WHITE PAPER

ITAM Modernization for Securely Managing the Enterprise Attack Surface

Table of Contents

Introduction

The digital landscape is rapidly changing, making it difficult for companies to track and secure the growing number of assets used for critical business operations. Simply put, more assets and devices often translates into a larger attack surface. This White Paper offers guidance on implementing strong security measures to protect your organization and maximize the the security of your assets and the organization.

Adopting New Connected Devices

Nearly every organization relies heavily on connected assets and devices to carry out various aspects of their operations. These assets encompass a broad spectrum, ranging from managed devices such as laptops, IT, OT, IoT and medical devices. And these assets can be physical or virtual.

The Internet of Everything

This interconnectedness results in billions of devices constantly connecting to critical data and infrastructure, with new devices being added daily. The rate of adoption has become exponential, especially given the distributed nature and interconnectivity which organizations have today. It is estimated the number of connected devices will increase to over 52 billion this year (2025), with **20-30% growth YoY**, driven by increased automation, IoT adoption, and network expansion.

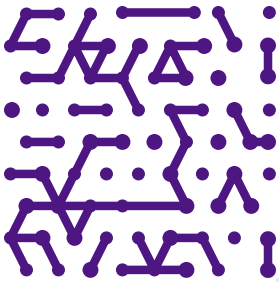
The Imperative for Enhanced Visibility, Security and Control

Asset proliferation has highlighted the need for better visibility and management of assets. Legacy tools contribute to a fragmented landscape, hindering complete visibility and real time asset information. IT and security teams struggle to understand their assets, manage risks and vulnerabilities, and enforce policies to ensure protection.

Comprehensive visibility, security and control across disparate tools are essential. Organizations must bridge gaps in asset management to gain accurate insights, enforce policies, manage risks, and protect assets for improved business resilience and continuity.

The critical question remains: do IT and security teams fully know and understand all the assets in their environment? The simple answer is **no**.

To address these challenges, organizations seeking to modernize their operations are increasingly turning to next-generation IT Asset Management (ITAM) solutions to enhance their visibility and control, safeguard against risks, and optimize digital assets for innovation, productivity, and business success in the digital age.



ITAM 101: What is it? Why is it important?

ITAM, or IT Asset Management, is the process of tracking and managing an organization's IT assets, including hardware, software, licensing, and behaviors. Gartner defines "A set of business practices that incorporates IT assets across the business units within an organization. It joins financial, contractual, and inventory functions to support lifecycle management and strategic decision-making for the IT environment."

ITAM has become increasingly important due to the complexity introduced by factors such as the proliferation of cloud services, Shadow IT, subscription-based software models, IoT, and IT/OT convergence.

Challenges Before Adoption

Before adopting IT Service Management (ITSM), organizations often face several challenges that hinder efficiency, compliance, and security. Key obstacles may include:

1. Lack of Asset Visibility & Inventory Management

- Organizations struggle with incomplete or outdated asset inventories, making it difficult to track IT, OT, and IoT devices.
- Shadow IT and unmanaged devices create security blind spots.

2. Siloed IT Operations & Disconnected Systems

- Lack of integration between IT, security, and business operations leads to inefficiencies.
- Different teams (IT, security, finance) work in isolation, causing misalignment in asset tracking and service management.

3. Manual & Inefficient Workflows

- Many organizations rely on spreadsheets and manual tracking instead of automated ITSM solutions.
- Slow, error-prone incident and request management affects IT response times and service quality.

4. Compliance & Security Risks

- Many organizations rely on spreadsheets and manual tracking instead of automated ITSM solutions.
- Slow, error-prone incident and request management affects IT response times and service quality.

5. Poor Change & Configuration Management

- No clear visibility into how IT changes affect services and security.
- Lack of automated tracking for software updates, patches, and configurations, leading to system resilience issues and vulnerabilities.

6. High Operational Costs & Budget Constraints

- Inefficient IT processes lead to higher costs for asset management and service delivery.
- Organizations lack cost optimization insights, such as tracking underutilized software or hardware.

7. Resistance to Change & User Adoption Challenges

- Employees may be reluctant to shift from legacy systems to structured ITSM frameworks.
- IT teams may lack the necessary training or expertise to implement and manage ITSM solutions effectively.

Limitations of the Legacy ITAM Approach

The legacy inventory management workflows that leverage traditional ITAM solutions available in the marketplace face several limitations and challenges that can hinder their effectiveness and adaptability in today's complex IT environments. Some of these challenges include:

1 Limited Asset Visibility

Most ITAM tools are designed to track managed IT assets such as desktops, laptops, and servers but struggle to identify unmanaged assets, including IoT devices, OT systems, and shadow IT. Additionally, they have difficulty keeping up with dynamic cloud and remote assets, particularly in BYOD (Bring Your Own Device) environments, where non-corporate devices frequently connect to the network.

2 Static & Inaccurate Asset Inventory

Because traditional ITAM depend on manual entry, scheduled scans, or agent-based discovery, asset records frequently become outdated or incomplete. This is especially problematic in modern IT environments where assets are continuously connecting and disconnecting. Furthermore, ITAM tools struggle to track ephemeral assets such as cloud instances and containers, leading to inconsistencies across IT, security, and compliance teams.

3 Siloed & Disconnected from Security Operations

Most ITAM solutions are not designed for real-time security monitoring, making them ineffective at detecting vulnerabilities, misconfigurations, or unauthorized assets as they appear. They also lack seamless integration with security tools such as SIEM, SOAR, and vulnerability management platforms, making it difficult for organizations to correlate asset data with security events or automate responses to emerging threats.

4 Poor Support for OT, IoT, and Cloud Environments

Traditional ITAM solutions struggle to scale across OT, OT IoT, and cloud environments effectively. These tools were primarily built for on-premises IT environments and often lack visibility into industrial control systems, PLCs, medical devices, and smart sensors. Similarly, organizations operating in multi-cloud or hybrid environments experience fragmented asset tracking, as legacy ITAM solutions cannot provide a unified view across different infrastructures.

5 Lack of Automated Risk & Compliance Insights

Most ITAM tools do not assess an asset's security posture in real time, leading to delayed identification of vulnerabilities and threats. As a result, organizations may fail to meet regulatory requirements because their ITAM tools cannot provide live compliance tracking or risk scoring. This limitation forces IT teams to take a reactive rather than proactive approach to asset management, delaying remediation efforts and increasing security risks.

6 High Operational Overhead & Manual Processes

Traditional ITAM solutions require extensive manual effort and have high operational overhead. IT teams often spend significant time reconciling asset records between ITAM, CMDB, and security platforms, manually updating software licenses, and ensuring hardware lifecycle tracking remains accurate. Duplicate, outdated, or missing records further complicate these processes, making ITAM inefficient for modern, fast-moving enterprises.

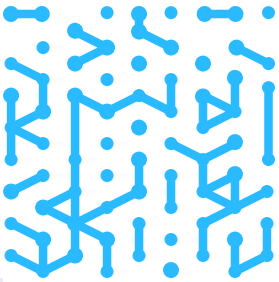
Best Practices

1. Implementing a robust **IT Asset Management (ITAM)** program requires organizations to take a strategic approach that goes beyond simple and often manual asset tracking. To maximize efficiency, security, and compliance, organizations should follow best practices that ensure full visibility, security and manageability across IT, OT, and IoT environments.
2. The foundation of an effective ITAM program is **comprehensive asset discovery and real-time visibility.** Organizations must ensure that all assets—whether IT, OT, IoT; physical or virtual—are continuously monitored, rather than relying on periodic scans or manual inventories. This real-time visibility is crucial for security, risk management, and operational efficiency. In addition to visibility, organizations must establish a **centralized asset repository** (CMDB) to maintain a single source of truth. This repository should be dynamically updated and integrated with ITSM, security, and compliance tools to avoid data silos and inconsistencies.
3. To further strengthen ITAM, organizations should **leverage automation and AI-driven** insights to minimize manual effort and human error. Automated workflows for asset discovery, software license tracking, and compliance reporting significantly improve operational efficiency. AI-powered risk assessments can help prioritize security vulnerabilities and lifecycle decisions, ensuring that high-risk assets receive immediate attention. Alongside automation, it is essential to **align ITAM with cybersecurity** initiatives by integrating asset data with vulnerability management, SIEM, and SOAR platforms as well as the rest of the organizations tech stack. This approach enhances threat detection and incident response by providing real-time insights into asset risk posture.
4. Governance is another critical component, and organizations must establish clear policies and procedures for asset management. These policies should define ownership, lifecycle management, and decommissioning processes to ensure compliance security frameworks as well as regulatory requirements. In parallel, **strong vendor and contract management** practices should be implemented to optimize software and hardware costs, track warranties, and avoid unnecessary renewals. By keeping a close watch on vendor relationships, organizations can prevent overspending and ensure that assets remain compliant with licensing agreements.
5. A key challenge in ITAM is managing the security and compliance risks associated with **shadow IT and unmanaged assets.** Organizations must take proactive steps to identify unauthorized devices and integrate them into their ITAM strategy. Without proper oversight, these assets pose significant security threats and can lead to compliance violations. **Continuous compliance monitoring** should be embedded into ITAM workflows, ensuring alignment with frameworks such as **ISO 27001, NIST, HIPAA, and GDPR.** Automated compliance checks can significantly reduce audit burdens and mitigate regulatory risks.

6. Beyond technology and processes, organizations must **foster cross-functional collaboration** between IT, security, finance, and operations teams. ITAM is not solely an IT function—it impacts procurement, risk management, and overall business strategy. Ensuring open communication and shared objectives across these teams enhances the overall effectiveness of ITAM. Finally, organizations must adopt a **future-ready approach** by continuously evaluating their ITAM strategy to accommodate emerging technologies, including AI, hybrid cloud environments, and an ever evolving threat landscape . A flexible and adaptive ITAM program ensures long-term success and resilience in an increasingly complex digital landscape.
7. Holistically, organizations must move beyond traditional asset management and establish a **strategic ITAM program that enhances visibility, security, and operational efficiency.**

ITAM Implementation Success Criteria

A well-implemented IT Asset Management (ITAM) program provides organizations with greater visibility, security, manageability and cost efficiency while ensuring compliance with regulatory standards. Tracking the success of an ITAM program requires an approach that measures its impact, identify gaps, and optimize processes over time. Organizations should establish key performance indicators (KPIs) and regularly assess their ITAM maturity to ensure continuous improvement.



The following checklist serves as a framework for organizations to evaluate the effectiveness of their ITAM program.

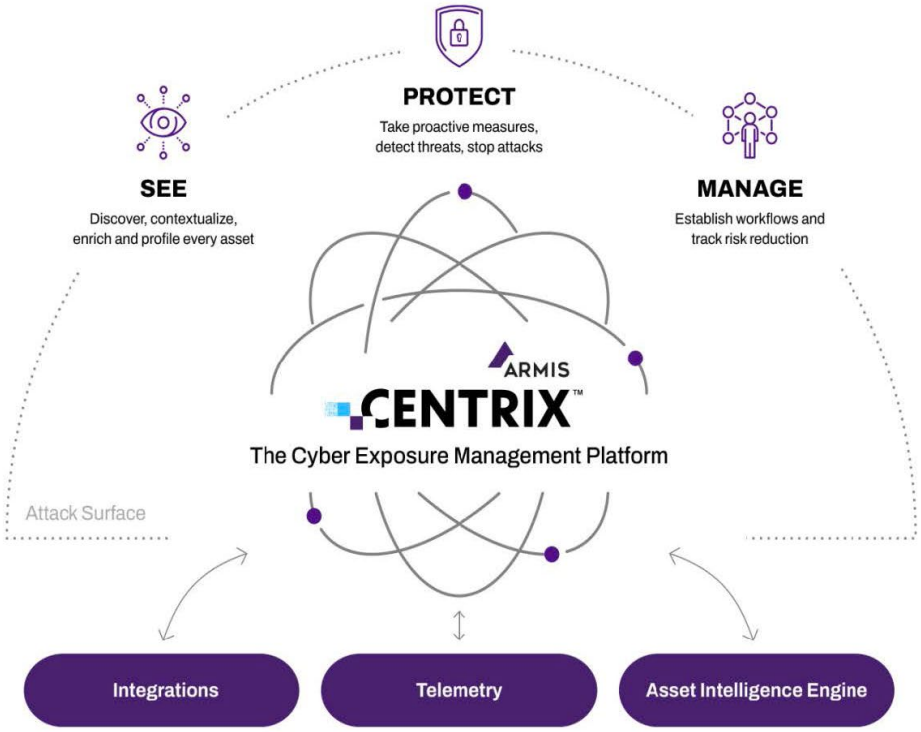
ITAM Implementation Success Checklist:

Asset Visibility & Inventory Management	• Have all IT, OT, IoT, and cloud assets been discovered and cataloged in real time? • Is there a centralized, continuously updated asset repository that eliminates silos? • Are newly connected devices automatically detected and categorized? • Can the ITAM solution track unauthorized or shadow IT assets?
Data Accuracy & Integrity	• Is asset data accurate, complete, and consistent across all integrated systems (e.g., ITSM, CMDB, SIEM)? • Are manual data entry and reconciliation efforts minimized through automation? • Does the ITAM solution provide real-time updates on asset status and changes?
ITAM & Cybersecurity Integration	• Is the ITAM solution integrated with security tools (e.g., SIEM, SOAR, vulnerability management)? • Can security teams quickly assess the risk posture of assets? • Are ITAM insights used to prioritize security patching and remediation? • Is the organization able to detect and mitigate unauthorized or high-risk devices?
Cost Optimization & Asset Lifecycle Management	• Is there visibility into hardware and software usage, preventing unnecessary purchases? • Are software licenses actively tracked? What about device utilization? • Are asset lifecycle policies in place for procurement, upgrades, and decommissioning? • Is ITAM helping to optimize maintenance and support contracts?

ITAM Implementation Success Checklist:

Compliance & Regulatory Adherence	• Is ITAM aligned with compliance frameworks such as ISO 27001, NIST, HIPAA, GDPR, and SOC 2? • Does the ITAM solution provide audit-ready reports for regulatory inspections (internal/external)? • Are automated compliance checks in place to detect and remediate non-compliant assets? • Can the organization demonstrate proper software license management for audits?
Process Automation & Efficiency Gains	• Have manual ITAM processes been automated to reduce workload and human error? • Are ITAM workflows improving IT service management efficiency (e.g., faster incident resolution)? • Does the solution provide AI-driven insights for proactive decision-making? • Has the organization seen a measurable reduction in asset-related downtime?
ITAM Governance & Cross-Team Collaboration	• Are roles and responsibilities for ITAM clearly defined across the organization? • Are teams regularly reviewing ITAM data for strategic planning and risk management? • Does the organization conduct regular ITAM performance reviews and maturity assessments? • Is executive leadership engaged in driving ITAM improvements and investments?

Armis Centrix™ for Asset Management and Security



Armis Centrix™, the cyber exposure management platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, secures, protects, and manages billions of assets around the world in real time. Armis Centrix™ seamlessly connects with existing data sources to see, secure, protect, and manage all physical and virtual assets – from the ground to the cloud – ensuring the entire attack surface is both defended and managed in real time.

Armis offers a unique approach to asset management by leveraging agentless technology, passive and active discovery methods to classify and protect all assets across an organization's network.

Key Elements of Armis Centrix™

ITAM Component (Gartner)	How Armis Centrix™ Supports ITAM
Asset Discovery & Inventory	• Provides **real-time, multi detection engines** across IT, OT, IoT, and cloud environments. • Identifies **managed and unmanaged devices**, phsical and virtualincluding shadow IT.
Lifecycle Management	• Tracks assets from **onboarding to decommissioning**. • Monitors device usage, vulnerabilities, and maintenance needs.
Financial & Contractual Oversight	• Integrates with **CMDBs, procurement systems, and ITSM platforms** for cost tracking. • Helps prevent unnecessary software or hardware expenditures by identifying unused or duplicate assets.
Compliance & Security	• Ensures compliance with **NIST, ISO 27001, HIPAA, and other regulatory frameworks.** • Identifies **risky, out-of-date, or non-compliant devices** to reduce security gaps.
Integration with IT Service & Security Management	• Syncs with **ServiceNow, Splunk, SIEM, SOAR, and other ITSM/security platforms.** • Prioritizes and automates incident response and remediation actions.
Risk & Vulnerability Management	• Assesses assets for **security risks, CVEs, and anomalous behavior.** • Provides **contextual risk** scoring to prioritize remediation efforts.
Software & License Management	• Identifies **unauthorized software** and monitors license compliance. • Detects **end-of-life or unsupported software** to mitigate risks.

Key Elements of Armis Centrix™

1 **AI-Driven platform for every industry**

Only Armis Centrix™ protects all verticals and industries including Manufacturing, Health and Medical, Information Technology, Energy and Utilities, Financial Services, Transportation, Telecommunications and Media, Public Sector and many more. One platform for every asset, and every industry.

2 **Complete device visibility**

Armis enables organizations to gain full visibility into all devices connected to their network, regardless of device type or location. This includes IoT devices, OT devices, medical devices (IoMT), building management systems (BMS), BYOD, and other similarly unmanaged devices. By providing a unified view of all assets, Armis helps organizations identify potential blind spots and security vulnerabilities. Armis Centrix™ combination of agentless, passive and active techniques of collecting data means the visibility is not a snapshot in time, it is continuous, happens in real-time and doesn't disrupt operations.

3 **Risk management**

After identifying a device, Armis calculates a risk score based on multiple factors, including risks like unpatched software versions, or known hardware exploits. Armis provides organizations with insights into the potential risks associated with each device to assess the risk posture and prioritize remediation efforts.

4 **Vulnerability Prioritization and Remediation**

Armis Centrix™ goes beyond vulnerability scanning to address the full cyber risk management lifecycle. Consolidating, prioritizing and remediating all vulnerabilities and other security findings is performed based on potential risk to the organization.

5 **Continuous monitoring and threat detection**

Armis continuously monitors device activity and behavior, looking for anomalous or malicious behavior that may indicate a security incident. By leveraging machine learning and behavioral analysis, Armis can identify potential threats, such as malware infections or unauthorized access attempts, in real-time. This proactive approach helps organizations detect and respond to security incidents swiftly.

6 **Policy enforcement and control**

Armis Centrix™ enforces security policies and control access to devices based on their risk profiles. It provides automated enforcement actions, such as isolating or blocking devices that violate security policies or pose a significant risk. This helps organizations maintain a secure and compliant environment.

7 **Integration and ecosystem support**

Integrate with a wide array of existing security tools, such as SIEM, SOAR, Identity Management (IDM), endpoint security, configuration management, virtually anything that is part of your existing technology stack. These integrations provide a holistic security ecosystem to streamline security operations, leverage existing investments, and gain a more comprehensive understanding of their overall security posture.

Measuring ITAM Success

Organizations should periodically review this checklist to assess their ITAM program's maturity and impact. Key performance indicators (KPIs) such as reduction in asset-related security incidents, cost savings from optimized asset utilization, improved compliance scores, and faster response times can further validate success.

Armis Centrix™ can help organizations automate and streamline ITAM processes by providing real-time asset intelligence, risk assessments, and deep security integrations, ensuring that ITAM remains a strategic enabler for operational and cybersecurity resilience.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial