ivanti

SOLUTION BRIEF

Continuous Diagnostics and Mitigation Solutions for Federal Agencies

The Continuous Diagnostics and Mitigation (CDM) program is designed to reduce cybersecurity risk and improve visibility for federal agencies. Ivanti is proud to offer foundational technology supporting CDM through our asset management and patch capabilities.

IT Asset Management Meets Compliance

Seven years after program introductions, agencies are looking to modernize their initial implementations with the latest Ivanti solutions—now available on the CDM Approved Products List (APL). With Ivanti, government entities and contractors gain better visibility into their security posture, reduce their threat surface, and improve cybersecurity responsiveness—all while propelling toward compliance with government regulations ranging from FITARA to FISMA, or the MEGABYTE Act.

We can help your agency meet security requirements of the CDM program through hardware and software asset management.

Hardware Asset Management Requirements

Operational/Functional Requirements	Requirement Description	Ivanti Asset Manager
HWAM _OR-1-1	Shall identify and track hardware devices (physical and virtual) that are on the network, authorization status and who (by individual, access group, or organization) manages each device.	▪ Provides a single asset repository that unifies asset, auto-discovery, and inventory data in a single database for consistent, secure access. ▪ User-defined asset structure lets you order and group assets your way for easy access to asset data. ▪ User-configurable forms let you collect exactly the data you need to support your business processes. ▪ User-defined notification dates trigger an e-mail informing you of pending asset requirements or expiration dates. ▪ Global lists and templates provide reusable building blocks that automate form creation and data entry, giving you consistency across asset types. ▪ Inventory linking connects asset forms to current inventory data from the management database. ▪ User-defined alerts let you know it's time to perform specific actions when an expiration date occurs. ▪ Role-based administration controls and secures access to asset data to support the asset administrator, data entry, and reporting roles. ▪ Data import and export enables asset analysis using your own tools and data import helps automate asset data entry.

HWAM_OR-1-2	Shall allow manual or batch creation of Agency approved device data (e.g., through integration with external asset information repositories or through business rules).	▪ Import wizards are provided to support existing scanning tools. ▪ Provide batch imports from files or other scanning solutions, such as barcode scanners and RFID scanners.
HWAM_FR-1-1	Provide a unique identifier (which may vary by device type) that supports device persistent of any network location changes for each device on the network.	▪ Provides a unique identifier to ensure consistency by using the MAC address (or other customizable identification) to create the unique identity number. ▪ Reports thousands of unique inventory data points related to hardware and software configuration beyond traditional information and includes RAID information, power settings, voltage readings, chassis information, IPMI sensors, and more.
	Identify and collect hardware inventory information on all IP addressable devices on the network on a scheduled and ad-hoc basis as specified by authorized users.	▪ Perform an Unmanaged Device Discovery (UDD) based on network range, Active Directory domain, LDAP directory structure, SNMP, IPMI-enabled devices. ▪ Supports extended device discovery (XDD) scanning, which relies on a device agent (deployed via an agent configuration) that listens for ARP broadcasts and WAP signals on your Ivanti network, alerting administrators to any device not running the appropriate agent.
	Collect appropriate data to match actual to authorized Agency approved (i.e., authorized devices) hardware inventory, including when detected and if the device is in desired state.	▪ Tracks contracts, maintenance agreements, telephones, office equipment, and more. ▪ Allows access to all your stored asset data from a single asset repository. ▪ Discover computers on your network automatically to create detailed inventories of installed hardware and software, and monitor and report on software license usage.
	Document and record Agency-approved (i.e., authorized devices) hardware inventory information, including device type (e.g., router, workstation, firewall, printer), owner/manager, and operational status.	▪ Provide a unified solution for knowing what you have, where it is, and how it's being used. ▪ Library of asset templates lets you quickly capture key data or build custom forms to define the specific data you want to capture. ▪ Track location, asset contracts, vendor data, service level agreements, asset tags, and other information as well as non-computer assets, such as printers and cell phones. ▪ Easily relate contracts, licenses, and service agreements to specific computers or users to create a more complete picture of your physical, contractual, and financial assets.
HWAM_FR-1-2	Collect data to enable staff to physically locate the hardware devices.	▪ Asset Mapping lets admins map IP addresses that are associated with locations, such as buildings, cities, or states. ▪ Can be configured with processes that add building numbers, or any geographical location to the IT asset data by associating the asset IP address to a location. ▪ IT asset reports can easily be filtered by location, and can reflect the number of software application installations at any given location. ▪ Mapping can also be used to generalize asset information where detailed information is not required.

	Collect additional data (e.g., subcomponents, attached peripheral devices, local account information), for managed and properly configured devices and with credentials sufficient to validate actual inventory data.	▪ Perform an Unmanaged Device Discovery (UDD) against all IT-based assets with a network address. ▪ Retrieve any assets that are physically on the network, including desktops, servers, laptops, printers, and routers.
	Detect the type of each hardware device based upon its network behavior.	▪ Perform discovery on SNMP and IPMI-enabled devices.

Software Asset Management Requirements

Operational/Functional Requirements	Requirement Description	Ivanti Asset Manager
SWAM _OR-1-1	Shall identify and track software products that are on the device for each hardware device (physical and virtual) on the network within Agency system boundaries, authorization status, and who (by individual, access group, or organization) manages each software product.	▪ Discover everything that connects to the network, including detailed hardware information such as manufacturer and part numbers. ▪ Get information about the memory, hard drive, monitor, software, and more. ▪ Perform discovery operations by connecting to existing network data located in network directories such as Active Directory.
SWAM_OR-1-2	Shall allow manual or batch creation of authorized software data (e.g., through integration with external asset information repositories or through business rules).	▪ Connectors and Import wizards support existing scanning tools and provide batch imports from files or other scanning solutions, such as barcode scanners and RFID scanners.
SWAM_FR-1-1	Provide a unique identifier (e.g., Common Platform Enumeration [CPE], Software Identification Tags) for each software product that is used to identify instances of installed software products and components, including version number, across devices on the network.	▪ A unique identifier is provided for each asset across the entire network, including software assets and their version number.
	Identify and collect software inventory information on Agency-defined and scoped devices on the network on a scheduled and ad hoc basis as specified by authorized users.	▪ Authorized users can discover and monitor applications, including the execution of all applications that are run on a device. ▪ Information collected includes utilization, device Name, Date/Time Last Used, Last User, # Executions, Duration (minutes), Days Since Last Used, and Discovery Date.
	Collect additional data (e.g., software components, component digital fingerprints) for managed and properly configured devices, with credentials sufficient to validate actual inventory data.	▪ Inventory scanning process provides a comprehensive listing of all applications that reside on a device, and information about which of them have been executed. This is accomplished by scanning the desktop, analyzing shortcuts, and monitoring the MSI database for any and all applications that reside on the box regardless of user profile. ▪ Automated process is configurable to monitor custom applications, files, or utilities. ▪ Flexible monitoring makes it easy to associate any file or series of files with a given application, improving visibility to patch levels and version differences.

	Document and record software inventory information, including product name, owner/manager, and operational status.	▪ User-defined asset structure lets you order and group software assets for easy access to asset data. ▪ User-configurable forms let you collect the data you need to support your business processes. ▪ User-defined notification dates trigger an e-mail informing you of pending asset requirements or expiration dates. ▪ Global lists and templates provide reusable building blocks that automate form creation and data entry, giving you consistency across asset types.
SWAM_FR-1-2	Malware (including, as configured, all on whitelisted software, and software not behaving as expected) at a rate comparable to existing anti-virus products, and provide a means for removing malware in time to prevent it from executing.	▪ Scan devices and look for all applications, patches, drivers, and utilities that are on the device. ▪ Software inventory data provides excellent analytical detail when performing proactive maintenance. ▪ Queries can be set to define all devices that have older software, patches, malware, or antivirus versions.
	Whitelist changes and software installation actions.	▪ Application “whitelisting” allows IT to approve a set of applications that users can run, consistent with licensing constraints and parameters set by the organization. ▪ Option to base each allow/block decision on file properties managed by the device operating system rather than a hash or signature of the executable, reducing the manual management of whitelisting apps, and is based on a list of approved publishers and file owners, identifying all files from those sources as trusted*.
	Unauthorized software execution by blocking based on an authorized software list specific to each hardware device. At a minimum, resident executables must be blocked.	▪ Configure which products will be monitored, including software license compliance, and deny the usage of unauthorized software. ▪ License information such as number of licenses purchased, purchase price and date, location of license, license number, and reseller information can be entered for software products. ▪ Software monitoring agent continues to record data, storing it in the managed device’s registry if a managed server loses connection to the network and re-syncs at the next inventory scan. ▪ Easily establish compliance groups to match the breakdown of organizational business units. Generate detailed reports to assist in resource allocation, budgeting, productivity planning, training, and employee performance metrics.
* Because a trusted publisher could produce a compromised executable, the list of trusted publishers should be minimal and restricted to highly trustworthy organizations.		

Let us show you how Ivanti Asset Manager helps you automate and modernize while aligning with regulatory mandates. Contact us for a demonstration.

Learn More

ivanti.com
1 800 982 2130
sales@ivanti.com