BUSINESS CHALLENGE

While a physical asset management system can tell you the location of a computer, it can’t answer questions like, “What operating systems are our laptops running?” and “Which devices are vulnerable to the latest threat?”

An effective IT asset management (ITAM) solution can tie together physical and virtual assets and provide management with a complete picture of what, where and how assets are being used. ITAM will enhance visibility for security analysts, which will lead to better asset utilization and security.

OUR APPROACH

ITAM is meant to make it easy for administrators to detect software changes in their network, including when unauthorized software is present, providing managers with an accurate and real-time accounting of software assets and what platforms, both physical and virtual, they are running on. The system is also intended to make it easier to answer security- and asset-related questions.

The ITAM system proposed here is designed to provide:

• a single solution that is capable of interfacing with multiple existing systems by using a standard application programming interface
• enforced software restriction policies
• the ability to know and control which assets are connected to an enterprise’s network

ITAM can answer the following questions:

• What operating systems are our computers running?
• Which devices are running a vulnerable version of software?
• What software version is running throughout the enterprise?

BUSINESS VALUE

A properly implemented and administered ITAM system can:

• enhance visibility – know where assets are and how they are configured
• improve asset management by reporting on asset utilization – save money by removing underutilized computing assets
• mitigate operational and regulatory risk by providing better accounting and reporting of assets, thereby reducing opportunities for exploitation
• reveal the software that is actually used, allowing for savings on licenses
• centralize views of enterprise-wide activity and security alerts
• join existing asset management systems with enabling technologies such as automated endpoint visibility, access and security
• allow asset-related questions to be answered quickly and accurately

» for example, questions such as “Which systems are running Windows 7 124 SP1?” can be answered in minutes with ITAM
EXAMPLE SCENARIOS

A new laptop is purchased: Physical information (e.g., barcode, serial number) is entered into ITAM, which then detects and registers a default/baseline software load. ITAM also detects and registers any software installed during provisioning by a specific department.

A server is transferred from one department to another: ITAM is used to transfer physical ownership from one department to another and then detects and registers that software specific to the original owner, which is removed. ITAM then registers and installs software for the new owner.

A virtual machine migrates between physical servers: When a hypervisor determines that a virtual machine needs to be migrated, it coordinates the move with ITAM.

Incident response and prevention: A vulnerability advisory is received regarding a particular software package. ITAM adds the software signature to a blacklist to prevent additional incidents, scans its database to determine which systems have the vulnerable software installed, and creates a report. If a patch is available, the system pushes the patch to the enterprise patch management system. Since ITAM is continuously receiving updates regarding software changes, it will know how many systems have been patched.

HIGH-LEVEL ARCHITECTURE

ITAM is a single solution with the ability to interact with existing and future access rights systems by using available communication standards and application programming interfaces.

LEARN MORE ABOUT THIS PROJECT


HOW TO PARTICIPATE

Contact financial_nccoe@nist.gov and watch the Federal Register for a notice inviting participation from the cybersecurity technology community.