

IT Asset Management - A Critical Component of IT Security

**An Executive White Paper
March, 2003**

Eracent, Inc.
5 Pine Bluff Road
Glenn Gardner, NJ 08826
Telephone: 631-271-3335
www.eracent.com

Abstract

Many organizations, both public and private, view the information stored on their computer systems as a critical asset. Even though it is listed on neither balance sheets, income statements nor operating budgets, most organizations would be critically disabled if their information assets were lost or destroyed. Consequently, an entire industry has been created to protect those information assets. Most organizations employ virus detectors, firewalls, isolated networks and scheduled password changes to protect their assets from outside intruders and theft. However, preventing outside access to information assets is only a partial solution to achieving a totally secure IT environment. Along with protecting the system from without, the organization needs to have full knowledge of the assets that comprise its IT asset infrastructure. Systems that inventory the IT asset infrastructure and track the location and proliferation of specific types of software and hardware need to be considered key components in maintaining the security of an organization's information. The right IT asset management system will provide the information that is fundamental to securing an organization's information assets, as well as providing information that will insure software license compliance and identify sub-standard or unprotected computer systems.

What is an IT Asset Management (ITAM) System?

IT asset management systems are designed to identify and catalog all of the intelligent devices connected to an organization's network and all of the software files resident on those systems. The systems typically span the entire network and are topology and are operating system independent. The collected information is exported to a database or repository where it can be extracted and manipulated by those departments and individuals responsible for maintaining the IT infrastructure. More capable systems will provide functions to reconcile the number of licensed software titles installed with the actual number of copies in use, alert management when unknown systems access the network, identify specific leased systems which are due to be returned and interface with organizational personnel and help desk functions to identify specific users and efficiently resolve their IT related problems.

ITAM and Security

Knowing what systems are in use, which are no longer in use and what types of software and files are resident on those systems is a fundamental component of IT system security. It is critical for an organization to know the configuration of each system in the organization, which systems have not logged onto the network for an uncharacteristic period, and hence may be missing, what systems are operating without the most current version of the selected anti-virus software, and which systems have software unauthorized for their use or clearance level. A properly configured IT asset management system will supply management with the information needed to recognize these, and other, situations.

In order to capture the data necessary to identify the scenarios described above, an IT asset management system must be able to discover the configuration details of each individual system on the network . Furthermore, use of the system cannot be dependant on the end user installing or maintaining any component of the system. Ideally the ITAM system is centrally administered but makes information widely available throughout the IT community within the organization.

Discovering Hardware

There are essentially five types of systems that attach to a network:

- Servers and Routers
- Desktop and laptop computers
- Engineering workstations
- Wireless PDA's and Wi-Fi devices
- Peripherals

For an IT organization to accurately inventory all of its assets each of these system types needs to be discovered, inventoried and tracked. That requires a system that is both platform and operating system independent, and which will deploy on the local network as well as on remote devices. With the advent of intelligent, portable, wireless devices which access organizational resources such as e-mail and intra-nets, remote devices must include those using traditional dial-up access as well as wireless access. Ideally, the ITAM system will apply a unique identifier to each discovered device so that its physical, MAC and IP address can be tracked, even if the device is moved. Moreover, the system must discover access by assets owned by the organization as well as devices privately owned by the personnel. This necessitates an auto-discovery and identification feature, which would be independent of any action taken by the end user. Very few organizations support a truly homogeneous network, and consequently the system must be able to identify different makes, models and manufacturers as well.

Security issues arise in various areas within hardware configurations:

- Component reliability
- System use and connection
- System capability

Component reliability can be a critical factor in system security, especially in the area of magnetic data storage. In the recent past several disk drive manufacturers have advised customers of problems related to their product, and some models have better reliability records than others. To insure the integrity of the data on individual systems it is incumbent on the IT organization to be able to identify the *components* of each system in use, along with the systems themselves. Being able to identify potential problems at the component level can avert a crisis resulting from lost information and can save potentially hundreds of thousands of dollars in repairs and lost productivity.

Establishing an initial inventory of physical computing systems is as simple as keeping accurate purchasing records. Determining what systems continue to be used and tracking their patterns of use is another matter. An IT asset management system that regularly monitors and captures individual system usage can give management the tools to identify systems that have been out of use for extended periods of time. In fact, it is as important to determine what has not been connected to the network as it is to identify new systems that are connected. Triggers can be installed in the ITAM system to create a low-usage alert. If the ITAM system is interfaced into the personnel system, vacation time and planned absences can be tied to systems usage reports. Monitoring low usage can provide an early notification of systems that have been illegally removed from the organizations premises, or which are simply excess and need to have the information on the disk drive removed or transferred.

As applications change and operating systems migrate, end user system capabilities need to adapt. By utilizing ITAM technology that recognizes components of individual systems IT managers can plan conversions more efficiently. This includes installation of new security software, individual firewalls and virus detection software. Any security plan that encompasses the entire organization would have weak links if every device could not utilize the new security features. ITAM systems allow planners to insure that the installed base configurations will be ready for the new security measures.

As important as discovering components is a systems ability to discover every device in the network. This requires the ITAM system to scan the entire network each time it is launched, and consolidate information collected by ITAM servers dedicated to isolated sun-networks as well. Consequently, to be truly effective the selected ITAM solution cannot have artificial limitations on the number of devices that can be inventoried at any given time. Commonly referred to as scalability, this capability needs to be engineered into the ITAM technology and should be dynamic, discovering every active device and network connection without any actions required by the end user or systems administrator.

Discovering Software

Hardware can be thought of as a repository for software. Most of a system's functionality, as well as much of its vulnerability, is found in the software. Furthermore, as data files are simply another form of software, most of the value of an IT system is embodied in software. Consequently, for an ITAM system to fully complement the organization's security program it must be able to discover, identify and inventory all of the software in the network. However, simply identifying software titles provides little practical value in terms of security. The system must be able to identify files down to the version and file type level. This is critical for several reasons.

File Types

In many organizations, certain file types have restricted uses or are limited to users in specific departments. Loss, or copying of these files could be critical to the security of an operation or the integrity of a database. By performing a routine, even daily, inventory of all files in an IT system, and then doing a compare of the locations of specific file types on past and current ITAM records, management can easily determine if any of those files are missing, have been moved to other devices, and if those devices have ever been off-premise. Using this information follow-up investigations can be done more swiftly and efficiently.

Conversely, some file types may not be authorized to reside on specific systems, such as shared access servers, personal laptops or systems that are not firewall protected. Auto-discovery of these types of files on unauthorized devices can lead to the speedy discovery of breaches in security, whether unintentional or not, and the unauthorized dissemination of restricted information whether it be inside or outside of the organization.

Applications and Software Identification

Every organization has an approved list of licensed software applications that are part of the resources made available to its personnel. The organization has trained its help-desk staff to assist end-users with problems encountered with these applications and has configured end-user hardware to efficiently run the software. In many cases an electronic software distribution (ESD) system is installed to insure that everyone in the organization has the most current release of the applications. However, individuals may load personal copies of non-supported software onto their desk-top or lap-top systems. Some of these applications are benign and have no impact on the overall network. However, some applications may interfere with the operation of the end user device due to file conflict or incompatibility. Other applications may be dangerous to the security of the networks, such as those that enable remote activation of the cameras and microphones of distant network-connected devices. The selected ITAM system must be able to detect and report the non-standard software, and flag specific applications for action. Furthermore, the ITAM system needs to identify specific versions of standard software applications. This is particularly critical in determining that all end-user devices have the most current release of selected anti-virus, anti "SPAM" and firewall software products.

In order for the ITAM system to make such identifications it needs to interface with a robust, vendor maintained database to identify the widest array of software titles and versions. Ideally the vendor would independently update this database weekly. The updates should be a combination of independent research conducted by the vendor and dynamic input on unidentified software titles, versions and files automatically sent from the ITAM system to the vendor's reference database. In this way the organization has a

constantly updated software identification database which benefits not only from its inputs, but from the vendor's actions and the input of other customers.

ITAM Administration

The data collected and held by the ITAM system is as critical to the organization as any other key databases. As such the administration of the ITAM system needs to be simplified, centralized and secure. If possible the entire ITAM system should be administered from a single server, with daily data backups made to a remote repository. Multiple ITAM servers necessitate multiple links and coordinated backups to a central repository, which could cause duplicate inaccurate entries. A single server, using resilient architecture if necessary, eliminates the weak links in the system architecture. Properly configured the single server architecture can service an entire network. If isolated sub-nets are implemented for security purposes, a single server can manage the ITAM system for each sub-net and then be polled by the main server, thus maintaining the benefits of a single-server and repository architecture.

Management Reports and Data Access

For the data collected by an ITAM system to fully augment an organization's security program, it must be both accessible and easily interpreted. A web based inquiry capability for dynamic data views, as well as the ability to store and generate standard reports is essential. Additionally the system must be able to interface with a standard report writer, such as Crystal Reports, or the report writer adopted by the organization. By making all fields addressable, management is able to interrogate the system and monitor system usage, software distribution, systems that are off-line and migration of software files and file types on a regular and ad hoc basis. Regular report analysis augments security and facilitates early action to stave off major problems.

Completing IT Security

Firewalls, anti-virus solutions and restricted access networks are now standard components of IT security solutions. However, an organization needs to have the information to detect missing systems, dangerous software and to pinpoint unauthorized access. To accomplish this a fully functional ITAM system is required. Coupled with the barriers to external threats it completes the IT security model and further insures the privacy and safekeeping of one of the organization's most critical assets, its information assets.