CDW PEOPLE WHO GET IT™

THE DYNAMIC DUO: SAM & SECURITY

Effective software asset management goes hand in hand with securing the IT enterprise.

Executive Summary

Enterprise computing has entered a new era. Mobility and its wide variety of devices, cloud computing, and virtualization's reach into networks and storage have all altered the definition of the enterprise network.

The fundamentals of security and management of software (the blood flowing through the network's veins) have not changed. But the new computing environment – mobile devices, cloud computing and virtualization – requires new approaches to familiar challenges.

What's more, software publishers are bringing a new energy to their own vigilance. A capricious economy has many of them stepping up the number of customer audits.

Table of Contents

As organizations deal with these software licensing challenges, they also face increasingly sophisticated security threats that continuously morph, just a step ahead of remedies to stop them.

More than ever, organizations need a comprehensive approach to security and software asset management. This white paper will examine the interconnection between SAM and security, offering practical advice on how enterprises can protect themselves and where to go for support.

The Current Situation

Security and IT asset management go hand in hand. Mobility, cloud computing and virtualization complicate them both. Mobility and cloud put more software outside the traditional network perimeter. Virtualization balloons the instances of licensed software.

Most organizations have software running both inside traditional network firewalls and outside on devices connected over wireless links. These hybrid infrastructures present challenges to both security and software asset management.

From a security standpoint, mobile devices share many of the same threats that desktop computers confront. But they also bring threat vectors of their own, such as data exfiltration from unauthorized or nonquarantined applications, mobile malware and loss of the device itself.

From a software asset management standpoint, mobile devices amplify the possibility of problems with license management, such as having more copies than needed or more than the enterprise is authorized to have under a volume license agreement.

Shifting Security Threats

The past year has produced sensational news of data losses, network penetration and malware implanted using social engineering techniques. For many, the case of former National Security Agency contractor Edward Snowden made real the insider threat.

Snowden was hardly the first. For more than a decade, the U.S. Computer Emergency Readiness Team (US-CERT) has been studying insider threats. There are two basic types: inadvertent losses that result from user carelessness or lack of training; and trusted insiders who commit deliberate malicious acts, resulting in data theft of one sort or another. One recent US-CERT study detailing insider theft of intellectual property found that it has occurred across all public, educational and commercial sectors.

US-CERT has a name for nonmalicious breaches by employees or trading partners: *unintentional insider threats*. UITs don't necessarily arrive by phishing or malware. Users manage to lose data all by themselves. They lose devices, forget to log off, visit questionable websites and work on sensitive material from untrusted devices or over unsecured networks.

Malicious insider threats are a different story. US-CERT research shows three main motivations for insiders to breach security: fraud, sabotage and theft of intellectual property. No one can read minds, but some behaviors that are detectable on the network can give clues to malicious activity. And implementing some basic security procedures can make it harder for a lone wolf to act.

Know Thy Software

Ultimately, most security issues involve software. In addition to traditional security threats, noncompliance with volume license agreements can create security problems. Further, many organizations face risks associated with unauthorized software that employees install on their devices — especially mobile devices, which some organizations do not lock down as fastidiously as they do desktop PCs.

Regardless of the source of software, IT managers should set up mechanisms for monitoring software use. The IT team needs to know what users have installed and what they are using. Knowing installations is essential to security, helping to ensure that users have only the correct software and that it is configured properly. Knowing usage patterns helps to control costs. It can also help an enterprise to avoid buying too many licenses when unused licenses are available in its inventory. Finally, knowing that all the licenses in the directory are valid, active and being used helps ensure that, should a security event occur, security staff aren't distracted by chasing down phantom machines and thus extending the remediation time.

Beyond that, data about users, applications, versions and configuration help the organization ensure data protection. It's a two-way street: Users need tools — but only authorized ones — to access internal information to do their jobs. Database and network administrators need assurance that only authorized users have access to information resources and applications that are appropriate to the users' roles.

Given the scope and dynamic nature of the information needed to manage security and licensing costs, how can an enterprise keep up? The answer is by using a software asset management solution. SAM is the only practical way an organization can maintain thorough visibility of, and control over, its software.

SAM enables structured, repeatable processes for cybersecurity, cost control and license compliance. SAM is no less necessary for users of cloud-hosted software than for organizations that host all of their software internally.

Information Security Management

Two trends have highlighted the need for enterprises to update their software management and security practices.

- Dependence on software for business operations has grown.
- Interaction with customers, constituents and trading partners has sharply increased both the amount and sensitivity of personal information that resides on an organization's IT systems.

Government agencies and commercial entities are operating in an era when software is inseparable from mission or business operations. For example, the federal government's struggle with the launch of the healthcare.gov website was technically a software development and testing issue. But it was much more than that. The healthcare insurance law (that the system supports) can't be fully enacted without a fully functioning system.

Traditionally, organizations have deployed software to replace or enhance an existing manual process. Now, missions are embodied in the software itself. Many other fields, such as transportation, retail, industrial design, drug development and energy, are similarly inseparable from the IT assets that support them.

Additionally, as online services become more widespread and more useful, they are likely to retain more personal information to enhance user or customer experiences. But those databases are juicy targets for hackers. The challenge is how to enable efficient business processes while ensuring adequate security.

The security team, for better or worse, must now address inside threats, whether malicious or inadvertent, with vigor equal to the approach they take against outside threats.

More Crucial Role for the Security Team

The growing importance of software and increasing prevalence of personal data has changed the job of enterprise security teams. For one thing, organizations face greater difficulty in their efforts to separate the job of physical protection of hardware from the cybersecurity equation.

Especially in the case of insider threats, access to server rooms and data centers requires more care even for those trusted with access. Access to a server running mission-critical software, such as a database containing sensitive information, may require two people, just as monetary checks over a certain size require two signatures.

In service-level agreements (SLAs) for cloud software hosts, organizations should consider asking for similar restrictions on access to the providers' hardware. These should apply to both the cloud company's staff and visiting customers.

Moreover, the IT shop should keep careful inventories of hardware and software under a formal IT asset management (ITAM) plan. After all, software must run on hardware, so until all of the hardware is accounted for, an organization can't fully account for its software. A well-crafted ITAM plan tracks hardware through its lifecycle. By ensuring removal of software before a machine is recycled, enterprises can better protect data and control software copies.

Inventories should include configuration information to ensure that machines are set up to the organization's specifications and stay that way. In certain regulated industries, or systems that amount to critical infrastructure, hardware configurations are a baseline requirement for layered security protocols.

Enterprises should not overlook policies for removable media. That means restricting the use of USB drives, external disks and writable media, or at least keeping logs of who uses them and when. Short of disabling all ports, this is likely to require both user training and policy changes.

Mobile fleets have expanded far beyond notebook PCs. Mobile device management software has developed to keep pace. MDM should let administrators control device security configurations, carry out policies regarding user-loaded apps, track devices and remotely wipe them.

Some organizations link cybersecurity and ITAM using radio frequency identification (RFID) systems that track when devices leave or enter facilities. In a highly secure environment, this would give IT administrators very fine-grained information about comings and goings. For example, an enterprise could tell if a person — either an authorized user or an outsider — left a facility with unauthorized equipment.

Security Process Challenges

An organization can't be sure that its protective measures are adequate unless it has a complete picture of the assets it is protecting. In the days before mobile and wireless computing, that was a simpler proposition because IT assets were fixed to a location.

ITAM expert Martin Thompson lists the five most important changes that affect assets: new projects; infrastructure upgrades; user requests; employees joining or leaving the organization; and upgrades, repairs and loss of equipment.

These changes take place in the context of unprecedented technological innovation. Mobility, cloud computing, virtualization (including of storage and the network) and ubiquitous wireless have altered the boundaries around an organization. They complicate IT asset management and its subdiscipline, software asset management, because both hardware and software assets exist inside and outside the boundary.

The multiplicity of threat vectors also adds to the security process challenge. External threats still include old-fashioned network hacking. But they also encompass sophisticated social engineering attacks as well as malware introduced through images, Java, web links and cloud services.

As IT security firm Sophos notes in its most recent *Security Threat Report*, attacks on cloud providers, advanced persistent threats, Android malware and attacks via apps and social media are emerging as the top dangers.

Vexing as the threat landscape may be, organizations can't address it effectively until they are able to account for all of their assets.

Pinpoint the Threat Vector

The SANS Institute, an IT security group, working with large organizations and government agencies, has developed a list of 20 critical controls that networks must have to be effective against cyberattacks. Several of them relate to full visibility of assets – not only their presence, but also their configurations and the applications on them. Among the controls:

- Inventory of authorized and unauthorized devices and software
- Secure configurations of all hardware, from servers to mobile devices
- Security tools installed at the network boundary and software application levels

In short, visibility is essential to strong security. The question becomes how an enterprise can achieve that visibility so that it can pinpoint the specific device through which a malicious attack is coming. In today's far-flung computing environments, automated tools are necessary to achieve this level of visibility. That's where ITAM comes in.

It's not hard to make the business case for an ITAM or asset discovery tool. Full network transparency also enables improved license management, expense control, and user service and lifecycle management of hardware and software. Such tools are available from a number of vendors including Snow Software, HP and Novell ZENworks. The latest of these tools accommodate mobile devices and the integration of public clouds into enterprise networks.

Although ITAM tools are developed to enable better IT business processes, asset discovery also gives systems administrators and security managers the information they need to remedy security events wherever on the network they originate.

A Definition of Software Asset Management

Software asset management is focused on identifying what software the organization really needs and then getting the most out of it. SAM establishes a careful approach to ensuring that an enterprise acquires, maintains, uses and eventually disposes of software in ways that promote efficiency, organizational mission, legal compliance and security.

SAM is a subset of IT asset management, which includes hardware. But SAM is growing in importance as a separate and distinct discipline. While hardware has become more commoditized over the past decade, a growing number of business functions have come under software control.

Internet Protocol (IP) communications, for example, have overtaken switched network telephony in many organizations. Whole lines of business in both the private and public sectors are, in effect, made of software – online services, healthcare record-keeping and data analytics are other examples of functions transformed or even made possible by software.

Virtualization, cloud services and mobility have not only added new software, they've complicated the process of license control and compliance.

Software spending is the fastest growing element among total IT spending, according to recent Gartner figures. So the pressure is on for organizations to sharpen their SAM skills.

What SAM Can Do

Functionally, a mature approach to software asset management gives an enterprise the tools it needs to control costs, optimize use of software and plan for the future.

As a primary requirement, SAM should give an organization 100 percent visibility into its software. Without that baseline of information, the entity won't be able to ensure licensing compliance or identify hidden costs. The SAM tool should therefore be able to detect every hardware asset on which software resides, including mobile devices.

A purchasing system can give an organization a lot of information on software acquisition history. But it won't reveal the physical location of each license, which department has it installed or whether it's actually in use. If an IP packet can reach the device, the SAM tool should be able to find out and report what software is aboard.

Given today's heterogeneous computing environments, it's wise to choose a tool that works across multiple operating systems – even for operations that might otherwise use only a single operating system. A single BlackBerry, Android or iOS device can add another OS to monitor.

A third capability of an effective SAM tool is the ability to detect instances of software inside virtual machines. Software vendors treat virtualization in a variety of ways for licensing purposes. For instance, some count total instances, virtual or physical. Others allow multiple VM copies, as long as they're on a single processor.

With a complete software picture, the IT shop can perform analysis leading to optimal software use. SAM can help an organization answer these crucial questions:

- **How does the software inventory compare with licensing rights?** This ensures compliance and avoids penalties following a vendor audit.
- **Does the organization have too many or too few licenses for each application?** This can help an entity more closely match its software spending to its needs.
- **Has the organization updated and patched the software it's running?** This allows better preparation for risks the organization may encounter.

SAM Best Practices

Because SAM is essentially a lifecycle management activity, it fits within the framework defined by the IT Infrastructure Library. Originally developed in Britain, the ITIL frameworks fall within the ISO/IEC 20000 standard. The five-volume ITIL is now in Version 3, updated in 2011.

ITIL breaks infrastructure management into procedures for service strategy, service design, service transition (for bringing ITIL discipline into the organization), service operation and continual service improvement.

Many ITIL-defined processes, such as management of service levels, availability, security, change, configuration and supplier management, apply directly to the deployment and maintenance of software.

4 Areas of Risk SAM Can Mitigate

Software asset management helps organizations overcome licensing challenges and offers several security benefits. These benefits are derived from the fact that a good SAM tool provides visibility not only into the licensed software on a network but also into rogue, pirated, unauthorized and poorly configured applications.

The chief security benefits include:

- SAM tools can find the software weeds in an organization's manicured lawn; namely, malware such as keyloggers, man-in-the-middle interceptors and password or credit card sniffers.
- Once it has found an unauthorized application, a SAM tool's blacklisting service can interrupt the use of unauthorized software.
- Because they monitor software usage by each endpoint, full-featured SAM tools allow network administrators to pinpoint users of suspect software, whether inadvertent or malicious.
- The SAM inventory function offers the benefit of detecting latent or underused titles. These might exist because of some obsolete need — or they might be the result of the purchase of an enterprise license for a title needed by only a small number of users. Either way, the IT staff will have the data it needs to see if the application can be deleted altogether, saving the support time and effort otherwise devoted to it.

ITIL Version 3 specifically supports SAM, outlined in ISO/IEC 19770-1 Standard. The standard defines processes for every step in the software lifecycle, from choosing applications and potential suppliers to eventual disposal. The latest ITIL version also encompasses license issues surrounding cloud deployments — which, according to ITIL and software asset management expert Ian Preskett, are of particular interest to software vendors these days.

No organization welcomes an audit by one of its major software suppliers. When a vendor initiates an audit, it generally suspects underlicensing. Third-party investigators usually carry out the audit. At its discretion, the supplier may merely demand that the customer purchase the requisite number of licenses, or it may go after fines in court.

The best way to avoid an external audit — or pass one cleanly — is for an organization to conduct its own audit using a SAM tool. If this audit reveals a shortfall, the enterprise has only to acquire licenses sufficient to reach compliance.

Audits should include mapping licenses to users — important in identifying unused licenses to avoid needlessly spending on new ones. Audits should also take into account all of the locations where software may exist, particularly on mobile devices and in third-party cloud providers (and, of course, within virtualized environments). The result should be a detailed report that the organization feels confident in sharing with a software vendor, proving its compliance.

SAM Uses

Modern IT staffs tend to be less hands-on than their counterparts of the early mainframe era, when computers had more mechanical components. Today's network and system administrators tend to hardware and software remotely through browser interfaces. But they face myriad dashboards showing network and application performance, endpoint issues and storage behavior.

So why use a software asset manager? One reason is that running software is the purpose of hardware. Business processes exist through software, so SAM is what ultimately keeps the enterprise running. Software has significant potential to cause financial harm when it fails or is hacked. Because the acquisition of software is the licensing of the vendor's intellectual property, license noncompliance exposes the organization to a variety of operational, legal and financial risks.

The team responsible for the operation of the software asset management toolset has a substantial list of duties.

Their responsibilities start with knowing what software populates the endpoints and other hardware — all of the titles and all of the devices. Initially, the process is a major effort at discovery, but it should move to routine maintenance once the network is mapped.

Beyond applications, the SAM solution should also reveal the operating systems running on devices. Application versions, patches and updates are often tied to specific versions of operating systems. To keep applications in shape and configured properly, the SAM tool needs to incorporate OS information.

In fact, the IT staff should consider the operating systems themselves as applications for purposes of management and security. Having a uniform operating system across device types and workgroups simplifies system administration and security.

Another crucial SAM feature links individual users to devices and software usage. Users' roles and locations change, so ensuring that individuals have the tools they need to do their jobs, while also ensuring software license compliance, becomes a dynamic activity.

SAM also helps administrators manage entitlements, a sister attribute of the rights granted by the licensing agreement. Under the entitlement function, the enterprise grants individual users permission to use any or all parts of an application. Comparing entitlements to licenses can help an organization's financial department manage chargebacks. It may give clues to license agreements that need trimming or expansion. And it provides another angle with which to view license compliance, because entitlements may not exceed licenses under certain licensing terms.

In addition, organizations always want to stay on top of any introduction of unauthorized software, whether rogue copies of licensed applications or simply untested or blacklisted packages. The SAM tool, as it performs periodic device inventory, should be able to generate reports on such software. The information should include the disallowed software's entry point, enabling the enterprise to take action to stop further occurrences.

SAM Challenges

Regardless of an individual's job, whether a user is a mechanic or chief financial officer, virtually every employee interacts with software in some way.

But that's where the certainty ends. For IT and other management functions, knowing the details of software acquisition, deployment and use is crucial. This knowledge gives the organization a powerful weapon against waste and legal liability associated with software. Unfortunately, it's easy to overspend on software and/or to slide into an out-of-compliance license situation.

Enterprises want to understand usage patterns to be sure their software spending matches their real requirements. SAM tools can help the enterprise refine its software spending and avoid needless license acquisition by answering these questions:

- Which users are actually employing the software, and how often?
- What are the patterns of usage by function? This might reveal surprising uses in one department for an application acquired for another.
- Where and with whom are dormant licenses hiding?

License True-up

Compliance with software license agreements begins with making sure the number of copies in use doesn't exceed the total number for which the organization has licenses.

Snow Software + CDW = Effective SAM

Every organization needs the capabilities of a software asset management tool as a component of its total IT asset management plan. But that doesn't necessarily mean the SAM tool must be hosted and operated locally. One alternative is a cloud-hosted SAM solution. CDW offers a cloud SAM service that utilizes Snow Software, a leading SAM vendor. Snow offers modules for license, inventory and software distribution management.

The software-as-a-service version of this solution includes an initial deep dive into an organization's network to create a complete inventory of all software running on all devices. The enterprise can specify the frequency of updates to this baseline assessment. It can also import entitlement data into the Snow software and match it to license and installation data to further ensure compliance.

CDW's Software Asset Management solution generates licensing and usage reports accepted by nearly every software publisher. And organizations that deploy this cloud solution avoid the capital expenses of the SAM software itself.

Other services offered by CDW's Software Asset Management solution include:

- Software recognition to detect whether a copy was made with authorized media or was copied without authorization
- Identification of unauthorized software that might create an unanticipated threat vector
- Visibility into operating systems and middleware to ensure that they are properly patched and up to date

Keep in mind that CDW's Software Asset Management is also offered as a hosted service and as an on-premises solution as well. And being a broad-range IT supplier, CDW also carries SAM and IT management products from several other high-profile vendors, including CA Technologies, LANDesk, Flexera Software, HP, Microsoft, Novell, ServiceNow and Symantec.

The organization must also install and use software in accordance with those terms and be able to show the vendor proof of compliance.

Terms vary from vendor to vendor, and with whether the volume license agreement is for concurrent users or total licenses. License agreements may have language pertaining to any of several conditions:

- Location of use, meaning mobile deployments might require negotiation
- Joint ventures, to address a lack of clarity over whose license agreement applies when two or more organizations collaborate using a particular application
- The number of servers on which the software may be installed, which can raise questions for virtualized environments when virtual machines are scattered across servers for backup or network performance reasons
- Departure of users
- Acquisition and divestiture (some allow for transfers, others require a new purchase)

Many major vendors' license agreements practically demand that an enterprise have a software asset management tool in place to verify compliance. One major software publisher's volume concurrent licensing agreement contains the following language:

"You must also maintain and use a license auditing and usage management tool that, at a minimum, is able to (i) track and manage usage of its Concurrent Use Licenses, (ii) govern the distribution and management of access to the Software, and (iii) enable an authorization process to allow/decline access to the software on an individual computer basis and/or incident basis. You must configure its licensing auditing and usage management tool to prevent the total number of individual users of the software from exceeding the total number of concurrent use licenses. ..."

Sound software management requires a lifecycle view, a demand that presents a couple of SAM challenges.

An important challenge is to identify software and hardware the organization no longer uses and can therefore decommission. It's important to disconnect and safely dispose of such IT assets, because if left untended, they can become avenues for malware or data theft.

Another challenge: Making efficient use of unused licenses that already exist in an organization's inventory. SAM tools keep a running count of licenses and let the IT team compare that number to the deployment figures, helping to avoid the acquisition of a new license every time IT receives a new request.

Findings from the Enforcers

An organization can do thousands — perhaps even millions — of dollars of business with a software publisher that can then turn around and sue the enterprise. That's the nature of the software business. And these days, says license and intellectual property attorney Rob Scott, it's getting worse.

Scott, of the Dallas-area law firm of Scott & Scott, says that over the past year he's noticed markedly more willingness by publishers to drag customers into federal court, suing them for copyright infringement.

"We see more lawsuits as opposed to audit or out-of-court resolutions," Scott says. "Audits are the main way of doing business. The major vendors have vowed to audit every customer."

The audits are often carried out by third parties such as trade groups, financial services firms, or hired investigators. The results can be expensive. A customer could be required to pay, as a penalty, three times the cost of the license shortfall, plus the cost of the licenses themselves.

The best strategy, Scott says, is for an enterprise to understand its own software situation and bring itself into compliance before being audited.

He has two suggestions:

1. An organization should know its licensing terms in detail. Software vendors won't forget them.

2. An organization should negotiate for the best terms it can. Favorable terms could include a no-penalty-audit agreement (although the enterprise still must buy the necessary licenses) or a multiyear period of audit forbearance. Terms should also detail what happens if the organization acquires another operation, or if it is acquired.

Scott also recommends the deployment of a SAM tool, but he adds a caveat.

"The biggest problem is that people buy a tool thinking it will help fix the problem. But they also need the skills to use them," Scott says. Otherwise, the SAM tool will produce reams of meaningless data. He says to be sure the tool can correlate device and software inventories with specific licensing terms, and that the IT staff has sufficient training in the tool.

Best Practice

Prepping for an Audit

Read this article for some tips on how to prepare for a software audit: **www.cdw.com/sam-security1**

CDW: A SAM Partner that Gets IT

Software asset management is an important task for an IT department, in part because of the complexity of SAM tools, in part because asset management involves other departments such as purchasing and finance, and in part because of the serious implications of poor asset management.

But an organization doesn't have to wade into SAM alone. Nor does it have to face the sometimes-bewildering array of licensing options without support.

CDW's expert software teams can help an enterprise plan for new technology and understand the optimal licensing terms for its situation. Software support teams consist of engineers, license specialists and requirements planning experts. They can help with a variety of software management requirements:

- Needs assessment and deployment planning so that new applications can come into the organization efficiently and productively (including configuration and making sure the most secure settings are in place)
- Contract management, to ensure that policies and practices comply with license terms
- Onsite installation of software and deployment to users

Organizations with established software inventories and images can also benefit from CDW support teams. When an enterprise wants to improve its software asset management, a CDW team will assist the IT staff with the discovery process to establish the initial baseline. Then it can guide the organization to the right choice of SAM tool. CDW's experts will conduct a detailed evaluation of how different choices apply to the organization's environment, along with a plan for buying and deploying.

Plus, CDW offers always-on telephone support and software lifecycle support, including upgrades, patches and eventual replacement.

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

snow SOFTWARE

Snow License Manager is an advanced and user-friendly SAM solution that provides you with the ability to significantly reduce licensing expenditures while mitigating compliance risk. The solution provides true software metering across all applications, allowing you to view what software is actually used and make more informed licensing decisions based on the most trustworthy data.

CDW.com

LANDESK

The ideal balance between user flexibility and readiness, LANDesk Management Suite gives you all the control you need – no matter how big or diverse your environment – to address IT concerns throughout your organization. It enables you to discover devices in your network and store information on its configurations, OS, processor speed, installed memory and more in a central database.

CDW.com

Novell

Novell ZENworks Asset Management combines sophisticated workstation inventory, network discovery, software management, license tracking, software usage and contract management into a comprehensive asset management solution with a single, unified administration and management console.

CDW.com/novell

ca technologies

CA Nimsoft Monitor helps you predict and prevent failures across your entire technology stack. The solution offers a unified monitoring view of the infrastructure so you can proactively manage your environment and meet your SLAs. Nimsoft Monitor can reduce training, deployment and management costs with an integrated monitoring solution.

CDW.com/ca

SHARE THIS WHITE PAPER

CDW PEOPLE WHO GET IT