



Unidentified Software Syndrome

Executive Summary

Business computers contain thousands of programs in the form of executable files (EXE files) that cannot be easily identified with current industry solutions. These unknown files represent hidden risk, hidden cost and waste. The available solutions to this problem are expensive and resource intensive. With the increasing regulatory pressure from government agencies, legal action by the software industry and budget pressures to better manage software assets, executives and IT management must clean house or risk a financial blow or public relations disaster.

This problem is coming to be known as Unidentified Software Syndrome, (USS). USS persists because identifying unknown executable files as valid software is an extremely complicated process that requires specialists who have the experience to view a myriad of factors to make accurate identifications.

As a result, we predict that the future of Software Asset Management (SAM) will become an outsourced service to companies with specialists who have the tools, efficient interfaces and skills to identify all the applications in a given organizations environment. These companies will continually refine their information with each client, creating solutions for a fraction of the cost of the current methods.



Overview

“Inventory process for SAM are the basis not only for SAM, but for all of configuration management.”¹

Identification of software in an organization’s computing environment has become an increasingly critical issue in the IT and Software Asset Management industry. Heightened licensing regulations and competitive demands for efficient infrastructure management have made it crucial for organizations to maintain accurate accounts of ALL the applications installed on their systems. Unidentified applications represent potential licensing shortages, compliance issues, fines, and security risks that companies cannot afford to ignore.

As the number, variety, and complexity of applications have snowballed, it has gradually become very difficult to discover and identify applications. The industry has not found an effective, viable means of identifying EXE files and so many of them remain perpetually unidentified despite the inherent risks that they pose.

¹ ISO/IEC 19770-1:2006(E) Information technology – Software asset management 4.4.1

Unidentified Software Syndrome

Overview continued...

We call this problem Unidentified Software Syndrome. In order to effectively resolve this pervasive problem the industry must first:

- Recognize it as an industry-wide problem and define it with common terminology
- Appreciate the motivations for resolving it
- Understand the complications of software identification and why it persists as such a challenging problem
- Examine the tradeoffs and costs of the established approaches
- Identify future trends in order to take advantage of emerging solutions

Clearly identifying the problem and defining it with common terminology will enable the industry as a whole to address the issue and move forward with more effective solutions. Awareness of the specific factors involved will enable companies to take advantage of the specialized services and advancements that are emerging to address the unique challenges of software identification.



Defining the Problem — Unidentified Software Syndrome

“The objective of the Software asset identification process is to ensure that the necessary classes of assets are selected and grouped; and defined by appropriate characteristics that enable effective and efficient control of software and related assets.”²

Unidentified Software Syndrome (USS) is the unresolved problem of unidentified EXE files on business computer systems. Companies today are inundated with a huge number of applications. The typical business computer today contains over 2,500 unique EXE files while large corporations have millions of unique EXE files in their computing environments.³ Out of all those EXE files a company must be able pinpoint which ones do or do not require licensing, which ones are security or compliance risks, which ones are valuable assets and which ones are a waste of resources.

Because of the extreme complexity and diversity of program files, however, an effective means of determining this needed information has remained elusive. Automated EXE discovery tools commonly used today aren't able to determine the important specifics that companies need to know about the software on their systems. Instead, they tend to just produce a lot of convoluted, unrefined data which the user must sift through and try to interpret. Because of this, current methods are very resource intensive, demanding a great deal of time and money to deploy and maintain. As a result, many program files remain unidentified and leave companies vulnerable to licensing shortages, support issues and unknown security risks.

“Identifying software applications on computers is an amazingly complex challenge for organizations. The software asset management services industry needs to refine their products and deliver solutions that are simple, inexpensive and easy to use.” Barbara Rembiesa, President and Founder of the International Association of IT Asset Managers.

² ISO/IEC 19770-1:2006(E) Information technology – Software asset management 4.4.2.1

³ Based on an audit of over 30,000 business computers.

Understanding the Complications of EXE File Identification

An adequate means of identifying programs from their EXE files has been elusive primarily because their properties are too varied and inconsistent for the identification process to be clearly defined and automated. These inconsistencies affect nearly all aspects of program files: the content of the EXE files themselves, the properties of the installation configurations and file structures, and differing licensing options and requirements.

Meta Data Information

Most EXE files contain meta data embedded in their that provides information about the publisher, product name, version, and so forth. The problem, however, is that this meta data is not universally standardized and is frequently too inconsistent, inaccurate or insufficient to be a reliable means of identification. Ten percent or more of the EXE files on any given system do not contain any embedded publisher information at all.⁴ Even mainstream programs from major publishers sometimes lack consistent meta data. For example, a number of Adobe programs lack complete meta data, and Microsoft alone has over one hundred unique representations in the publisher field of its EXE files.

In addition to simply being unclear or incomplete, meta data can also be intentionally counterfeited to contain fraudulent information. Illegitimate programs can masquerade as legitimate software and will be misidentified by methods that rely on meta data. This both overlooks these security risks and makes it seem as though a system requires more licenses than it actually does.

Incomplete Add/Remove Registry Inclusion

Some software identification tools and services use the Windows Add/Remove Registry data to catalogue software installations. Although most major publishers conform to the Microsoft installation standards and are included in the Add/Remove Registry, many other programs do not. For example, Business Works, an accounting program, does not make an entry into the Add/Remove Registry. Many independent or illegitimate programs will also be missed by methods that rely on this information. In addition, often times a program that has been removed from a system will leave behind information in the Add/Remove Registry.

Unique Profiles and Configurations

Software can often only be accurately identified in the context of its program folders and installation configurations. Programs can vary widely in both their default configurations and the user-defined, custom options. This is particularly true for large companies where individual departments may have differing software management procedures. Identification based on these profiles is inaccurate because the many different configuration options create too many variables to predict.

³ Based on an audit of over 30,000 business computers.

Unidentified Software Syndrome

Understanding the Complications of EXE File Identification continued...

Obscure User-Installed Programs

Individual users install a multitude of non-standard programs for their own use that IT has no way of identifying. These can include virtually unknown shareware, independently developed programs, random little applets or scripts, games, or accidentally downloaded spyware, malware and viruses. These programs can be installed in obscure folders, either out of ignorance or intentional attempts to avoid detection, and generally don't conform to installation standards.

Licensing Complications of Application Suites and Packages

Simply identifying an EXE file with its application is not always enough to correctly determine licensing needs. You also need to know whether that particular installation is independent or whether it belongs to a suite's package license. It is very difficult to determine whether a program is part of a suite because of the inconsistencies in how suite software is deployed. For example there are seven different versions of the MS Office 2007 suite alone, each of which has different installation and meta data details. Discovery tools that simply identify individual programs do not take these suite packages into consideration and therefore cannot give accurate information on licensing needs.

False Positive From Active Applications

Identifying EXE files outside of the context of their environment (such as "runtime" instances) can cause multiple "counts" of a single installation copy. This can also skew perceived licensing needs.



Motivations for Resolving USS

Despite the challenges of USS, there are many strongly motivating reasons for organizations to resolve the issue and maintain accurate records of the software on their systems. These include audit protection, licensing negotiations, infrastructure control and planning, and minimization of counterproductive programs.

Audit Simplicity and Protection from Licensing Shortages

Having all software confidently identified makes audit compliance simple, efficient, and worry-free. It protects the company from getting caught with accidental licensing infringements and facing legal action, fines, and a compromised reputation. Having all the information up-front also streamlines the audit process so that valuable time and resources aren't wasted on scrambling to comply with unexpected demands.

Optimal Licensing Negotiations

Having all software accurately identified also enables a company to negotiate for optimal licensing. It allows precise software needs to be pinpointed and prevents vendors from applying pressure about possible licensing errors. This allows full license needs to be met without overpayment or waste.

Improved IT Infrastructure Control and Planning

Having comprehensive information about current software status empowers IT to manage their computing infrastructures more efficiently and proactively. It allows for accurate and cost-effective budgeting, streamlined implementation of software changes or upgrades, optimal licensing agreements, refinement of company-wide installation procedures, and minimization of waste from unutilized software assets.

Control of Counterproductive Applications

Regularly identifying program files enables companies to control undesired, counterproductive games or entertainment applications and discourage employees from wasting company time and resources on diversions. It also catches security risk software early, and prevents a build up of unnecessary applications from bogging down the system.

Previously Established Approaches to Software Identification

“The lack of standard identifiers for EXE files is one of the most daunting challenges of the industry. The costs associated with clear identification during any type of compliance auditing substantially affect the total costs of the event over any damages.” David J. Keith, Director of Government Relations and Research for the International Association of IT Asset Managers.

Until recently there have been several established approaches to dealing with software identification: ignoring the problem, outsourcing it conventional contractors, or managing it internally either by using commercial discovery tools or developing in-house discovery tools. Each has a number of relative advantages and disadvantages, but so far none of them have been able to adequately overcome the challenges of USS.

The Do-Nothing Approach

Currently the most common, default stance taken towards software identification is to turn a blind eye and ignore the issue. This is not due to negligence on the part of IT or administration, but rather due to the fact that the problem is discouragingly cumbersome. The available means of dealing with it are so resource intensive that it is often not pragmatic to implement them and it is easy to put off in the face of more critical issues.

Unidentified Software Syndrome

Motivations for Resolving USS continued...

The Do-Nothing Approach continued...

However, while unidentified files may seem trivial on a day-to-day basis, USS can put the company at significant risk and undermine major corporate events such as mergers, acquisitions, negotiations, and audits.

Pros

- Avoids a direct, up-front budget expense
- Leaves IT personnel free to focus on more immediate, core tasks.
- Provides the path of least resistance

Cons

- Leaves the company vulnerable to litigation, fines, public disclosures and security breaches that can compromise company integrity and public relations
- Can cause costly, unexpected delays and impediments in mergers, acquisitions, and negotiations
- Can entangle the company in compliance enforcement proceedings, and make audits very costly, resource intensive, and productivity crippling

Outsourcing to Traditional IT Consultants

Some companies outsource their software identification to traditional IT consultant firms. This is an expensive option because these firms employ skilled engineers who must then do tedious, time-consuming work. Since they aren't accustomed to dealing with USS, they don't have the specialized tools, methods, training, or experience to efficiently deal with its unique challenges. They must generally start the process from scratch and resort to using cumbersome spreadsheets to collect and analyze the immense amount of data produced by discovery tools. This method takes so long that it is nearly impossible to keep up to date and complete.

Pros

- Gives IT a defensible 'Best Effort' case for management
- Allows the company to deal with known third parties
- Provides a sense of safety in dealing with big name companies that have deep pockets in case of errors

Cons

- Is very expensive
- Is time consuming
- Leaves unidentified files
- Exposes internal company information
- Is quickly outdated and can't be maintained regularly

Internal Solutions Using Discovery Tools

Discovery tools search for and index EXE files and compare them to a database of known program files for identification. IT departments attempting to manage software identification internally can either use commercially available discovery tools or develop their own in-house. Each approach has slightly different advantage over the other but, in the end, both require untrained IT staff to deal with mountains of unclear data and software databases that are difficult to keep current. Of the 2,500 files on each business computer, experience shows that between 5% and 15% will be left unidentified by either commercial tools or programs developed in-house.

Commercial Discovery Tools

Use of a commercial tool, such as SMS, Altiris or Eracent, is faster to implement and doesn't burden development team resources. However, since they are not tailored to a company's particular system configuration, the details of which can vary widely, they are prone to significant errors and omissions.

The databases that the commercial discover tools use to recognize programs are perpetually incomplete and out of date. 10% to 20% of the EXE files on the average company computer will not be in the known program database and will remain unidentified. For example, one government agency that we spoke with has a six-person team dedicated solely to identifying the unknown EXE files left over from their commercial discovery tool. They do an audit every quarter and the team is never able to identify all of the files for each term before a whole new batch of unknown EXE files arrives.

Pros

- Reduces implement time
- Saves having to reinvent the wheel
- Requires minimal change in current operations
- Eliminates burden on development team

Cons

- Fails to completely resolve problem
- Uses perpetually out of date database
- Leaves a lot of work for the company
- Can require deployment of a tool agent on every computer

In-house Discovery Tools

Building an individual discovery tool can be better customized to an individual company's system but it also requires each development team to start from scratch and reinvent the wheel in an area that may be outside of their expertise. With the large learning curve presented by USS issues, this can take a very long, open-ended time to implement. It puts a resource strain on development teams in addition to the IT teams who implement them.

Pros

- Allows company to maintain control of the entire process
- Grows IT department personnel
- Keeps all information internal

Cons

- Requires a long, open-ended time to implement and ongoing maintenance of program
- Is usually outside of the core competency of IT or programming staff
- Can fail because of difficulty and other resource priorities
- Puts a significant strain on resources
- Requires dedicated staff

Unidentified Software Syndrome

Motivations for Resolving USS continued...

Costs of Internal Management

While internal management of software identification may seem more cost effective than the large upfront expense of hiring traditional consultants, it comes with significant hidden costs. When you consider how much time and resources salaried employees must spend identifying the 5% to 15% of unknown files not recognized by automated discovery tools, the costs can quickly become daunting. Assuming that it takes an average of two minutes for an IT employee to find and identify each unknown EXE file, and then the minimum total cost can be extrapolated for different system sizes as shown in the following table.

Cost of Internal Identification of Unknown EXE Files				
Organization Size (Number of computers)	250	500	1,000	5,000
Total Number of EXEs (2,500/computer)	625,000	1,250,000	2,500,000	12,500,000
Number of Unknown EXEs (5% of Total EXEs)	31,250	62,500	125,000	625,000
Time to Identify EXEs (2 minutes/unknown EXE)	62,500	125,000	250,000	1,250,000
IT Staff Cost (\$45/hr total compensation cost)	\$ 46,875	\$ 93,750	\$ 187,500	\$ 937,500



Future Trends in USS

“IT departments are constantly challenged to maintain their business environment with a streamlined staff. Software product use rights and volume licensing agreements change frequently and require a level of expertise and ongoing education that does not make sense for most organizations to maintain. By outsourcing their SAM responsibilities, clients have been able to leverage the extensive knowledge and collective experience to provide the value of SAM to their organizations while still focusing on their core business needs.” Cynthia Farren, President, Cynthia Farren Consulting.

As the demand for accurate, efficient software accountability continues to rise, the shortcomings of the previously established methods will drive the industry towards better emerging solutions. Considering the pervasiveness of USS and the complex challenges of software identification it is clear that specialization is needed to address this industry-wide need.

Regulatory Compliance Demand Will Continue to Rise

Regulatory demands and enforcement will continue to escalate and put pressure on businesses to demonstrate proper licensing compliance. This will make incomplete solutions increasingly risky. Third party verification of all system software will protect companies from this adversity and may even become a mandatory requirement.

Software Inconsistencies Will Remain Problematic

The inconsistencies and lack of standardization will continue to be a problem. With over 7,000 publishers worldwide, and more software being introduced every day, it is not realistic to expect unanimous standardization of meta data or the Add/Remove Registry. While it is important for the Software Asset Management industry to work with publishers to improve identification standards in order to mitigate the problem as much as possible, these endeavors will probably only be able to reduce unidentified files by 25%. Regardless of future improvements in standardization, there will always be some software that doesn't conform, from independent or illegitimate programs, to older versions that predate new standards. These continuing complications will require a concerted effort to find viable means of dealing with the issues in the long-term.

Move to Outsourcing – Advantages of Third Party USS Specialists

It is incredibly inefficient for every company to attempt to resolve this pervasive problem on its own. The notion that each company must individually solve this shared, complicated problem will change as the advantages of outsourcing become apparent and specialization evolves in response to industry need. USS will follow the outsourcing trends that have already been adopted for other specific infrastructure needs that are outside of the primary scope of any one company but necessary to all of them. Other key functions such as payroll, CRM, and tech support have already benefited from outsourcing to specialized third party services and software identification is no different.

Core Competency Advantages

Specialization in the unique challenges of USS allows for development and refinement of a core competency in dealing them. This produces the most effective tools and processes and provides much more complete and cost effective solutions.

Experienced USS specialists use customized tools with innovative GUI interfaces, enabling them to process and identify EXE files with much greater efficiency and accuracy. They can compile the largest, most complete software database from multiple companies, and continually update it with the most current program file information to minimize the number of unrecognized program files.

Third Party Verification

Third party verification and storage of software records satisfies stringent regulatory demands and provides external backing for audit compliance. It provides the necessary information to negotiate licensing deals with confidence and gives vendors less room to apply pressure regarding potential licensing shortages.

Unidentified Software Syndrome

Future Trends in USS continued...

Potential Expansion of USS Specialists

Once software identification is achieved these companies will also be able to branch out to include other valuable services such as licensing and contract tracking, system security, asset management, application upgrades, and OS migration assistance.

Summary of Future Trends

Outsourcing software identification to USS specialists is clearly more efficient, cost effective, and reliable than other approaches. These emerging USS services will greatly benefit the companies that take advantage of them and will become the predominating solution within the industry.



Frequently Asked Questions

What are the motivations for companies to respond to SIS?

The primary motivation is regulatory compliance, especially in the sensitive industries of banking, finance and health care. License enforcement is bringing additional pressures on companies with lax licensing controls, and we are also seeing increased audit requirements for corporate events such as mergers and acquisitions. In addition, with the competitive business landscape putting budgets under pressure, the importance of cost effective system management and minimization of wasted licensing expenses continues to grow.

How can I maintain security of our corporate information using a third party services?

The way to maintain information security in using a third party service is to send them only the data that they need without sensitive proprietary information. It is possible to identify EXE files with no corporate content. As an added level of data security, we recommend that the security practices of potential third party vendors be researched and resolved to your satisfaction

What are the pricing models and alternatives that we are likely to be offered?

This depends on the service offered. If you are considering outsourcing EXE file identification the standard pricing model you are likely to encounter is per seat or per file. Another model that can be negotiated is an annual fixed fee for the entire organization.

Remember, accurate EXE file identification is a detailed and time-consuming activity. You want to be sure that your potential vendor has an efficient system for handling the task and meeting your needs.

Why does my IT staff tell me that they have a handle on the problem and don't need additional assistance?

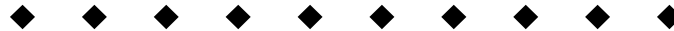
IT staffs, understandably, are reluctant to expose the extent of the hidden difficulties associated with USS. They think that the chances of having a problem with these files is minimal and downplay its importance primarily because they have thus far been unable to resolve the issues. They talk to their colleagues and all relay the same frustration. We spoke with a major bank and they admitted to having over 1 million unknown EXE files that they simply did not have the time or staff to deal with.

How do I educate IT staff that resolving USS is critical?

Providing your IT staff with the tools and methods to easily resolve USS puts them back in control of their environment. Even companies that have strict lock-down policies find that a certain percentage of employees will circumvent those regulations and expose the entire company to unidentified software.

How do I get executive management buy in?

Educating management about the many benefits, potential savings and mitigation of risk is your best method of attaining executive buy-in. As federal and state regulations become more stringent additional compliance initiatives will be mandatory. An economical solution to USS will easily receive executive management approval.



SWident – EXErelief™ Services

This white paper was written and sponsored by SWident, the exclusive provider of EXErelief services. To our knowledge SWident is the only EXE identification solution available today that uses a proprietary application and trained research specialists to provide the missing piece to the puzzle of Software Asset Management – managing unknown EXE files. Our purpose is to resolve the daunting task of accurately identifying installed software at a **cost much lower** than you are currently spending.

SWident was founded in 2006 by Herbert M. Gottlieb, formerly the CEO/President of a Attest Systems, Inc., the provider of a software discovery tool, PC computer consultant and former management consultant for Arthur Young and Alexander Grant. Herb co-authored what is today the SIIA's Certified Software Manager course, served as Director of Education for the International Association of IT Asset Manager (IAITAM), is a CPA, Certified Software Manager and Certified Hardware Manager.

For additional information please send an email to info@swident.com or call us at +1 415-493-5127.