Deloitte.

Minimizing the threat landscape through integration of Software Asset Management and Security

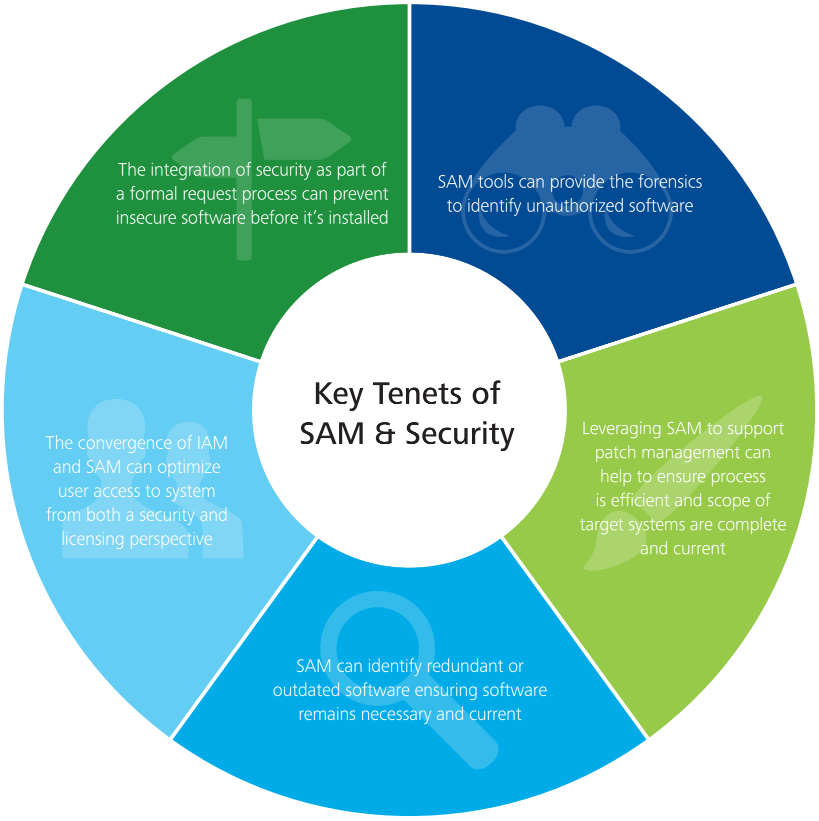
The point of intersection

As companies evolve and grow, the cost and complexity of their software assets increases in lockstep. In 2014, software licenses and maintenance costs were approximately 21 percent of companies' information technology (IT) budgets.[1] Spending on enterprise software is expected to increase 5.5 percent in 2015, compared with the previous year and then increase 6.8 percent in 2016.[2] Although software spend makes up almost a quarter of IT budgets and is projected to continue to grow, software asset management (SAM) is still not a top priority for CIOs.

SAM helps control software expenditure, capitalize on volume discounts, avoid non-compliance with licensing contracts, and deploy software more efficiently. Equally important, but less often considered, is the fact that an effective SAM initiative can help reduce organizational risk and help the enterprise establish a solid foundation to become secure, vigilant, and resilient. According to Deloitte UK's 2014 CIO survey, "strengthening risk and security management jump into the top three priorities, perhaps due to high profile security incidents in the last year."[3]

Good software asset management is crucial to effective security practices to help combat cyber-attacks that can cost companies an average of $20 million a year[4] — not to mention the long-term reputational damage any leak of customer information can cause. Although many organizational processes and tools are adequate at maintaining specific information on software assets, very few offer the intelligence required to help IT professionals manage complex networks with multiple vendors and platforms across a global IT landscape. An effective SAM practice delivers intelligence on software across the enterprise, driving value by providing managers with the necessary visibility to make the most informed cyber security decisions. When integrated, SAM and information security tools and processes become mutually reinforcing. SAM helps to minimize the attack surface of an enterprise by preventing unauthorized software from being installed, detecting and removing unwanted, redundant and unsupported software, reducing exposure to vulnerabilities through effective patch management processes and validating access controls.

As security breaches happen more frequently — and publicly — it is more imperative than ever that companies implement robust SAM practices to complement their procedures and mitigate their risk exposure.



Key Tenets of SAM & Security

The integration of security as part of a formal request process can prevent insecure software before it's installed

SAM tools can provide the forensics to identify unauthorized software

Leveraging SAM to support patch management can help to ensure process is efficient and scope of target systems are complete and current

SAM can identify redundant or outdated software ensuring software remains necessary and current

The convergence of IAM and SAM can optimize user access to system from both a security and licensing perspective

[1] "IT Metrics: IT Spending and Staffing Report, 2014" Dec 15, 2014, Gartner, Inc.
[2] "Forecast Analysis: IT Spending, Worldwide, 4Q14 Update" Feb 13, 2015, Gartner, Inc.
[3] "The Deloitte CIO Survey 2014 CIOs: At the tech-junction" Sept 22, 2014, Deloitte Touche Tohmatsu Limited
[4] "2014 Cost of Cyber Crime Study: United States" Oct 9, 2014, Hewlett-Packard / Ponemon Institute

Prevent unauthorized software before it’s installed

Individuals outside the IT department are typically more concerned with the utility and convenience of software as opposed to whether or not it is secure. If the software benefits their job, they are inclined to install and use it. Often, business units will purchase software that has not been vetted or authorized by the organization’s IT department, let alone a security specialist. SAM, when married with solid security practices, can reduce the likelihood that potentially harmful software from entering the environment.

One of the most basic SAM practices and preventative security measures—one that many companies fail to fully employ—is compiling a catalog or list of authorized software from which business units can select the most appropriate options. Maintaining a catalog of authorized software, and making sure business units only purchase from the catalog, means that IT are better positioned to place security measures (once software in the catalog is evaluated and approved by security processes) for when the software is installed. It improves the chances of monitoring the security posture of the software and eradicating unauthorized software posing risks to the organization. It is important to include security considerations when evaluating software for inclusion in the catalog. A security advisor can be involved to assess the security of the software, inclusion into the software catalog and pre-authorize the distribution through an organization’s standard request process.

The software catalog is the first line of defense; however, since a catalog won’t always include everything a business user might need, a formal software request process for both catalog and non-catalog software should be established. Enforcing a formal request process gives IT administrators better visibility into what software the business wishes to introduce into the environment, and improves their ability to forecast demand and make more informed decisions regarding installation approvals. While many organizations only include procurement within the approval process, including representatives from SAM and security is essential to getting full value out of the process. Including a security advisor as part of the software purchasing team offers a number of advantages. First and foremost, it can ensure that security considerations enter into the purchase decision. Security specialists will dig into such issues as whether the software has any known vulnerabilities, whether it is supported by the vendor, whether it is aligned with the company’s security standards, and whether the company’s network firewall rules will need to be altered in order to run the software. Ignoring these considerations can result in additional costs or significant exposure for the organization. Having a security specialist vet requested software can make it possible to address security requirements prior to installation, although continuous monitoring throughout the lifecycle of the software is still necessary as new threats and vulnerabilities emerge. Trying to remediate software vulnerabilities post-installation can be difficult and costly, and can affect the software’s functionality and ability to meet business requirements. Ultimately a formal request process gives IT a comfort level with purchase decisions. If a piece of software poses security concerns, there are several options. IT can work with the business user to perform a product rationalization analysis to determine whether there is software already in the approved catalog that can deliver similar functionality. They can purchase the software and incorporate compensating controls to mitigate risks. Or they can simply reject the request preventing vulnerable software in the environment. Regardless of the final decision, incorporating SAM and security into the software request process will ensure decisions are made with every consideration in mind.

Preventative controls

1. Maintain approved software request catalog
2. Implement formal software request process
3. Include a security & SAM advisor as part of the software purchasing team

Some key takeaways:

- Adopt security controls before installing purchased software.
- Establish a catalog of software that has been approved from both a functionality and a security perspective.
- Develop a formal request process to ensure IT is apprised of any software the business wishes to acquire.

Find and weed out the renegades

Having a formal request process reduces the likelihood that unauthorized software will enter the environment, but it's not a guarantee. Companies, therefore, need ways to ferret out rogue software that has made its way inside the network using detective controls as part of a vulnerability management program. Part of this task can be accomplished by security tools, which scan servers looking for known vulnerabilities and as a result may identify specific software that has introduced a security issue. The security tool would then notify IT administrators so it can be removed or remediated by a patch or upgrade.

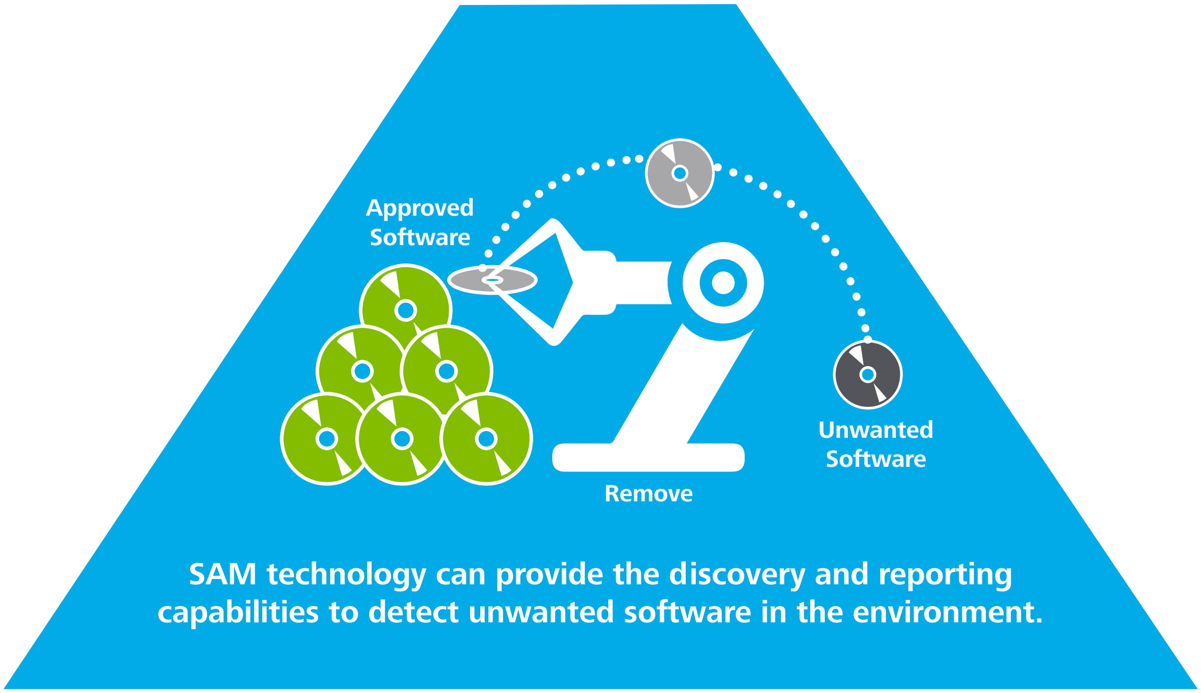
SAM discovery tools approach the same problem from a software inventory angle. They take security to the next level by scanning all software running in the environment and comparing it against both the whitelist catalog and a "blacklist" of prohibited software. For example, it is not uncommon for an employee to download a plug-in for an Internet-based game to his or her work computer, introducing a potential vulnerability or entry point to the company network. Even though the preventative control (software catalog) was configured to allow browser plug-in installations, a SAM tool can flag the unfamiliar software and automatically notify IT administrators so that it can be compared against the vulnerability scan results and removed if necessary. As the SAM tool discovers more and more unauthorized software, the blacklist grows and the removal process becomes more efficient.

Security and SAM tools can provide different kinds of intelligence that when combined and cross-referenced make it easier for the organization to reduce its vulnerability to rogue software.

Some key takeaways:

- Unauthorized software may bypass preventative controls therefore detective controls as part of a vulnerability management program are essential.
- Maintain a blacklist of software to easily identify rogue software.
- SAM tools have the capability to maintain and detect blacklist software.

SAM Technology



SAM technology can provide the discovery and reporting capabilities to detect unwanted software in the environment.

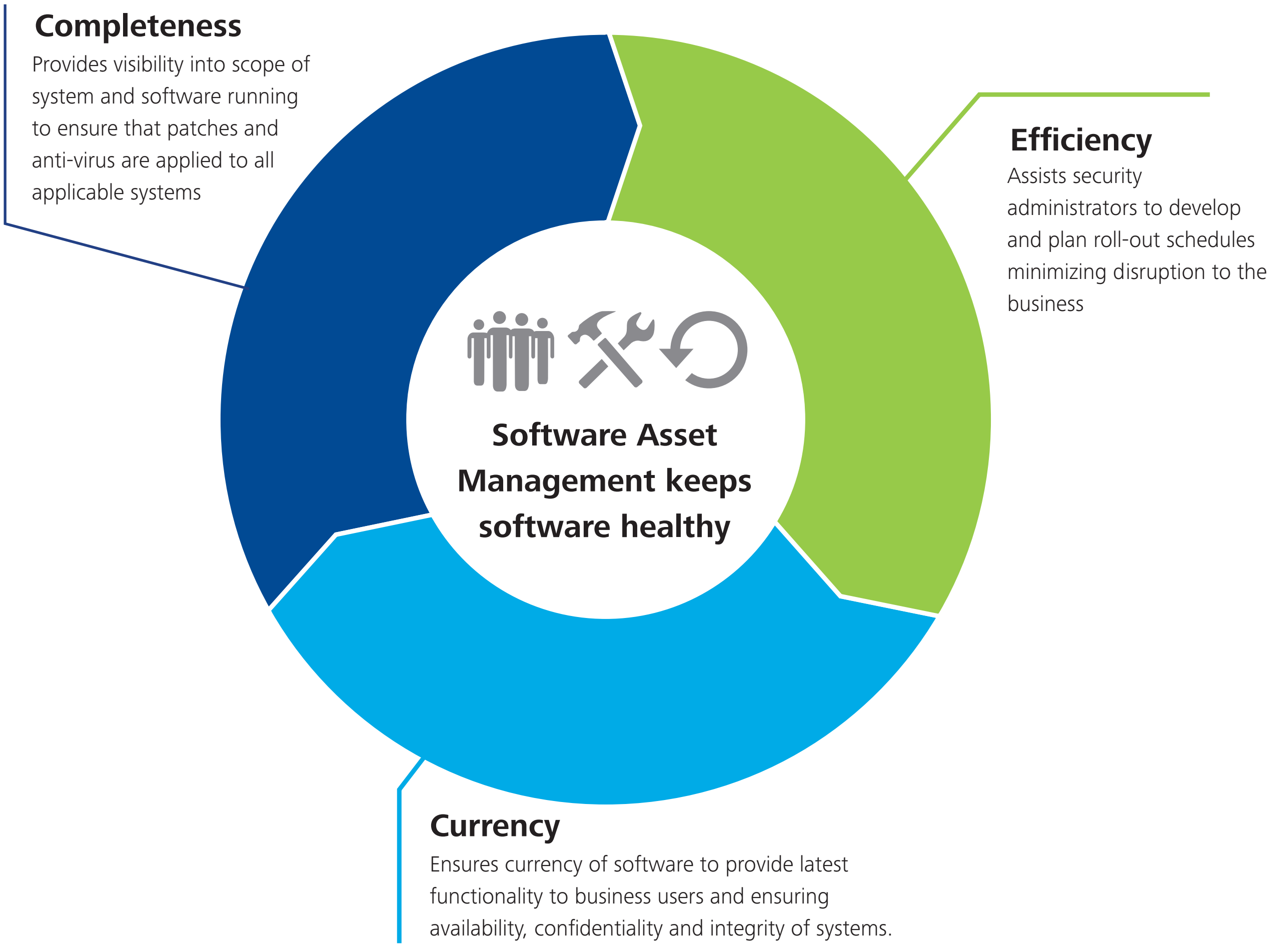
Keep software healthy

To help maintain the functionality and security of their software, vendors issue new patches, releases, and upgrades. Patch management is important to all software — across operating systems, applications, databases, and firmware. Failure to patch or upgrade can result in a vulnerability that can be exploited by hackers. Patches have varying levels of impact and criticality, and orchestrating their deployment — including outage timing, change management, and testing — adds further complexity to security management. A patch rollout may also need to be phased across multiple business units, involving other systems directly or indirectly.

The first step in planning a patch or upgrade release is determining where it needs to be deployed. By integrating asset intelligence with other data sources, SAM can provide administrators with an accurate account of where software resides in the organization, vastly improving the efficiency and effectiveness of the deployment and minimizing disruption to the business.

For example, maintaining current operating system versions through patching and upgrades can be a very large undertaking for any organization. It's also critical in maintaining a proper level of security. Understanding what operating system types and versions are deployed, where they are deployed, and in what quantities can make this process much easier. Using SAM tools to support these types of upgrade cycles can help ensure secure and efficient upgrade cycles. This is also important for critical software applications widely deployed across the environment, such as antivirus software. Ensuring antivirus agents are deployed everywhere they're supposed to be and that they're always correctly patched and up-to-date is arguably one of the most important reasons to utilize SAM tools.

Finally, because SAM involves tracking software licenses, IT administrators can use it to confirm that vendor contracts are up to date and allow for version upgrades or patches. Just because a software patch is available from a vendor, does not necessarily mean the patch is free to download and deploy. Involving a SAM advisor in this process helps ensure support contracts are in place before upgrades are deployed.



Completeness
Provides visibility into scope of system and software running to ensure that patches and anti-virus are applied to all applicable systems

Efficiency
Assists security administrators to develop and plan roll-out schedules minimizing disruption to the business

Software Asset Management keeps software healthy

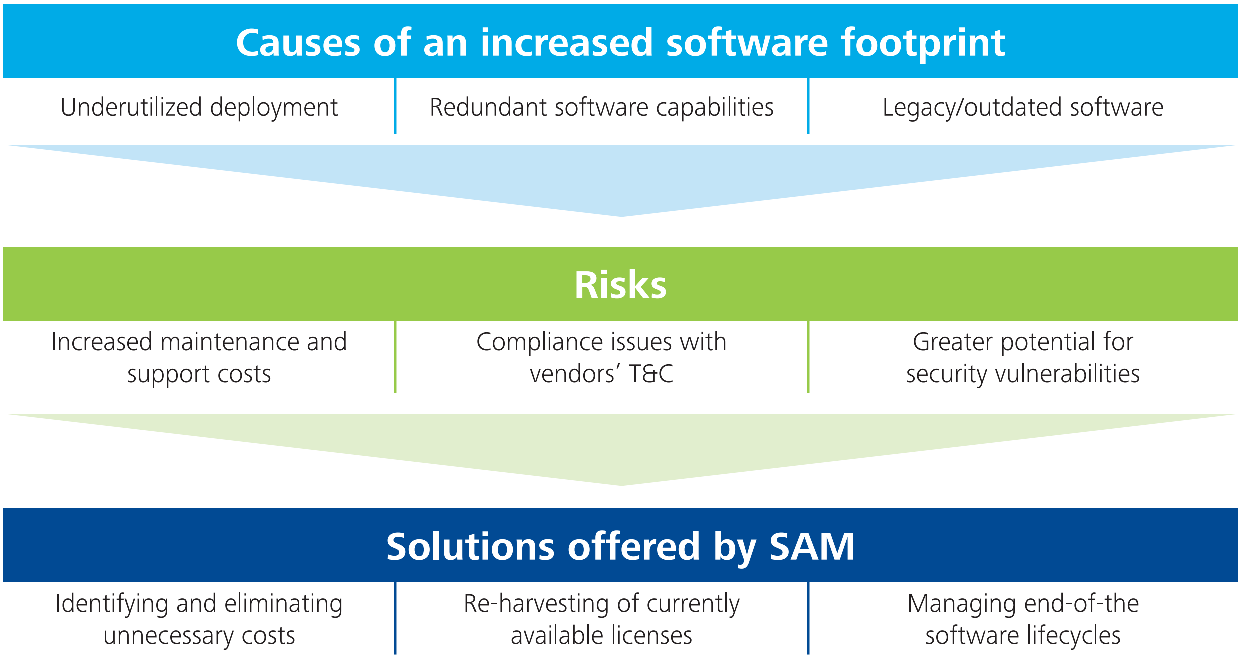
Currency
Ensures currency of software to provide latest functionality to business users and ensuring availability, confidentiality and integrity of systems.

Show redundant and outdated software the exit

Underutilized, redundant, or legacy software increases an organization's software footprint beyond what is required, increasing costs and creating unnecessary security issues. For instance, employees often install software on their desktops for specific projects and then forget about it. If IT administrators are unaware where this software resides, they may fail to upgrade it or apply security patches. Licenses may also expire, compromising compliance and incurring financial risks. Software that is not being used in one part of the organization can often be re-harvested and deployed elsewhere, saving the company money in licensing fees.

SAM, especially when it includes the capture of historical usage data, can help an organization reduce its software footprint by pinpointing redundant or underutilized software. While the removal of software is trivial from a security perspective, if there is an opportunity for re-harvesting, it is important that a security specialist determine that there are no security issues before installing the software elsewhere.

SAM is also important for managing legacy software that is nearing the end of its lifecycle. Vendors eventually stop supporting and maintaining these products, exposing them to potential security vulnerabilities that may extend to dependent software as well. Organizations with robust SAM practices can stay abreast of vendor communications and are aware of 'end of life' timelines. As a result, IT administrators can engage with the business early to plan for software decommissioning. If necessary, the process of requesting alternative software, vetting it with the security and SAM advisors, and deploying it can be started.



Causes of an increased software footprint

Underutilized deployment

Redundant software capabilities

Legacy/outdated software

Risks

Increased maintenance and support costs

Compliance issues with vendors' T&C

Greater potential for security vulnerabilities

Solutions offered by SAM

Identifying and eliminating unnecessary costs

Re-harvesting of currently available licenses

Managing end-of-the software lifecycles

Optimize user access

As users leave the organization or move into other roles, their access privileges to certain systems need to be revoked or changed. Failure to do this not only adds costs from redundant licenses, but can compromise security. Security programs often employ tools, such as identity and access management (IAM) systems, that issue user privileges based on job descriptions. Tying these security practices to a robust SAM process that not only tracks licenses, but is linked to HR systems that track users as they leave an organization, improves the efficiency of license deactivation and re-harvesting.

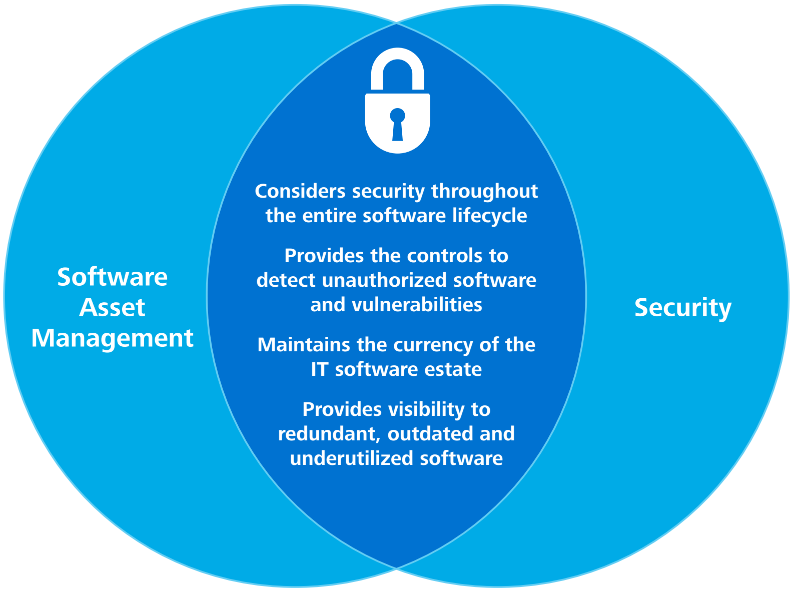
When security departments go through their annual or semi-annual recertification processes — as part of their IAM requirements — to determine who requires access to various applications, a SAM tool can provide additional intelligence on usage that either supports or rejects the findings. Together, security and SAM processes create a more accurate picture of who requires user privileges to software, which licenses should be revoked, and whether there are any rogue users accessing the system. Furthermore, when user access to software is revoked, IT can re-harvest licenses rather than procure new ones, reducing incremental spend. This all effects vulnerability management as well. When a vulnerability is detected, SAM processes can help determine the scope of the issue across the enterprise while IAM processes pinpoint who is affected and will be involved in the remediation of the vulnerability. SAM, IAM, and vulnerability management can work together to provide real-time cyber defense by expediting discovery of infected software and prioritizing the remediation process.

The convergence of SAM and IAM:

- Enables least-privileged and role-based access controls
- Provides visibility to usage of software
- Optimizes user-based licensing

Conclusion

While SAM has traditionally been thought of as simply a cost minimizing function, its potential to drive value in an organization goes far beyond that limited viewpoint. Even the best security program can be hamstrung if IT administrators don't have a firm understanding of where all of the company's software assets reside, if they are being used, and who needs access to them. Security tools focus on locating known system vulnerabilities, but they can miss potential problems if they are not deployed on all of the company's assets. That data is also underutilized if it is not compared against additional asset intelligence to identify unapproved or legacy software. By bringing inventorying capabilities into the mix, SAM complements and strengthens security tools and processes, significantly improving the company's ability to protect its data and systems and reduce operational risk.


Software Asset Management
Considers security throughout the entire software lifecycle
Provides the controls to detect unauthorized software and vulnerabilities
Maintains the currency of the IT software estate
Provides visibility to redundant, outdated and underutilized software
Security

Authors

Adam Cahn
Senior Manager
Deloitte & Touche LLP
acahn@deloitte.com

Christine Bryan
Senior Manager
Deloitte & Touche LLP
chribryan@deloitte.com

Dan Waters
Senior Consultant
Deloitte & Touche LLP
danwaters@deloitte.com

Nicholas Duston
Senior Consultant
Deloitte & Touche LLP
nduston@deloitte.com

Contributors

Tony DeVincentis
Partner
Deloitte & Touche LLP
tdevincentisjr@deloitte.com

Dave Dawson
Principal
Deloitte & Touche LLP
davedawson@deloitte.com

Derek Han
Director
Deloitte & Touche LLP
dhan@deloitte.com

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.