solarwinds

BEST PRACTICES FOR IT ASSET DISCOVERY

The more you know the better you can manage—and secure

SOLARWINDS
FEDERAL WHITEPAPER

BEST PRACTICES FOR IT ASSET DISCOVERY

Asset discovery has been both a long-standing priority and a challenge for federal IT pros. As federal IT management has become more centralized, the consequences of not knowing what IT assets are on your network have increased. There are many stories about IT operations not having timely information about all of the devices on their networks and, in some cases, not knowing about entire network segments. Keeping track of the presence of dynamic IT assets on federal networks is a problem that is not going to go away.

IT asset discovery has also risen to become a far more critical aspect of managing and securing federal IT environments. Everyone knows that you can't secure a device on your network if you don't know that it exists. Asset discovery is essential to maintaining the appropriate level of IT security and compliance. Fortunately, technology has advanced to enable federal IT pros to more easily (and automatically) discover and track network assets. Automated IT asset discovery and notification helps IT pros keep up with the dynamic networks for which they are responsible.

Why is IT asset discovery a bigger concern now? The answer is multi-fold, ranging from new federal mandates to data-center consolidation to new security requirements.

Let's start with new federal mandates. According to the 2016 Fiscal Year guidance for Federal Information Security Modernization Act (FISMA) and a concurrent update to OMB's Circular A-130, federal agencies are now required to perform inventory and provide inventory reports. Agencies also must identify "high-value assets" within their environments that require special protection against outside threats.

The new rules also specify that federal Chief Information Officers (CIOs) identify which systems within their environments are oldest—specifically, which system rely on older infrastructure and which are due for modernization. Older systems can be more vulnerable and can be more costly to keep secure.

Now let's look at data center consolidation, which is a significant, ongoing effort within many agencies. The challenge, particularly for an organization the size of the Department of Defense, is the decades-long evolution of decentralized IT implementations that must now be brought together. Asset discovery is a critical piece of that, and has a broad impact on the long-term success of the Federal Data Center Consolidation Initiative (FDCCI).

Finally, but perhaps most important, is security. Simply put, you cannot secure an asset or a network segment that you don't know exists.

Federal IT pros have seen a dramatic increase in demand for asset discovery and network mapping efforts. As agencies are getting more centralized, and security becomes an even bigger priority, it has become even more important to have current and complete knowledge about every aspect of your network, in order to implement the most effective security. The more you know, the more secure you can be.

ASSET DISCOVERY ESSENTIALS

Given the need to know precisely what's within your environment, where do you start? To help answer that question, we've put together a description of the "must-have" aspects of asset discovery that combine to make up a best-practices approach.

1. Baseline Discovery

First, get a baseline understanding of your devices. You'll need a tool that will discover all of your IT assets—including routers, switches, servers and workstations. In fact, there is no need to stop there; get as much information as you can in order to enhance the effectiveness of your discovery.

Make sure the tool you choose can discover a vast amount of device information including server and workstation manufacturer and serial number, individual cards within each device, MAC addresses of network interfaces, power supply information, warranty and support information, machine temperature, fan status, peripheral devices, USB control numbers, processor information, etc. Make sure you're getting operating system and firmware information, as well.

This baseline discovery should include support for Windows server and workstations, Linux and Unix systems, ESX hosts and storage arrays.

Once you've got a baseline understanding of your assets, schedule regular automated discovery processes. The goal is to have ongoing, up-to-date information.

2. Connections

It's one thing to have all that device information; the next logical step is to understand how all these devices are connected to one another.

Your asset discovery tool should be able to create a network topology (layer 2 and layer 3) map—a visual representation showing all your assets. It should be able to show you where everything is geographically and topologically (relative to your network), and how everything is connected hierarchically. It should allow you to drill down to each device individually to see all the additional information that you've collected regarding each device.

3. Configurations

An equally important part of discovery is understanding the configuration of your IT assets, especially your network devices. First, make sure your tool discovers and tracks device configurations. In addition to the operational usefulness, tracking configuration information can also help you ensure your devices are meeting DISA STIG, NIST FISMA, or other compliance requirements. Compliance is critical. Your network asset tool should be able to create automated daily STIG, FISMA, or other compliance reports for your network devices and automatically generate a list of potential vulnerabilities from the current list of CVEs.

Your network device asset management tool should also be able to integrate with NIST's National Vulnerability Database, in order to keep up with the constantly evolving vulnerabilities in the CVE database. By automatically comparing CVEs with the current firmware and IOS versions of

your network devices, and then alerting you of any known CVEs that apply to your devices, your network asset management tool serves a much higher purpose than just backing up and rolling back your network device configurations.

4. Maintenance

The value in effective asset discovery goes well beyond simply having information. For example, now that you have serial numbers down to the card level per your baseline information, you can use that to track maintenance or capital replacement schedules. Devices for which you can no longer receive support may be a security risk—best to upgrade or update before you find yourself in this situation.

5. Software

So far, we have discussed discovery of system and network hardware, and network device configuration information. All this information is critical—but it's only part of what you really need.

Complete IT asset discovery means you have a record of all the software installed on each system. That includes everything from software-version information to individual drivers. Discovering installed software assets on Windows servers and workstations as well as various Linux and Unix systems and your ESX hosts should be part of your IT asset discovery tools.

Software asset discovery is useful for several purposes such as audits of license usage, identifying un-approved software, and finding out-of-date software versions installed on your systems. Poorly maintained software is a source of vulnerability and your agency's software needs to be regularly patched.

6. Usage

Devices do not sit idly within your environment. One of the key pieces of information you'll need for complete asset discovery is information about how the devices are being used—who, and what, is connected to your network. A good tool will let you discover IP MAC addresses connected to your switches and wireless access points, and which port they're connected to in your network.

With this information, you'll be able to see how your switches and ports are being used. Which switches are nearing capacity? Which ports are over used? Which switches and ports are being overloaded with traffic on a daily basis? This is all part of the IT asset equation.

A good tool will also let you see individual user logins, to the point where you can query your security log to tell you when each individual logged into your network, where they logged in, what device they used to log in, what IP/MAC address they used, and more.

7. Storage

While storage should be included as part of your baseline device information, the importance of including storage as part of your asset discovery process warrants its own discussion. The reason: storage devices are unique. To successfully track your storage devices as assets you'll need in-depth information (including serial numbers) for each array, each disk, which arrays and disks make up each cluster, etc.

As with network information, your ideal storage monitoring tool will provide visibility in the form of a map that will let you see storage hot-spots, those nearing capacity limits, as well as latencies that may lead to application slowdowns.

8. Remote

For federal IT pros in particular, asset discovery in remote locations may be a challenge owing to the multitude of disparate sites, remote-location firewalls, limited port access, and more. A best-practices way to include these remote devices in your asset discovery is through remote polling engines. This is a device that sits within the remote location—inside the firewall—and collects asset information, monitors assets, and sends information back to the main monitoring server—through one port—for integration into the rest of your asset discovery information.

Another advantage this has for federal IT pros is the advantage this provides for very large environments; this approach provides the scalability many other methods of asset discovery do not allow.

DISCOVER TO MANAGE—WHAT TO DO WITH THE INFORMATION YOU'VE DISCOVERED

As we discussed at the start of this paper, asset discovery is a high priority for federal IT pros, and getting higher each day. The information collected will help more effectively meet new federal mandates, data-center consolidation efforts, and increasingly strict compliance and security requirements.

Highly effective asset discovery will also allow for dramatically enhanced asset management. The information you collect can be used by the IT operations team, the IT security team, and across the organization to enhance application management, network management, and much more.

In fact, the best way to ensure the information you collect is used most effectively is to store everything within a central repository that automatically synchronizes every time new information is added. This enhances accuracy across the entire organization (every team is using the same information) and provides a way to track and report on changes. This approach also allows you to plan more effectively as you can perform capacity planning and forecasting based on warranty information, end-of-life tracking, and more.

SOLARWINDS PRODUCTS FOR ALL YOUR IT ASSET DISCOVERY NEEDS

From baseline discovery through remote polling, SolarWinds has the tools to help you implement the most effective asset discovery solution and provide your agency with in-depth information to make the most informed management—and security—decisions.

» Network Performance Monitor (NPM)—Discovers network devices and computers, from manufacturer to serial number to operating system version; discovers MAC and IP addresses; discovers device health; discovers network topology information; and much more.

» Network Configuration Manager (NCM)—Automatically backs-up configurations of switches, routers, and firewalls; keeps an inventory of device-component serial numbers; automatically compares configurations to DISA STIG or NIST FISMA configuration requirements; provides vulnerability tracking against the latest CVEs; provides network health assessment reports; and much more.

» Server & Application Monitor (SAM)—Discovers servers, workstations, virtual hosts, installed software, and much more.

» User Device Tracker (UDT)—Monitors connected devices; discovers and stores MAC addresses that are connected to your switches or wireless access points; maintains device connection and user logon histories, which can be useful for forensics, and more.

» Storage Resource Monitor (SRM)—Discovers and monitors storage arrays; discovers disk-drive serial numbers inside NAS and SAN devices; provides real-time, agentless NAS and SAN performance and capacity monitoring; and much more.

» Additional Polling Engine—Allows discovery and monitoring to take place from a Windows server installed in a remote location to support automated IT asset discovery in the largest enterprises.

ADDITIONAL RESOURCES

» Webinar—Best Practices for IT Asset Discovery: Improving Visibility for IT Operations and Information Security

ABOUT SOLARWINDS

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide from Fortune 500 enterprises to governments including nearly every U.S. civilian agency, DoD branch, and intelligence agency, National Health Service, European Parliament, and NATO Support Agency. In all market areas, the SolarWinds approach is consistent—focusing exclusively on IT Pros and striving to eliminate the complexity that they have been forced to accept from traditional enterprise software vendors. SolarWinds delivers on this commitment with unexpected simplicity through products that are easy to find, buy, use and maintain while providing the power to address any IT management problem on any scale. Each solution is rooted in the company's deep connection to their user base, which interacts in an online community, thwack®, to solve problems, share technology and best practices, and directly participate in the product development process.

SolarWinds provides IT management and monitoring solutions to numerous common public sector IT challenges including continuous monitoring, cybersecurity, network operations, compliance, IT consolidation, data center operations, cloud computing, mobile workforce and devices, DevOps, and scaling to the enterprise. SolarWinds software is available through numerous channel partners and systems integrators worldwide as well as the U.S. General Services Administration (GSA®) Schedule, Department of Defense ESI, United Nations Global Marketplace (UNGM), Crown Commercial Service (CCS), United Nations Atlas. For more information and fully functional free trials visit: http://solarwinds.com/federal or http://solarwinds.com/nationalgovernment.

federalsales@solarwinds.com
solarwinds.com/federal
877-946-3751

nationalgovtsales@solarwinds.com
solarwinds.com/nationalgovernment
+353 21 2330440