

# IT ASSET MANAGEMENT

## Securing Assets for the Financial Services Sector

The National Cybersecurity Center of Excellence (NCCoE) addressed the challenge of Information Technology Asset Management (ITAM) for the financial services sector through collaboration with members of the IT community, including vendors of cybersecurity solutions. The example solution is detailed in NIST Cybersecurity Practice Guide, SP 1800-5. The NCCoE solution is not the only one available in the fast-moving cybersecurity technology market. Please contact us at [financial\\_nccoe@nist.gov](mailto:financial_nccoe@nist.gov) with suggestions and comments.

### CHALLENGE

Large financial services organizations employ tens or hundreds of thousands of individuals. At this scale, the technology base required to ensure smooth business operations (including computers, mobile devices, operating systems, applications, data, and network resources) is massive. To effectively manage, use, and secure each of those assets, you need to know their locations and functions. While physical assets can be labeled with barcodes and tracked in a database, this approach does not answer questions such as “What operating systems are our laptops running?” and “Which devices are vulnerable to the latest threat?”

Computer security professionals in the financial services sector told us they are challenged by the vast diversity of hardware and software they attempt to track, and by a lack of centralized control for these assets. A large financial services organization can include subsidiaries, branches, third-party partners, and contractors, as well as temporary workers and guests. This complexity makes it difficult to assess vulnerabilities, respond quickly to threats, and accurately assess risk in the first place by pinpointing the most valuable assets.

### SOLUTION

By tying existing data systems for physical assets, security systems, and IT support into a comprehensive IT asset management system, financial services companies can automatically and dynamically apply business and security rules. To demonstrate the applicability of ITAM, the NCCoE used

commercially available technology to develop an example ITAM solution that will provide the tools an organization can use to centrally monitor and gain deeper insight into an entire IT asset portfolio with an automated platform.

The work and development of this example solution is documented in NIST Cybersecurity Practice Guide 1800-5: *IT Asset Management*. Financial institutions can use some or all of the guide to implement a comprehensive ITAM system using NIST and industry standards. Commercial, standards-based products, such as the ones used in this example, are readily available and interoperable with commonly used information technology infrastructure and investments.

### BENEFITS

The example solution described in the guide has the following benefits:

- enables faster responses to security alerts by revealing the location, configuration, and owner of a device
- increases cybersecurity resilience
- provides detailed system information to auditors
- determines how many software licenses are actually used in relation to how many have been paid for, allowing for reduction in costs associated with unused or under-used physical software assets
- reduces help desk response times—staff will know what is installed and the latest pertinent errors and alerts
- reduces the attack surface of each device by ensuring that software is correctly patched

---

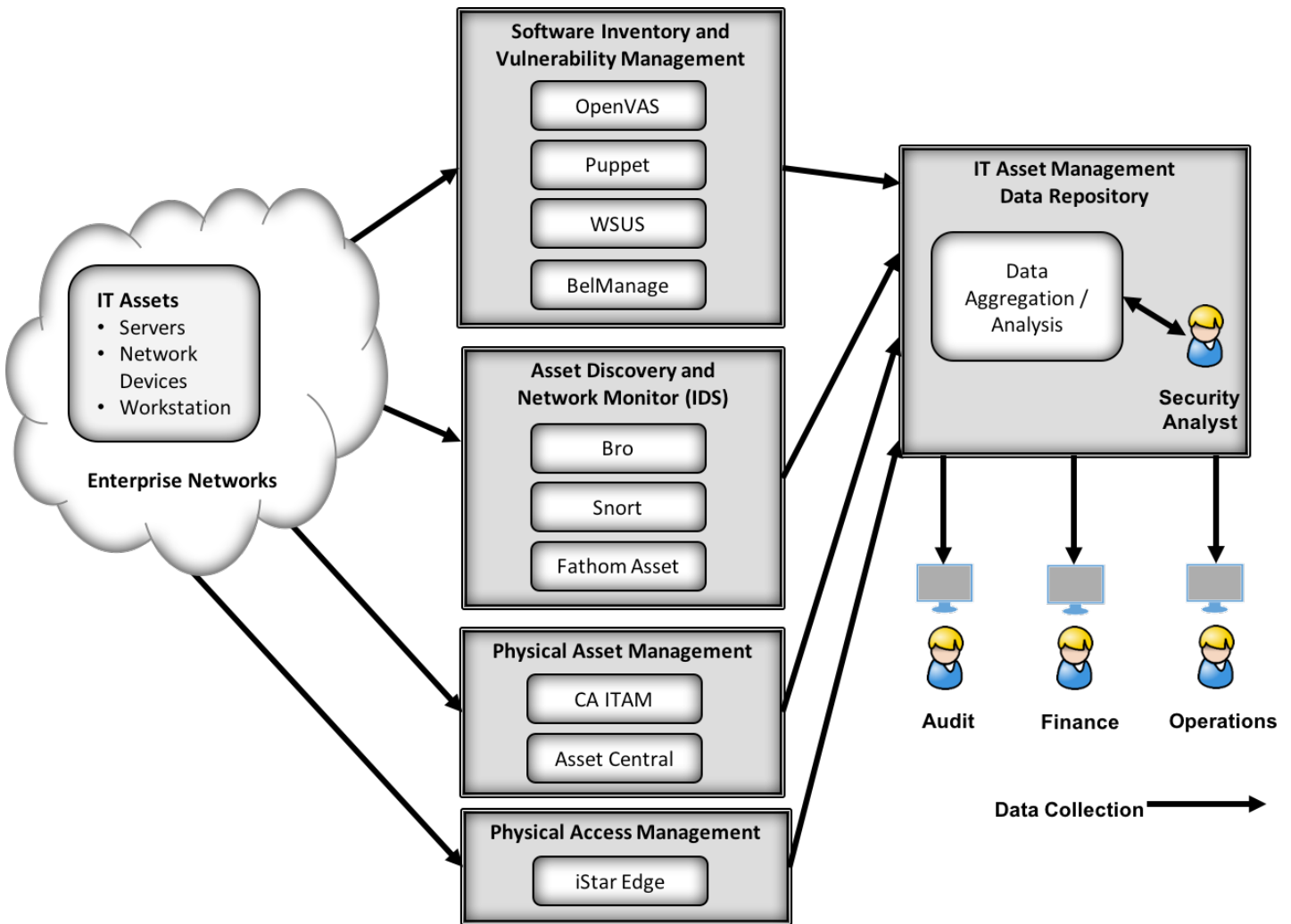
The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

**LEARN MORE ABOUT NCCoE**  
Visit <http://nccoe.nist.gov>

**CONTACT US**  
[nccoe@nist.gov](mailto:nccoe@nist.gov)  
301-975-0200

## HIGH-LEVEL ARCHITECTURE

The ITAM processes supported by our high-level architecture include: data collection, data storage, configuration management, policy enforcement, data analytics, and reporting/visualization.



## TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:



Certain commercial entities, equipment, products, or materials may be identified in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

### DOWNLOAD THE PRACTICE GUIDE

For more information about this project, visit:  
[https://nccoe.nist.gov/projects/use\\_cases/financial\\_services\\_sector/it\\_asset\\_management](https://nccoe.nist.gov/projects/use_cases/financial_services_sector/it_asset_management)

### HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, please email [financial\\_nccoe@nist.gov](mailto:financial_nccoe@nist.gov).