



Physical Asset Management and IT Security An Xterprise White Paper

Jim Caudill, SVP Marketing & Strategy, Xterprise

Abstract

IT Security requires effective control over physical IT assets. Radio-Frequency Identification (RFID) methodologies bridge gaps left by conventional process, electronic/software, and barcode tracking solutions. Using compact, rugged, specially designed tags and flexible integration frameworks, leading RFID solutions like Clarity-ITAM™ from Xterprise help implement effective perimeter control, discovery and audit, chain of custody visibility, and end-of-life processes. Implementation is quick, with rapid financial and operational returns.

Physical Asset Management—the Missing Link in IT Security

Information Technology involves virtual assets and transactions, but security vulnerabilities may lurk in its physical foundations. Identifying, tracking, and managing risks to physical servers, storage devices, and network hardware closes security gaps electronic asset management can't address. This paper outlines Radio Frequency Identification (RFID) methods to integrate IT security across physical and virtual domains.

The stakes are high. Costs of lost or stolen hardware are significant, but can't compare to the direct and indirect costs of lost data, including damage to a company's reputation, brand, and shareholder value.

Effective defenses require physical asset control

Electronic defenses continually evolve to meet new security challenges, but experts agree that once criminals get unrestricted physical access to computers, storage media, or networks, there is little that electronic defenses can do.

That's why disciplined monitoring and management of physical IT assets is an essential component of IT security—and methods used to authenticate personnel offer a guide. To identify, authenticate, and protect physical IT assets, physical asset identifiers should be:

- *discoverable*, even when assets are powered down, off-network, or concealed
- *tamper-resistant* to avoid counterfeiting or substitution
- *compact and durable*, so they can fit and perform in IT environments
- *"smart"*: writable as well as readable, to link physical and virtual domains

Process considerations such as operational efficiency, cost, and adaptability are just as important as technology features.

IT asset management: three security scenarios

Perimeter control

Millions of dollars worth of customer records or intellectual property can walk out of a data center in stolen laptops or hard drives removed from critical servers. Identification badges control personnel, but physical perimeter controls for assets is more difficult. Few companies are willing to impose physical inspection on employees, contractors, and visitors. And as computers and storage devices proliferate and shrink, risk of loss will rise, and attempts at full physical inspection will grow even more burdensome.

Discovery and audit

Discovery and audit processes that combine physical and electronic methods identify both security gaps and underutilized assets. Assets that appear on the physical but not the electronic inventory may be powered down, disconnected, or malfunctioning. Assets that appear on the electronic but not the physical inventory may be:

- legitimate assets that escaped physical inventory
- rogue devices connected by well-intentioned but unauthorized employees
- deliberate attempts at network intrusion

Any of these represents a security vulnerability that should be addressed immediately.

Process assurance

Discovery and audit are only two critical events in an asset's lifecycle. Linking an asset's electronic and physical identities is also critical when devices are patched or upgraded, or at the end of its useful life.

Patch management across a network misses powered-down and off-network assets. Physical asset discovery—in desk drawers and file cabinets as well as at checkpoints—helps keep computing assets current, protected, and productive.

Hard drives are especially vulnerable at the end of their useful lives. Off-inventory and scheduled for destruction, they may still contain sensitive data. Physical processes should confirm their chain of custody and ultimate destruction—electronic measures are of no use with disconnected and possibly unreadable assets.

Conventional approaches

Some approaches to IT asset management neglect the physical domain entirely; others use time-consuming and unreliable methodologies that add little protection:

- *process solutions* based on purchasing records depend on fragile chains of custody, can't recover from errors, and are susceptible to asset substitution
- *electronic and software solutions* rely on network connections, can't recover disconnected or powered-down assets poorly, and are easily neutralized
- *barcode solutions* requiring line-of-site access are useless in finding misplaced assets, inconvenient for racked or embedded assets, and easy to counterfeit

Introducing RFID

Radio-Frequency Identification is the state-of-the-art in supply-chain and asset-management applications. Already proven in the management of high-value and sensitive assets, the technology offers compelling advantages for IT Security.

RFID uses either small, cheap *passive* tags as "electronic barcodes", or *active* tags that act as "smart transponders" ideal for tracking larger high-value assets. Both tag technologies are evolving quickly, and their costs continue to drop.

RFID solutions, such as Clarity-ITAM™ from Xterprise, leverage RFID frameworks like the Microsoft BizTalk RFID platform to deliver flexibility, integration and low cost of ownership for solutions that integrate across IT's physical/virtual border, and support a growing network of solution providers who can capable meet even custom requirements quickly and cost-effectively.

RFID in IT Security scenarios

In IT environments, RFID offers automated discovery with no power or line-of-sight requirement, and outperform other electronic or physical asset management solutions:

- They *defend perimeters*, detecting assets without physical inspection—and RFID-triggered video cameras effectively detect and deter theft
- They *discover and audit* even disconnected and powered-down assets, checking assets' physical identities against electronic identifiers like MAC addresses
- They help *manage* assets on- or off-line, at checkpoints as they return from the field, and document their destruction at end of their useful lives

Documented success

Companies outside IT have used RFID asset management solutions from Xterprise to secure high-value assets throughout complex lifecycles. Sotheby's auction house, for example, uses the Xterprise/Microsoft solution to monitor and track billions of dollars worth of high-value art, rare wines and antiques from receipt through transfer to the buyer. Their network includes readers at key locations and security cameras automatically triggered by RFID reads. Sotheby's eliminated the cost of manual inventory counts and time lost searching for misplaced items, improved asset security, and enhanced customer service with real-time, push-button asset tracking.

Making your decision

RFID projects are surprisingly fast, and returns on investment are almost immediate. For a first project, choose a small-scale initiative with the potential for quick improvements, and adapt RFID into existing processes so you don't try to change too much all at once.

Choose an RFID specialist rather than an IT generalist as your technology partner, so you can profit from your partner's RFID experience instead of climbing the learning curve together. RFID specialists are experts at integrating new technology into proven processes, so they can help you introduce solutions with minimal disruption.

Time to act

Large data centers at banks, brokerages, and other financial-services firms are discovering major financial and security returns from modest investments. RFID-enhanced IT asset management in busy data centers, at critical checkpoints, and throughout the lifecycles of critical assets delivers dependable physical security for the foundations of your virtual world.

About Xterprise

Xterprise Incorporated was founded in 2002 as a provider of RFID-based solutions. Today our solutions combine Microsoft platform technology, continuous improvement and lean supply chain expertise, enterprise supply chain systems integration along with RFID technology to deliver previously unachievable levels of visibility, assurance, accuracy, process improvement and value to clients. Xterprise customers include Alcon, Allergan, Bell Helicopter, Cytec Engineered Materials, Chicken of the Sea, Corning, Continental, Dairy Fresh, Dial, Eureka, ExxonMobil, General Mills, Georgia Pacific, Kraft, iGPS, Intel, L'Oreal, Nokia, Samsung, SchoellerArca Systems, ShopVac, Sotheby's, The Libman Company, The US Department of Veterans Affairs, TIMCO Aviation Services, TNT Express, Toyota Motors N.A. as well as many leading US and International financial institutions.

For additional information please call +1-972-690-9460, email info@xterprise.com or visit www.xterprise.com.