified in the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework.

REMEMBER

The five core functions in the NIST Cybersecurity Framework are Identify, Protect, Detect, Respond, and Recover. The Identify function is composed of the following categories:

- Asset management
- Business environment

- Governance
- Risk assessment
- Risk management strategy
- Supply chain risk management

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19770-1:2017, *Information technology – IT asset management – Part 1: IT asset management systems – Requirements*, section 8.5 also addresses the critical role of asset management in security.

Despite its importance, identifying and managing assets is challenging for most organizations today. IT software assets are located practically everywhere, including on-premises, in data centers, in the cloud, in remote offices, on mobile devices, and on Internet of Things (IoT) devices.

A SAM solution can help you gain complete visibility of hybrid computing environments to help you not only effectively manage your software assets, but also improve your security posture. For example, an agentless SAM solution that automatically and continuously scans your network and discovers new software can augment agent-based collection methods such as those used for a centrally managed anti-malware solution.


TIP

A SAM solution can help organizations maintain compliance with certain regulations, such as the European Union's General Data Protection Regulation (GDPR), the U.S. Sarbanes–Oxley (SOX) Act and Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry's Data Security Standard (PCI DSS), and many others. For example, PCI DSS (among others) requires organizations to install anti-malware protection and patch vulnerabilities. A SAM solution can help you ensure that all your computers have anti-malware software and the latest security patches installed — and prove it!

Seeing Where Risk Is Coming From

After you know what you're protecting, you need to know what you're protecting it from. Vulnerability management programs identify known software bugs, vulnerabilities, and misconfigurations that can potentially be exploited by an attacker.

The challenge with vulnerability management programs is that they often identify literally thousands of software issues that an organization needs to address. Although vulnerability management programs typically prioritize the issues in terms of severity (for example, critical, important, or informational) and provide remediation instructions (for example, how to download and install a specific security patch), beyond a network IP address, these programs provide limited contextual information about which computers, servers, and devices need to be patched or updated.

There is often a disconnect between enterprise security and operations teams that results in costly delays between the time that vulnerabilities are identified and patched. According to research by the Ponemon Institute and ServiceNow, 57 percent of organizations that suffered a data breach in the last two years could attribute the breach to a known software vulnerability that hadn't been properly patched. The average time to patch known vulnerabilities is typically greater than 30 days between the time that a patch is available and when it's installed.

Compounding this problem further is the fact that most organizations prioritize their web-facing server applications over desktop systems. Although patching high-value, high-impact systems first is important, remember that cybercriminals will target the "path of least resistance" to get a foothold in a network environment. That "path" is most often through an end user or end user device, such as a desktop computer or mobile device.

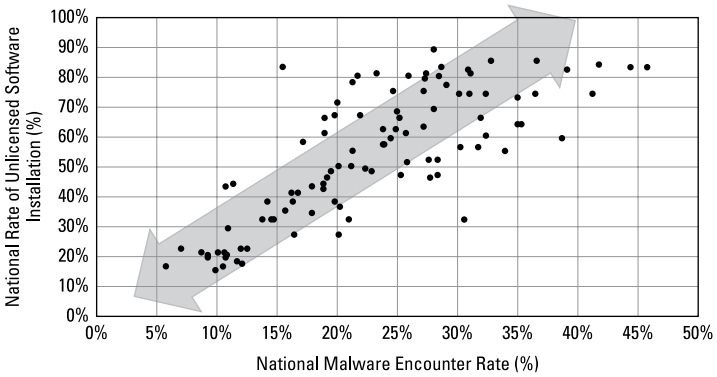
In addition to external threats, there are internal risks that a SAM solution can help identify. Many employees install unauthorized or unsanctioned software applications in a well-intentioned effort to simply be more productive or effective in performing their job functions. However, these applications can introduce vulnerabilities, particularly if the IT department is unaware of these applications and, therefore, does not routinely patch or update these applications. There is also a growing risk that an application downloaded from the Internet may contain malware. Finally, there are, unfortunately, some employees who may have malicious intent. These employees may install pirated software for gaming or entertainment purposes, or to share personal files, photos, and music using company compute resources, for example.

SAM provides an organization with ongoing, updated information about the state of its operating environment. Scans performed by SAM can be linked to Microsoft security servers to help identify missing patches and their potential consequences. This information helps identify which desktops are vulnerable and which technology assets are at risk. Other security capabilities in SAM include

- Identifying patch deficiencies, weak passwords, and port vulnerabilities
- Continually monitoring virus protection compliancy
- Visualizing open network shares and other administrative weaknesses
- Discovering asset information that is not discoverable by Microsoft System Center Configuration Manager (SCCM)

Understanding the Consequences

The consequences of unlicensed and unknown software for an organization can be severe. According to the June 2018 Business Software Alliance's (BSA) Global Software Survey, there is a high correlation between unlicensed software and malware infections (see Figure 3-1).



Source: June 2018 BSA Global Software Survey

FIGURE 3-1: Unlicensed software and malware encounters are tightly linked.

Unfortunately, unlicensed software accounts for 37 percent of all software installed on computers worldwide and 50 percent or more in the majority of countries, according to BSA.


WARNING

According to BSA, organizations that use unlicensed software on their computers have a one-in-three chance of a malware infection. A malware infection can cost a company an average of $2.4 million in damage and takes up to 50 days to fully resolve.

Malware infections in and of themselves can be quite destructive, but also serve a more devious purpose. Attackers use malware to gain access to network assets, establish persistence, and communicate with command-and-control (C&C) infrastructure to carry out their attack objectives.


TIP

A SAM solution can help organizations accurately identify installed software, which can help improve the effectiveness of anti-malware solutions that use application whitelisting to block the installation and use of software applications that aren't explicitly allowed.

Identifying Software Assets On-Premises and in the Cloud

Yet another security challenge is identifying and protecting software assets regardless of where they're installed or executed. For software assets that are installed on-premises, an automated SAM solution that automatically discovers software assets on a frequent (or continuous) basis can address issues of incomplete visibility such as when computers are turned off, not connected to the network, or located in remote locations.

In most public cloud Software as a Service (SaaS) environments, the customer can't install any sort of agent to help track their SaaS-based assets. Here again, an agentless SAM solution can help organizations track their software assets in the cloud, including licensing, entitlements, and usage.


TIP

An effective disaster recovery (DR) plan requires organizations to know what software assets they have and where they're installed so that the business can be restored to normal operations after a DR event has occurred.

IN THIS CHAPTER

- Paying only for what your organization is using
- Avoiding procurement headaches
- Getting rid of licenses for legacy software
- Identifying unused or rarely used software
- Re-assigning software resources as needed

Chapter 4
Managing Costs

In this chapter, you learn how software asset management (SAM) can help your organization save money by proactively managing its software licensing, support, and maintenance agreements.

Avoiding Overspending

Do you remember the popular slogan from just a few years ago, "There's an app for that"? It was so popular, in fact, that Apple trademarked it! Though you may not hear it so much today, it is no less a reality — there's a software application for practically everything. Knowing where those applications are installed, who is using them, and how often they're being used is a critical function of SAM that enables organizations to better manage their software budgets by matching software licenses to entitlements to ensure the most efficient allocation of software resources.

In addition to the numerous applications that businesses install on their users' desktop computers and laptops, the use of cloud-based Software as a Service (SaaS) applications has grown exponentially — and many of these SaaS applications aren't necessarily sanctioned by the business.

WARNING

Another popular mantra — associated with the usage-based SaaS model — is "pay for what you use." However, this is a bit of a misnomer. In many cases, if you don't proactively manage your SaaS license subscriptions, you still pay for the number of licenses you've reserved for your users — regardless of whether they regularly use the software.

The culture of "shadow" IT, in which individual users or lines of business procure software without the knowledge and support of IT, has become prevalent in organizations everywhere. Although there are both security and support challenges, perhaps one of the most easily quantifiable challenges associated with shadow IT is cost. When individuals, workgroups, departments, or business units procure their own software applications, they may not be leveraging preferred vendor relationships that provide the organization with economies of scale due to their overall software spend. There are also indirect costs associated with lost productivity caused by shadow IT, including

- **Technical support:** IT doesn't support the application, so individual users must resolve any issues themselves.
- **Interoperability:** Different file formats may require application data to be converted to a compatible program in order to be shared with others in the organization.
- **Shadow processes:** Key business processes that are built on unsanctioned or unauthorized software may cause business issues if the processes and associated software are only known to a few users.

REMEMBER

SAM enables organizations to avoid overspending on software by

- Identifying what software is being used, by which users, and how often so that software licenses can appropriately be matched to entitlements.
- Reducing or eliminating shadow IT software procurements so that organizations can maximize their buying power to achieve economies of scale and avoid indirect costs caused by lost productivity.
- Proactively managing SaaS subscriptions to ensure you truly pay only for what you use.

Addressing the Procurement Dilemma

Without a complete and accurate understanding of an organization's software assets, procurement becomes extremely challenging. Anticipating the software needs of the organization and planning and budgeting appropriately become impossible. Inevitably, certain software applications will be over-procured and other important applications will be overlooked. Limited budget resources may require decisions about which applications to cut from the organization's software portfolio, but without accurate information important applications may be cut.

The procurement process itself is less effective without SAM information. Organizations are in a much better negotiating position with software vendors when they know exactly what software they have and what they need. Additionally, when all of the organization's software is centrally procured, the organization has greater buying leverage and can achieve economies of scale in its licensing.

Finding "Hide and Seek" Software

Shadow IT, in which end users purchase or download and install software themselves — without IT involvement, has become a common trend in organizations everywhere. Unfortunately, these "hide-and-seek" software installations can create serious security issues for the organization (see Chapter 3), as well as IT workflow challenges.

These software installations are typically not tracked by IT, security, or finance, so they can cause inaccuracies in financial asset reporting, licensing violations, security vulnerabilities, and untracked cost expenditures. Some examples of hide-and-seek implementations include

- Legitimate commercial off-the-shelf (COTS) software installed by individuals or business groups, outside of normal IT, procurement, and security policies and processes
- Modifications to gold-master databases on authorized and unauthorized systems

- Personal applications, video games, and Software as a Service (SaaS)–based personal productivity apps that communicate outside the company firewall
- Unpatched/outdated applications, firmware, and agents
- Malicious installations causing data loss or breaches, and system crashes

Identifying Unused "Shelf-ware" Costing You Money

Organizations need to identify what software is being used and supported on a constant basis. A SAM solution can provide an organization with insight not only into potential license violations, but also into where they may be overspending on software assets — either continuing to automatically make the same payments for the use of software that is no longer of value to the organization or whose use is minimal. Equipped with this knowledge, purchasing managers can approach their software vendors to renegotiate licensing parameters and support fees for software that no longer has as many concurrent users or that doesn't need to be installed on as many devices.

With greater transparency comes the ability for IT to comprehensively rationalize assets and even retire legacy software based on evolving business requirements — and stop paying maintenance and support for software that no one realized was retired.

This information can have a huge impact for the business. After all, if you don't know what software is being used, you could be paying for software licenses and ongoing maintenance and support for hundreds, or even thousands, of unused applications installed throughout your organization. When applications are never retired — even though they should be — you could also be paying more maintenance and support costs than necessary.

Visibility into software assets and use isn't a one-shot deal either. Businesses can gain long-term control over software assets as their use fluctuates over time, including the finance department's budgeting processes and financial controls. As part of having ongoing insight, the opportunity exists to also review whether the company is using the appropriate software delivery

model — such as virtualized applications or desktops, SaaS, or other cloud service models including Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) — to ensure the highest productivity at the lowest cost.

Discovering and Reallocating Resources

Rough implementations of software by individuals and business groups outside of procurement and IT workflow processes can cost the business more money for these one-off installations and can open a Pandora's box of security and compliance issues (discussed earlier in this chapter and in Chapter 3).

Shelfware deprives other individuals and business groups in the organization of access to important applications because budget is needlessly consumed. Likewise, when software is purchased for everyone in an organization, rather than only for the individuals who actually need the software or the data it accesses, resources are wasted.

In many cases, unused or rarely used software may still be needed within an organization, but in a different department or business unit. By discovering where these software instances are installed, organizations can further reduce new software costs by reallocating software licenses to other users who need access to the software application.

Determining software distribution and usage allows IT and procurement to reallocate applications where they're most needed. Usage information can also highlight potential training issues where individual users may need a better understanding of how to efficiently use an application to perform their job functions. Finally, licensing, support, and maintenance can be renegotiated with software vendors in cases of over-acquisition of licenses, as well as during software "true-ups" when licenses are overextended.

REMEMBER

SAM technology enables organizations to identify where all their software is installed and how often it's being used so that these assets can be intelligently redeployed as needed.

IN THIS CHAPTER

- Defining core requirements and add-on modules
- Looking at business use cases and capabilities

Chapter 5
Exploring the Modern Software Asset Management Solution

In this chapter, you learn about important components and capabilities to look for in a modern software asset management (SAM) solution and different business use cases for SAM.

Software Asset Management Solution Components

When exploring a SAM solution for your organization, there are several important capabilities and components to consider. Some "must-have" capabilities and features include the following:

- **Agentless scanning technology:** Avoid the pitfalls of agent-based SAM solutions (discussed in Chapter 1) with an agentless solution that crawls the network at a predetermined start and endpoint to discover software assets, regardless of their physical or virtual locations.

- **Automated data collection:** A simple, automated method for collecting data from process tables, daemon servers, services, and all other data will help you create a complete and accurate inventory of all your software assets. This inventory will provide clear insight into your organization's software assets. The SAM technology should be able to automatically throttle up or down while staying "quiet" and running on a predetermined inventory schedule. If standard protocols are disabled, a proprietary device inspector is needed with an intelligent, independent protocol that speaks directly to the operating system or hardware device.
- **Access to other IT and business systems:** The SAM technology must be able to integrate with other systems such as enterprise resource planning (ERP), fixed asset, and order management systems to find and reconcile purchase orders.
- **Archive searches with normalized data:** The SAM tool needs to be intuitive enough to understand human requests and produce a customized report for intelligent business decisions.
- **Alert capability:** If something is detected while scanning, or the IT staff needs to know about a specific category or software publisher, alerts and incident tickets must be automatically generated.
- **Software usage and metering:** The SAM tool should be able to identify who is using which applications and how long these applications are being used, as well as the software version and from where the application is being run (locally or in the cloud).

In addition to these core capabilities, a robust SAM solution should have available add-on modules that extend its functionality, including

- Technology asset management (TAM)
- Asset integrity monitoring (AIM)
- Data center service management (DCSM)

These add-on modules are described in the following sections.

Technology asset management

TAM lets organizations automate the process of IT discovery and inventory through the intelligent collection and normalization of asset information. A TAM solution that provides seamless integration with enterprise applications and deployment allows companies to lower their operational costs, lower their life-cycle costs, and increase business efficiency and asset information accuracy.

Key capabilities, features, and benefits to look for in a TAM solution include

- **Automated technology discovery**
  - See any device connected to the network regardless of protocol.
  - Reduce time spent on inventories and audits.
  - Comply with software publisher entitlement verification audits.
- **Agentless and protocol agnostic**
  - No intrusive software or devices added to your network.
  - Discover and catalog previously undiscoverable assets.
  - See everything between two nodes on your network and their usage.
- **Out-of-the-box connectors and reports**
  - Ability to connect to configuration management databases (CMDBs), ERP, and human resource management systems (HRMS) for accurate accounting.
  - Single source of truth for all IT and business systems.
  - No additional engineering or maintenance costs to connect.
  - Tailored vendor-specific reports for entitlement reporting and contract renewals.

Asset integrity monitoring

AIM ensures the integrity of physical assets by providing a baseline of all assets, power systems, and processes in your data center or colocation facilities. It improves management and strengthens the chain of custody of all network-connected assets in your

technology stack from procurement through decommissioning. AIM identifies the following:

- Undocumented equipment
- Incorrect and unauthorized changes
- Unauthorized network connections
- At-risk equipment, firmware, and software

Key capabilities and features to look for in an AIM solution include

- **Reducing power/cooling outages and risks**
  - Simulate failures and identify critical systems that are affected.
  - Define critical assets (logical, physical, and virtual).
  - Identify application redundancies.
  - Proactively monitor power and heat in real-time, set alarms for important thresholds, and identify risk trends.
- **Reducing asset vulnerabilities**
  - Discover all assets on the network.
  - Identify known issues in software and firmware.
  - Audit for deltas and introduced vulnerable patches or assets.
  - Enforce consistent installation, management, and decommissioning processes.
- **Reducing unplanned changes**
  - See changes in assets and reconcile actual changes with expected changes.
  - Monitor unauthorized movement of assets or "outside" change processes.
  - Identify root causes that introduce risk.
  - Continuously monitor networks for unplanned changes.

Data center service management

DCSM improves transparency between organizations and systems and acts as a single source of truth. DCSM keeps data consistent by providing enriched data to IT service management (ITSM) systems.

DCSM enforces Information Technology Infrastructure Library (ITIL) and ITSM processes with integrated workflow management and ensures workflows meet change management and security guidelines, thereby ensuring compliance with service-level agreements (SLAs) and reducing risk.

DCSM also improves efficiency by making better use of IT assets and human resources. DCSM centralizes workflow process management and communications, enabling a rapid response to change requests and improving the cost effectiveness of facilities and IT infrastructure.

Key features and capabilities to look for in a DCSM solution include:

- **Prebuilt connectors**
  - Connect to major ITSM solutions such as BMC, ServiceNow, HPE, and others.
  - Extend out-of-box functionality to meet specific business needs with comprehensive application programming interfaces (APIs).
- **Bidirectional communication**
  - Increase the value and reach of your service desk change management solution.
  - Save time and effort while lowering risk between disparate change request systems.
  - Enable faster moves, adds, and changes by preplanning for asset life-cycle management.
  - Align business processes across multiple departments and software platforms.
- **Seamless integrated workflow**
  - Increase accuracy and reduce redundant data entry.
  - Automate and track install and move/add/change processes.
  - Reduce audit time and enhance ITIL and Control Objectives for Information and Related Technologies (COBIT) best-practice processes.

Software Asset Management Use Cases

A modern SAM solution must be able to support multiple business use cases for different purposes, including the following:

- **Installed software by asset:** Helps maximize the production value of your assets over time. End-to-end asset management ensures accurate knowledge of all asset and locations. Key capabilities include
  - Manage versions, licenses, and support costs by tracking installed applications.
  - Optimize software licenses to reduce redundant or wasted assets.
  - Easily identify high-security risk software or services.
  - Track legacy systems for security and retirement.
- **Software audit and license compliance:** Enables discovery of all commercial off-the-shelf (COTS) and custom applications, distribution, and user information to comply with vendor audits and regulatory reporting. Key capabilities include
  - Automate vendor licensing to meet regulatory compliance reporting requirements.
  - Reduce risk of fines and penalties and/or negative publicity for inability to track applications from software vendors.
  - Support regulatory compliance audits.
- **Risk mitigation and business compliance:** Meet your contractual obligations and avoid unexpected costs, penalties, and unfavorable publicity. Key capabilities include
  - Identification of unapproved and potentially compromising software.
  - Enforce IT and security policy compliance.
- **Sharing information across groups:** Supports sharing information across groups from a central system of record and enables complete life-cycle management. Key capabilities include
  - Track application usage to departmental chargeback.
  - Ensure ERP, HRMS, and IT asset management (ITAM) systems are synchronized from a single source of truth.
  - Reconcile software contract, purchase, and procurement records.

IN THIS CHAPTER

- Defining your strategy and getting executive support
- Automating software asset management processes and ensuring data integrity
- Matching licenses and entitlements throughout the asset life cycle
- Integrating with other systems and maximizing the results

Chapter 6
Ten Keys to Successfully Implementing a Software Asset Management Solution

Here are ten tips to help you get started today with a software asset management (SAM) solution for your organization.

Define and Communicate Your Software Asset Management Strategy

A successful SAM program begins with a clearly defined and communicated strategy. Simply implementing a new SAM tool to automate software discovery and data collection without supporting processes will inevitably lead to your SAM solution becoming another unused piece of "shelfware." Likewise, implementing

manual processes, no matter how thorough and well planned, will be unsustainable without the right SAM technology to support the processes.

It's also important to communicate your SAM strategy to your entire organization. Communicating your SAM strategy helps end users understand the importance of SAM to your organization and will help address any cultural changes that may be necessary, such as reducing "shadow" IT processes and encouraging individuals, workgroups, departments, and business units to proactively work with IT to ensure all software is properly accounted for, secured, maintained, and fully supported, and that the overall organization can effectively manage software procurement and licensing costs.

Get Executive Buy-in for Your Software Asset Management Strategy

Executive sponsorship or buy-in is critical to the success of any major organizational initiative or project and implementing a SAM solution is no exception.

Your executives should help you evangelize your solution and empower your entire organization to be a part of the solution.

REMEMBER

If IT and business leaders don't make SAM a business priority, no one else in the organization will either.

Automate Discovery, Monitoring, and Reporting

Manual discovery, monitoring, and reporting processes are not sustainable in any modern IT environment. The sheer number of software applications and the volume of change on a single computer necessitates an automated SAM solution.

TIP

Implement an agentless SAM solution to automate discovery, monitoring, and reporting of your software assets.

Store Asset Information in a Central Repository

Storing your software asset information in a central repository establishes it as a single source of truth and helps to reduce or eliminate common data quality issues such as accuracy, consistency, integrity, and redundancy.

Create a Trusted Data Source for All Software Assets

Your SAM solution should be your single source of truth for all your organization's software assets, regardless of the operating system or point of execution (on-premises, remote, cloud).

Conduct SAM Discovery on an Ongoing Basis

Your SAM solution should automatically perform discovery on a frequent, ongoing (if not continuous) basis to determine when new software is installed, existing software is updated or removed, or software entitlements change.

Reconcile Software Licenses and Entitlements

Software licenses should be reconciled with entitlements to ensure you have sufficient licenses for your users and devices and, conversely, to ensure that you don't purchase more licenses than your organization needs.

Manage Software License Pools across Asset Life Cycles

Software license pools need to be proactively managed throughout the entire asset life cycle including planning, requisition, deployment, maintenance, and retirement. As hardware assets, such as new desktop computers, are provisioned and legacy assets are decommissioned, software entitlements need to be updated accordingly.

Integrate with Other IT and Business Systems

Your SAM solution shouldn't become another silo of information within your organization. Look for a solution that easily integrates with other IT and business systems, such as help desk ticketing systems, configuration management databases, security management, and enterprise resource planning (ERP).

Leverage the Results

Use the information in your SAM solution to help your business improve security, optimize licenses, manage entitlements, negotiate software license purchases, and reduce costs.

Notes

Notes

Notes

Notes

Take control of your software assets

Software asset management needs to be a strategic focus for today's businesses. Vendor licensing requirements are too complex; software hosting environments — from the desktop to the cloud — are too numerous; the consequences of licensing noncompliance are too high; and the probability of security breaches is too great. A successful software asset management program, supported by the right processes and technology, enables businesses to optimize their software assets and make better business decisions.

Inside...

- Get complete visibility in your environment
- Create a single source of truth
- Be proactive in software audits
- Automate software discovery
- Ensure version control and patching
- Enable accurate life-cycle management
- Reduce software licensing costs

Lawrence Miller has worked in information technology in various industries for more than 25 years. He is the co-author of *CISSP For Dummies* and has written more than 150 other *For Dummies* books on numerous technology and security topics.

Go to Dummies.com®
for videos, step-by-step photos, how-to articles, or to shop!

ISBN: 978-1-119-56528-4
Not For Resale

for dummies®
A Wiley Brand

Also available as an e-book

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.