

The CDM Learning Community Event (LCE)

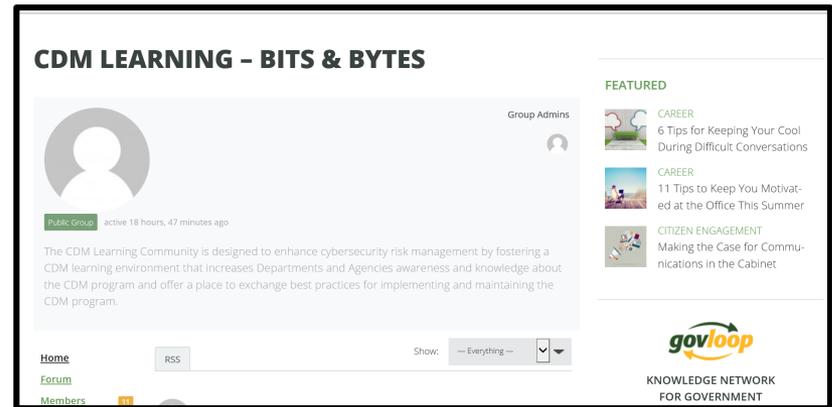
We will begin at 11:00AM EST

Welcome to the CDM LCE – Automating Software Asset Management: Notes From the Field

While you wait, check out:



Our CDM Homepage



Our CDM Bits and Bytes Blog

Have a topic suggestion for a future webinar or LCE? Please send it to cdmlearning@hq.dhs.gov



U.S. DEPARTMENT OF
**Homeland
Security**

Federal Network Resilience



Homeland Security

Automating Software Asset Management: Notes from the Field

June 30, 2016

11:00 am – 1:00 pm

A CDM Learning Community Event



CDM Learning Community - Roadmap



	Apr-16	May-16	Jun-16	Jul-16	Sep-16
Webinar	CDM Readiness: Cover your Assets	Moving Forward: Automating Hardware Asset Management	Moving Forward: Automating Software Asset Management	Moving Forward: Automating Configuration Settings Management	Moving Forward: Automating Vulnerability Management
LCE	Federal Network Resilience: Impacting Cybersecurity through Agency Engagement	Automating Hardware Asset Management: Notes from the Field	Automating Software Asset Management: Notes from the Field	Automating Configuration Settings Management: Notes from the Field	Automating Vulnerability Management: Notes from the Field

<https://www.us-cert.gov/cdm/training>



Event Goal

The goal is to discuss the automation of software asset management, including sharing best practices and lessons learned through experiences from the field.



Software Asset Management

- Preparing for SWAM Automation
- Whitelisting and Blacklisting
- SWID Tags
- Unauthorized vs Unmanaged Software
- Best Practices



Ask questions!



Share experiences!



Discuss challenges and solutions!



Today's Agenda

- Welcome and opening remarks
- Panel introductions and presentations
- Breakout room discussions
 - Challenges, best practices, lessons learned
- Closing remarks



Today's Speakers

- Dan Frantz, SSA
- Peter Crichlow, DOJ
- Greg Witte, G2 Inc
- Stacy Leidwinger, RES Software
- Mike Wilson, Splunk



Technical Advisor for the Social Security Administration

- CDM Program Manager overseeing the implementation of DHS CMaaS program
- Dashboard, automation of CDM data, and FISMA reporting experience
- Worked in variety of IT and Information Security roles across the private sector, education and the public sector



Software Asset Management at the Social Security Administration

1

**Office of Information Security
(OIS)**

June 17, 2016



Agenda

2

- Welcome / Bio
- The End Game
- The Journey
- Challenges and lessons learned



Who we Are, Who I am

3

The SSA:

- Old-Age, Survivors, and Disability Insurance (OASDI) (“Social Security”)
- Supplemental Security Income (SSI)
- Monthly OASDI benefits paid to **59M** individuals, including retirees, spouses and children, workers with disabilities, dependents of the deceased and SSI benefits to 8M+ recipients
- HQ in Woodlawn, MD with over 1200 field offices serving 40M+ visitors nationwide

The IT:

- **300,000+** IP-addressable assets across **400,000+** IP addresses
- **165,000** Windows endpoints (workstation and server)
- Highly centralized and homogenized
- Remaining assets are in support of networking, storage, VoIP, Printers, and MFDs

Me:

Technical Advisor for the Office of Information Systems and CDM Program Manager



The End Game

(...because goals are important)

4

- Move from Blacklisting to Whitelisting
- Streamlined Process to Expand Whitelist
- Interact with License Management and Software Distribution
- Strengthen our overall ISCM capability



Where We Started

5

- Highly centralized, homogenous endpoint environment with standardized platforms
- Long-standing installation of Microsoft System Security Center, which is integral to our change management and centralized software deployment
- SCCM is accessible to Splunk (via DBX)
- ...Thought -- “Everything was in the standard image!” (we were wrong)



Software Authorization / Exceptions

6

- Began to Baseline software in 2012
- We wanted to have an “Authorization” process for software
- Non-Enterprise Supported software would need an “Exception”
- Exceptions would be regularly reviewed and could be revoked for non-compliance (ex. failure to patch)
- Leverage Splunk for automated reporting, alerts, correlation, triggers, etc.



Unauthorized vs Unmanaged

7

- It quickly became clear that was a difference between “Unauthorized” and “Un-managed”
- Discovered instances of installed software which had a legitimate business use but not centrally managed, or widely used free tools that only certain privileged people should have.
- Examples:
 - Procured software locally approved and managed with legitimate business use
 - Games, Exam prep, VM and emulation software
 - Admin tools like PuTTY, WinSCP, Wireshark, FileZilla
 - 3rd party browsers
- Not all users are created equal. Exceptions for one may not be valid for another.



Lessons Learned

8

- Business process will drive a technical solution
- An onerous, tedious process will prevent adoption
- Software Asset Management isn't just a security concern. Other impacts are licensing, procurement, centralized supportability, change management, in-house development
- Take a risk-based approach; focus on privileged users, high value assets, users with VPN access, etc
- Integrate with Splunk, but not everything needs indexing



Engineering Lead for the ISCM Program and the DOJ CDM Program Manager

- Provides authoritative guidance related to DOJ IT security program
- IA Lead ensuring the integration of IT security programs and services
- Designs, develops, and manages security into systems based on mission risk





DOJ Cybersecurity Software Asset Management

OCIO, Cyber Security Staff

6/30/2016



Enterprise Software Asset Visibility

- Implemented an enterprise endpoint management system based on an agent based technology
 - Desktops, laptops, servers
 - Developed MSI to customize agent install with unique file per administrative domain
 - Used as an identifier for Asset inventory
 - Logon GPO used for client install to capture new managed systems



Software Asset Discovery

- Currently decentralized
 - Supported using approved software list at the enclave/Component
- Enterprise view focused on high risk unsupported software
- Develop centralized asset management approach
 - Discovery for software, processes, and file systems
 - Correlate CPE information
 - Focus on the highest risk software first
 - Volume of data expected to be great
 - Automate software list appendix for SA&A effort



Hosted System Model

- Owner:
 - The GSS, System, Site, or Accreditation Boundary that is responsible for the maintenance and management of the hardware asset
- Consumer:
 - The GSS, System, Site, or Accreditation Boundary that makes use of the hardware asset
- One to many relationship
- An asset can have one owner but multiple consumers

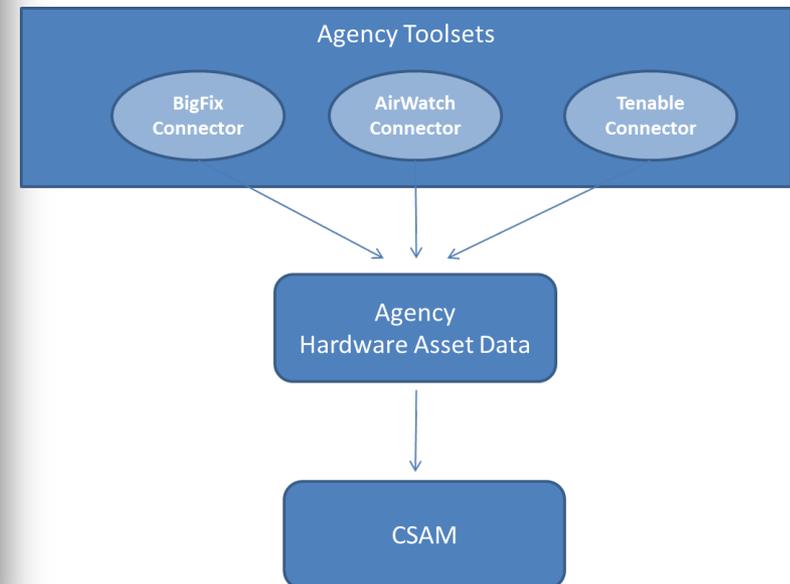


Asset Management

- Developed a way to automate a manual process incorporating sensor data
 - “Tag” authorized assets to system boundaries in our SA&A tool and have the functionality align with the security professionals.

The screenshot shows the 'Asset Management' interface. The 'Filter By' section includes fields for Hostname (HW-6*), Hardware Asset Type (-All-), Operating System (-All-), Operating System Type (-All-), IP Address with Wildcard, MAC Address with Wildcard, Active Directory Path, BigFix Group (DEA), and Ownership (-All-). A 'Message from webpage' dialog box is displayed, stating: 'This rule will tag all HW assets that meet the search criteria to this system. Click OK to continue.' The 'Existing Rules' section shows a rule named 'HW-6* for DEA Big Fix Group' with 'Save' and 'Cancel' buttons. Below is a table of existing rules:

Zone	Org	Hostname	Hardware Type	OS	cpu	Active Directory Path	MAC Address	IP Address	Has an Owner	
<input type="checkbox"/>	BIGFIX_DOJ	CDO	HW-60	Desktop	Win7 6.1.7601	3100 MHz Core i5-2400	cn=HW-60,ou=CDO,ou=doj,ou=gov	35-39-32-34-71-49	1.1.100.212	False
<input type="checkbox"/>	BIGFIX_DOJ	CDO	HW-62	Desktop	Win7 6.1.7601	3000 MHz Core 2 Duo	cn=HW-62,ou=CDO,ou=doj,ou=gov	00-04-f3-0f-93-09	1.1.100.34	False
<input type="checkbox"/>	BIGFIX_DOJ	CDO	HW-61	Desktop	Win7 6.1.7601	3100 MHz Core i5-2400	cn=HW-61,ou=CDO,ou=doj,ou=gov	37-39-32-3a-30-29	1.1.100.220	False
<input type="checkbox"/>	BIGFIX_DOJ	CDO	HW-64	Desktop	Win7 6.1.7601	3100 MHz Core i5-2400	cn=HW-64,ou=CDO,ou=doj,ou=gov	04-03-4f-10-10-14	1.1.100.135	False





Provide Security “Scoring” against assets

- DOJ Risk Score of 20
- Each instance of unsupported software installed on asset contributes 20 points of risk

Department of Justice
Unsupported Software Dashboard
LIMITED OFFICIAL USE

Department of Justice	Department of Justice		10,915 assets	
Monday, June 27, 2016				
Table of Contents				
Organization	Number of Assets			
	10,915			
	4			
	77			
	2			
	2			
	6			
	6			
	6			
	6			
	6			
	6			
	10,837			
	5			
	2			
	3,806			
	10,836			
	9,266			
	6,029			
	1,664			
	833			
	833			
	108			
	1,556			

Unsupported Software Summary				
Software Unsupported Risk Score	Number of Unsupported SW Titles	Number of End Of Life SW Titles	Number of Software Titles	Number of Assets with Unsupported Software
0.2	38	2	151	7,108

Unsupported Software Summary									
		Software Status							
Software Category	Software Type	Unsupported		EndOfLife		Supported		Total	
		Number of Software Titles	Number of Assets	Number of Software Titles	Number of Assets	Number of Software Titles	Number of Assets	Number of Software Titles	Number of Assets
Adobe	Adobe Acrobat					8	3,825	8	3,825
Acrobat	Adobe Reader					20	2,894	20	2,894
Adobe Flash	Adobe Flash					4	143	4	143
Java	Java JDK	12	20			11	22	23	36
	Java JRE	10	41			30	6,610	40	6,642
Other	Other	16	27	2	56	38	7,052	56	7,108

All Unsupported and End-of-Life Software Assets	
Software Status	Software Item
Unsupported	Java 7 Update 80
	Java(TM) 6 Update 95 (64-bit)
	SQL Server 2008 SP1
	Java(TM) 6 Update 95
	Java 7 Update 80 (64-bit)
	Java 7 Update 75
	Java SE Development Kit 7 Update 80 (64-bit)

Software Item	Number of Assets
Java 7 Update 80	15
Java(TM) 6 Update 95 (64-bit)	9
SQL Server 2008 SP1	9
Java(TM) 6 Update 95	8
Java 7 Update 80 (64-bit)	6
Java 7 Update 75	5
Java SE Development Kit 7 Update 80 (64-bit)	5

Software Status

- Unsupported
- EndOfLife



DOJ Scoring Objectives

- Provide a single cybersecurity risk assessment for the Enterprise
- Measure risk across multiple areas
- Motivate IT administrators to reduce risk
- Motivate management to support risk reduction
- Measure improvement/performance
- Provide visibility of risk
- Provide risk assessments for each host
- Provide risk assessments for each Component and FISMA system
- Be demonstrably fair
- Be scalable to future data



Governance

- Governing Body - DOJ IT Security Continuous Monitoring Working Group
 - All changes are brought before this group for input and concurrence
 - Members include all DOJ Components that have a Component level CIO
 - Chaired by Deputy CISO
- Communication to system administrators and operation personnel is critical
- Approved Changes take 3-6 months to implement into reporting tools.

G2 Inc. Senior Security Engineer

- Supports federal and commercial clients, primarily the NIST Computer Security Div
- 30+ yrs in IT with 20 yrs of that in security
- One of several primary authors of the NIST Cybersecurity Framework
- Co-authored the McGraw Hill S-CAP textbook
- Built software and hardware asset management for the State Department



Software Asset Management Automation through the use of Software Identification (SWID) Tags



Greg Witte, greg.witte@g2-inc.com

Software Inventory Management

- A key component of Software Asset Management (SAM)
- Includes confirmation and monitoring that software is installed in accordance with organizational requirements
 - Change management
 - Licensing requirements
 - Patching regimens
 - Removal processes
- Software Inventory is a critical component of effective cybersecurity risk management

Software Identification (SWID) Tags

- Software inventory depends upon consistent and accurate identification and management of software products
- NIST has been working with the security and SAM communities to conduct and publish research regarding the use of software identification (SWID) tags for that purpose
- Working with the international standards development orgs to enhance the SWID tag standards and to promote their use in software and security management protocols.
- Great work by David Waltermire (NIST), Brant Cheikes (MITRE), and Larry Feldman (G2)

ISO Standard 19770-2:2015

- International Organization for Standardization / International Electrotechnical Commission (ISO/IEC) Standard 19770-2, Software Asset Management – Part 2: Software Identification (SWID) Tags
- Specifies the use of SWID tags for a broad range of SAM use cases
- NIST worked with the SAM and security community to produce an updated version of the ISO/IEC standard, released in 2015.



What's a SWID Tag?

```
<SoftwareIdentity
  name="ACME Roadrunner Detector 2013 Coyote Edition"
  tagId="com.acme.rrd2013-ce-sp1-v4-1-5-0" version="4.1.5">
  <Entity name="The ACME Corporation"
    regid="acme.com" role="tagCreator softwareCreator"/>
  <Entity name="Coyote Services, Inc."
    regid="mycoyote.com" role="distributor"/>
  <Link rel="license" href="www.gnu.org/licenses/gpl.txt/">
  <Meta activationStatus="trial" product="Roadrunner Detector"
    colloquialVersion="2013" edition="coyote"/>
  <Payload>
    <Directory root="%programdata%" location="rrdetector">
      <File name="rrdetector.exe" size="532712"
        SHA256:hash="a314fc2dc663ae7a6b6bc...57396e6b3f569cd50fd5ddb4d1bbafd2b6a"/>
    </Directory>
  </Payload>
</SoftwareIdentity>
```

NIST Internal Report 8060

Guidelines for the Creation of Interoperable SWID Tags

- Complements 2015 SAM/Continuous Monitoring Building Block
- Introduces SWID tags in an operational context to a broader audience
- Provides specific tag implementation guidelines that supplement the SWID tag standard
- Provides a set of operational usage scenarios that illustrate how SWID tags can be used to achieve a variety of cybersecurity goals

Available from: <http://dx.doi.org/10.6028/NIST.IR.8060>

SWID Tags and the Software Lifecycle

- **Primary, patch, and corpus** tags have similar functions - describe information about software in several different stages of the lifecycle
 - **Primary** – identifies/describes info about SW products installed
 - **Patch** – identifies/describes each patch installed. Can be placed on the device when patch installed, or discovery tools can create a patch tag to indicate previous patch application
 - **Corpus** – identifies/describes products in pre-installation state (e.g., installation package, distribution media CD). Corpus tags support integrity verification of software to be installed
- **Supplemental** tags furnish additional information
 - Provides flexible/extensible means to augment information provided in other tags
 - Assists with overall software management
 - Supports related processes (e.g., configuration management, vulnerability management)

SWID Tags and the Software Lifecycle (cont'd)

- **Pre-Installation** - Before a software product is installed, a *corpus* tag provides hash values that help verify file integrity
- **Installation** - *Primary* tag installed w/ SW product (or created later) uniquely identifies/describes it. *Supplemental* tags augment those with additional site-specific or extended information. *Patch* tags provide information about software fixes deployed along with the base software installation.
- **Patching** - When a new patch is applied to the software product, a new patch tag is installed, supplying details about the patch and its dependencies.
- **Upgrading** - As a software product is upgraded to a new version, new primary and supplemental tags replace existing tags for the older software version, enabling timely and accurate tracking of updates to software inventory.
- **Removal** - Upon removal of the software product, inventory will be updated to reflect that information.



SWID Tags as Part of Managing Cybersecurity

- Use of SWID tags supports a broad array of cybersecurity use cases
- In the CDM context, especially in the use of automated software discovery or monitoring tools:
 - Tags created by vendors and in conformance to an international standard = highly interoperable and reliable
 - Historically, discovery tools had to rely upon proprietary methods
 - Tools have had varying levels of success reliably understanding inventory, authorization status
 - SWID tags help consistently recognize installed software, supporting continuous monitoring of software inventory changes.
- SWID tags also help orgs track the software lifecycle for custom-built and/or in-house developed software

SWID Tag Usage Scenarios in NISTIR 8060

- Minimizing Exposure to Publicly Disclosed Software Vulnerabilities
 - Continuously monitoring software inventory
 - Ensuring that software products are properly patched
 - Identifying vulnerable endpoints through correlation to databases (e.g., NVD) and vulnerability advisories issued by vendors and independent security analysts (e.g., CIRT) with the inventory information collected by discovery tools
- Enforcing Organizational Software Policies re: Authorized Software
 - Supports blacklists/whitelists
 - Specific products and/or versions may be designated as mandatory
- Preventing Vulnerable Devices from Accessing Network Resources
 - Forward-looking approach to improving cybersecurity by preventing potentially vulnerable endpoints from connecting to the network, or to move endpoints to an isolated network segment for remediation or investigation.

SWID Tags' Role in Security Automation

- SWID tags help to provide consistent and accurate software inventory information
- Use of SWID tags as installation evidence is described in the next minor version of the Security Content Automation Protocol (SCAP), SCAP 1.3, (currently in development)
- SWID tags are also part of the ongoing work in the Security Automation and Continuous Monitoring (SACM) working group of the Internet Engineering Task Force (IETF)
 - SACM Information available from: <https://datatracker.ietf.org/wg/sacm/charter>
 - SACM mailing list: <https://www.ietf.org/mailman/listinfo/sacm>
 - The international standards being developed in the IETF SACM working group are expected to be the basis for the next major version of SCAP, SCAP 2.0.

Putting this into context

As exciting as the implementation of a new XML-based automation standard is, in and of itself, let's see how the use of SWID tags might support your organizations and your application of CDM

What can orgs do to prepare for transition from traditional manual/proprietary SAM to an integrated and automated approach?

- Some of the work for this needs to be done by software product vendors and software discovery tool vendors
- Begin to stay aware of the use of SWID
- Read the building block and NISTIR to get familiar with SWID concepts
- Stay tuned to the community's ongoing work and include this automation in your plans for achieving SAM

How can organizations balance good software authorization practices with the need to execute important system/maintenance/update processes?

- The use cases describe how to use SWID tags to ensure that only authorized software is installed and executed
- Digital signature methods are still being developed, but we anticipate the ability to only execute properly authorized and signed software
- We can ensure that required processes are actually executed
- We can detect that a software product might be tampered with or may be unauthorized, and use methods to prevent execution

What should organizations do if they encounter software that does not have an associated SWID tag or Common Platform Enumeration?

- As your orgs adopt the use of SWID, work with your vendors to encourage them to include SWID tags with products and patches
- Work with discovery tool vendors to support their integration of SWID so that they can create what are called “non-authoritative” tags
- Consider use of SWID tags for in-house developed software
- NIST is developing a new NISTIR that will describe how to create CPEs from SWID tags

How Does a SWID Tag Compare with a CPE?

- CPE is widely used to reference software items
- Currently uses a unique, compact and human-readable URI
- Matching algorithm is uncomplicated and doesn't require access to a central dictionary
- Seven components capture much of what's needed to distinguish among products: Part, Vendor, Product, Version, Update, Edition, Language

```
cpe:/o:microsoft:windows_xp::sp1:professional
```

Where is the SWID tag repository ideally located for agencies? What actions will they need to take to ensure the SWID tag data is directed to the repository?

- This is more of an implementation question and less about the technology
- Several “dictionaries” are centrally located now (e.g., CPE, CVE) with some benefits and some challenges
- SWID supports organizational and federated repositories with some pros and cons

What is the importance of using the Trusted Computing Group's Trusted Network Connect architecture for secure communication to the policy server?

- My answer would be less specific to the TNC-specific architecture, although that is a reliable and demonstrable example
- Many network connection decisions are based upon security posture, including inventory information
 - Whitelisting – do I have updated and mandatory software (e.g., AV definition)?
 - Blacklisting – is software installed that is known to be prohibited?
 - Can I place the device into a quarantine until known to be “compliant”?

How can SWID tags help to enforce an authorized software list (whitelist)?

- SWID Tags help accurately identify what is installed, perhaps using a digital signature to confirm an executable's integrity and provenance
- Not bulletproof, but getting better. During development of the IR, NIST taught me that, due to the use of 64-bit word values in the algorithm, SHA-512 hash function implementations may perform better than SHA-256 implementations on 64-bit systems
- It all depends upon a reliable execution process, but where that exists, it can refuse to execute any program not on the whitelist, and the tags can help enforce that

The building block does not address how to deal with cloud-based applications or virtualization software.

- Do you have any recommendations on how to handle those types of apps/software that are ephemeral instances?
- That's a tough one – the rise of virtualization and cloud change the very definition of what it means to be a computing device
- There is a critical need to manage this ephemeral inventory, but it brings a large number of challenges
- Not really a technical issue, but I'm looking forward to seeing how the community tackles this myself

What actions are recommended for endpoints that are found to have a non-compliant software inventory?

- Recommended actions are beyond the scope of this discussion, but I think the action is relatively straightforward
- In the past, such as at State, the bigger challenge was identifying instances of installation of software that didn't conform to Dept. policy, and then providing solid evidence
- As we've seen, the use of SWID Tags to discover and track the installation and updates to various software products support a broad array of cybersecurity use cases, including this one.

Follow up?

My contact info:

Greg Witte

greg.witte@g2-inc.com

301-346-2385

VP of Products at RES

- Responsible for product/customer success in the areas of end user computing and security
- Led product mgmt team at Directworks, a sourcing/supplier management solution
- Managed roadmap, product positioning, and go-to-market strategy at Vivisimo, an enterprise search solution
- Responsible for Vivisimo/IBM product integration after IBM acquired Vivisimo





Automating Software Asset Management: Notes from the Field

Presented by: Stacy Leidwinger, VP of Products at RES

@stacyleidwinger



Why is Automating Software Asset Management Critical?

- Many often buy into software asset management as a cost control measure. But a significant driver should also be security:
 - User access authorization
 - Trustworthiness of software
 - Safe configuration of software
 - Patch management



3 Steps To Drive Secure & Automated Software Asset Management

#1 Define your Whitelist

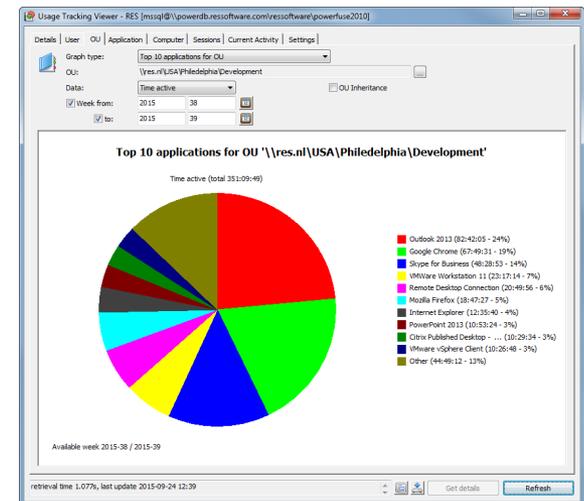


Create a Baseline of What is Good vs. Bad

Track usage across physical & virtual environments which can assist in software asset & license management projects.

Look to Identify

- Top used software applications
- Least used software applications
- Unauthorized software applications
- Unauthorized executables
- Unmanaged settings/patches



Why Hasn't Whitelisting Worked in the Past?

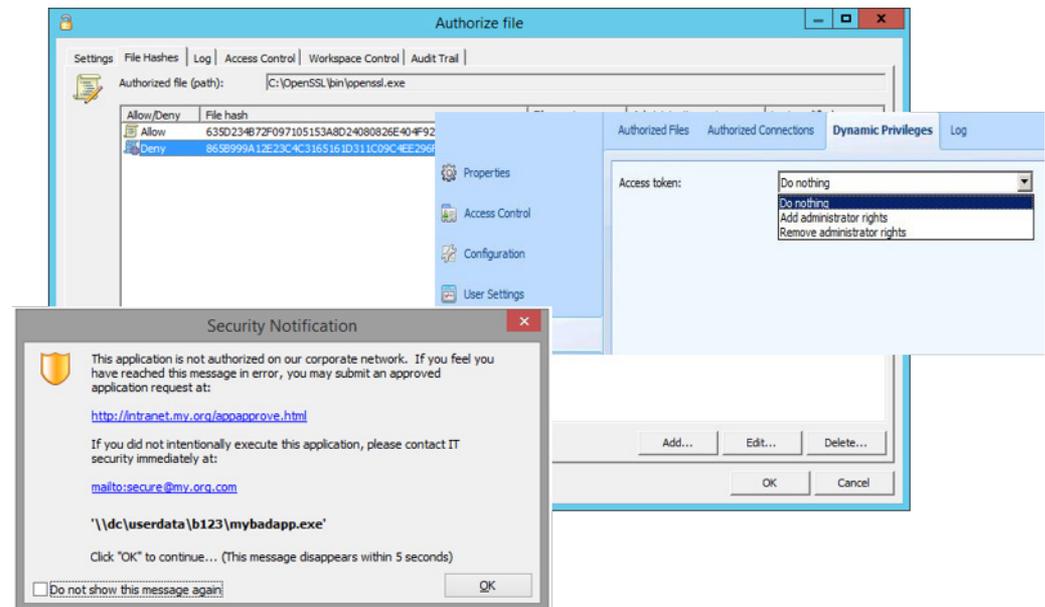
- It is difficult to manage
- It places end users at the mercy of waiting for approval from admins for every task
- Prevents developers from doing their jobs
- Issues working with Antivirus and performance overhead



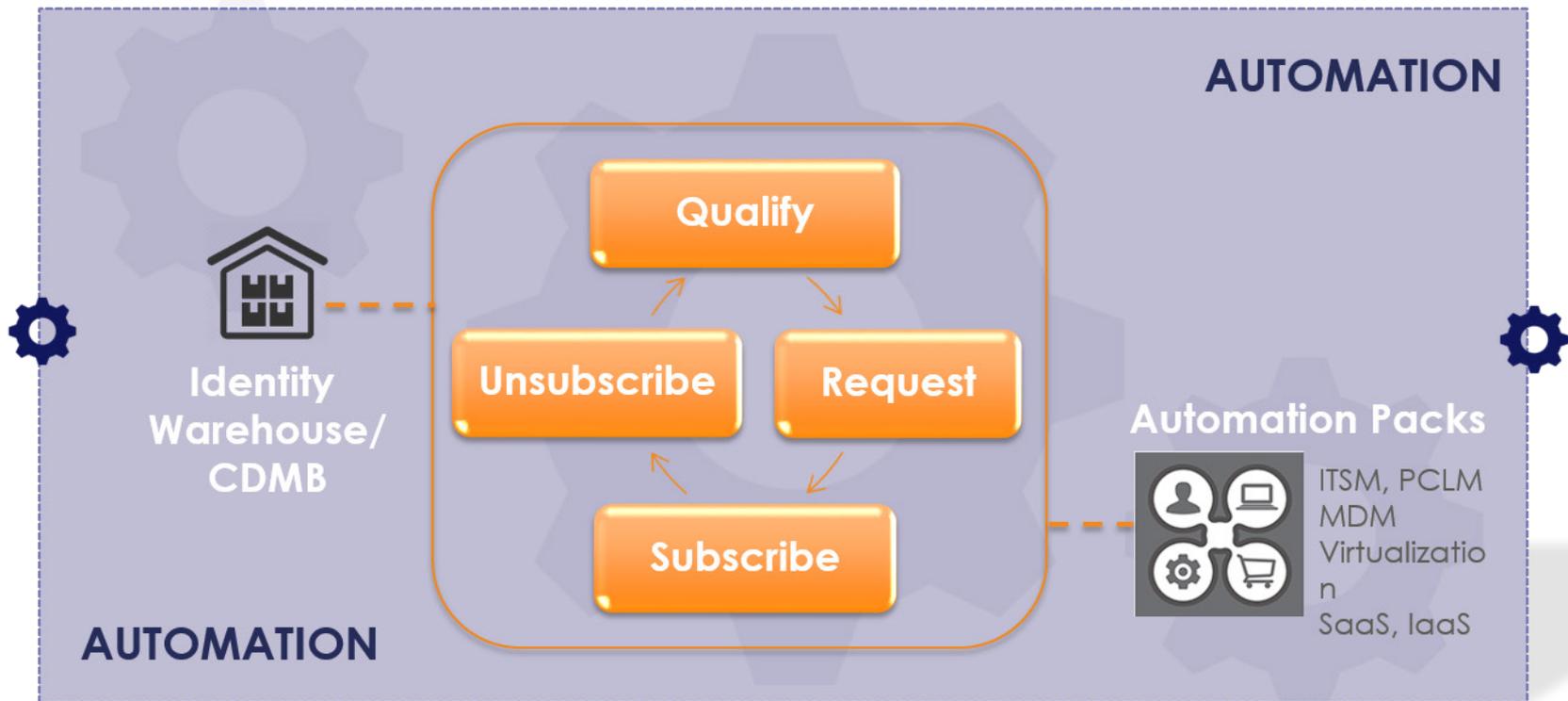
Solution: One Pass, Context Aware Whitelisting

Offer application based security that is:

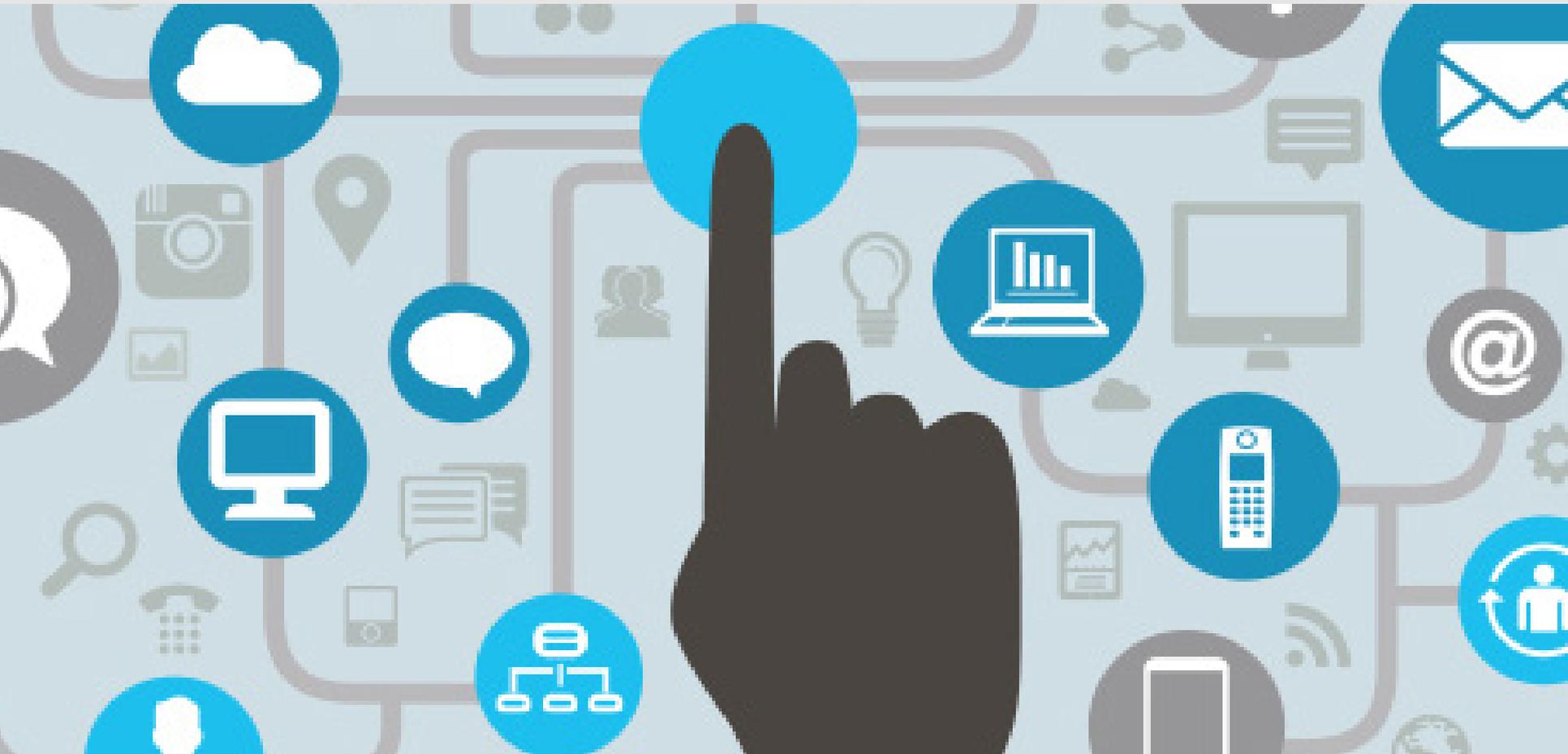
- Contextually aware
- Easily scalable & integrated
- Quick to deploy



Automate Software Application Delivery Based on Policy & Workflow

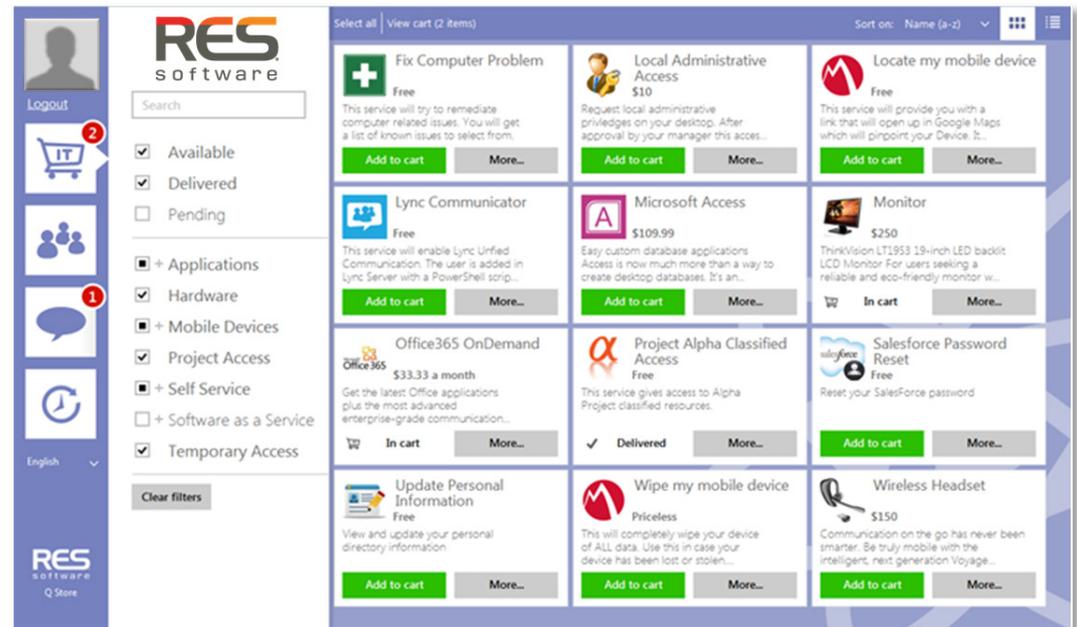


#3 Promote Self-Service & Workflow

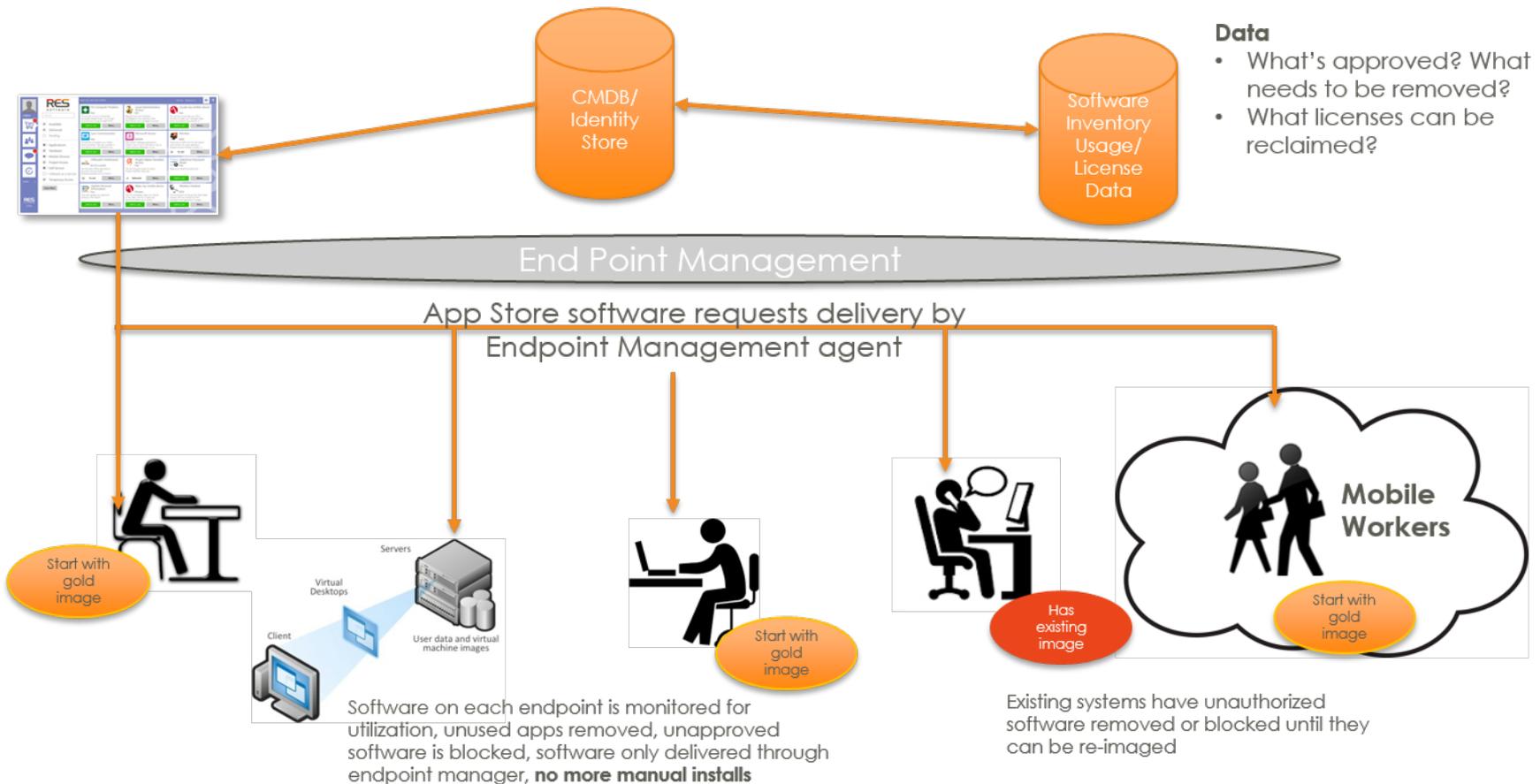


Intuitive Self Service

- View active and available services offered through an app store
- Services should be both IT and non-IT related
- Apps & services should be delivered through automated workflows



Final Result: Secure & Automated Software Asset Management



Thank You!

s.leidwinger@ressoftware.com



Principal Sales Engineer for the Public Sector Team

- Developed FISMA monitoring solutions, Cyberscope applications, and other security and compliance apps
- US Army
- Contractor for US CBP working in Unix administration, Identity Management, and Desktop Management
- Sales Engineer at BigFix



splunk

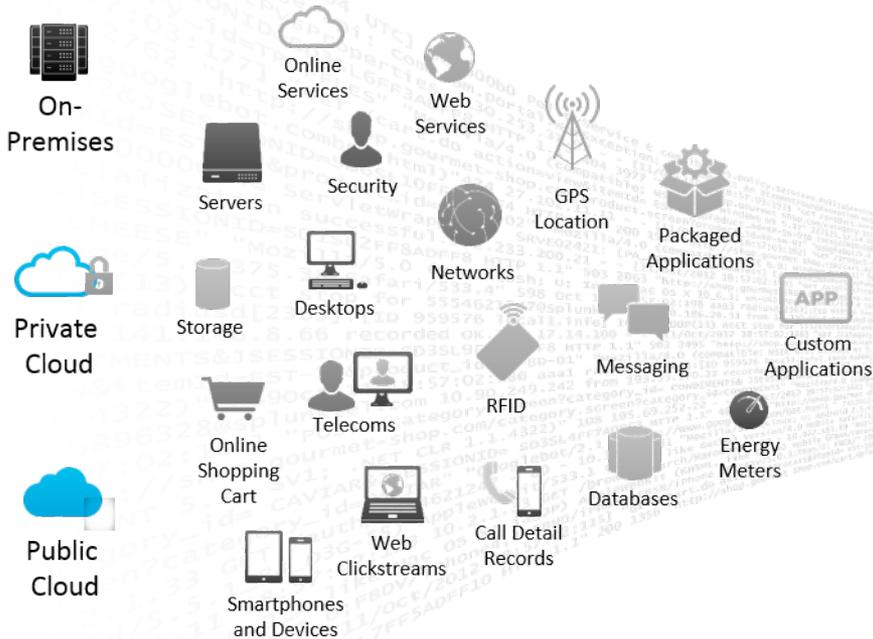
Make machine data accessible, usable
and valuable to everyone.

What is Splunk?

```
01:45:62 - - [02/Feb/2011:16:00:23] GET /product.screen?product_id=FW-4020.JSESSID=504557&category_id=FLOWERS Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322.5002) http://www.myflowershop.com/category.screen?category_id=FLOWERS
01:45:62 - - [02/Feb/2011:16:00:24] POST /category.screen?category_id=TEDDY&JSESSIONID=5D9SL4FF4ADFF8 HTTP 1.1*200 3439 Windows NT 5.1; SV1; .NET CLR 1.1.4322.5002 http://www.myflowershop.com/category.screen?category_id=TEDDY&JSESSIONID=5D9SL4FF4ADFF8
01:45:62 - - [02/Feb/2011:16:00:24] GET /category.screen?category_id=TEDDY&JSESSIONID=5D9SL4FF4ADFF8 HTTP 1.1*200 3439 Windows NT 5.1; SV1; .NET CLR 1.1.4322.5002 http://www.myflowershop.com/category.screen?category_id=TEDDY&JSESSIONID=5D9SL4FF4ADFF8
```

Industry Leading Platform For Machine Data

Machine Data: Any Location, Type, Volume



Answer Any Question

-  Ad hoc search
-  Monitor and alert
-  Report and analyze
-  Custom dashboards
-  Developer Platform

splunk > enterprise

splunk > cloud™

Platform Support (Apps / API / SDKs)

Enterprise Scalability

Universal Indexing

What is the Continuous Diagnostics and Mitigation Program?

- **Dynamic** implementation approach to fortifying the cybersecurity of computer networks and systems.
- Provides capabilities and tools that enable network administrators to know the **state of** their respective **networks** at any given time
- Helps **protect** government IT networks **from cybersecurity threats** and enhances **risk-based decision-making**.
- Helps enhance the Federal government's ability to identify and **respond, in real-time** or near real-time, to the risk of emerging cyber threats.
- Creates an implementation of NIST 800-53 (security) 800-37 (risk) and 800-137 (continuous monitoring) Called Information Security Continuous Monitoring (ISCM) by OMB

Why CDM? (Cont.)

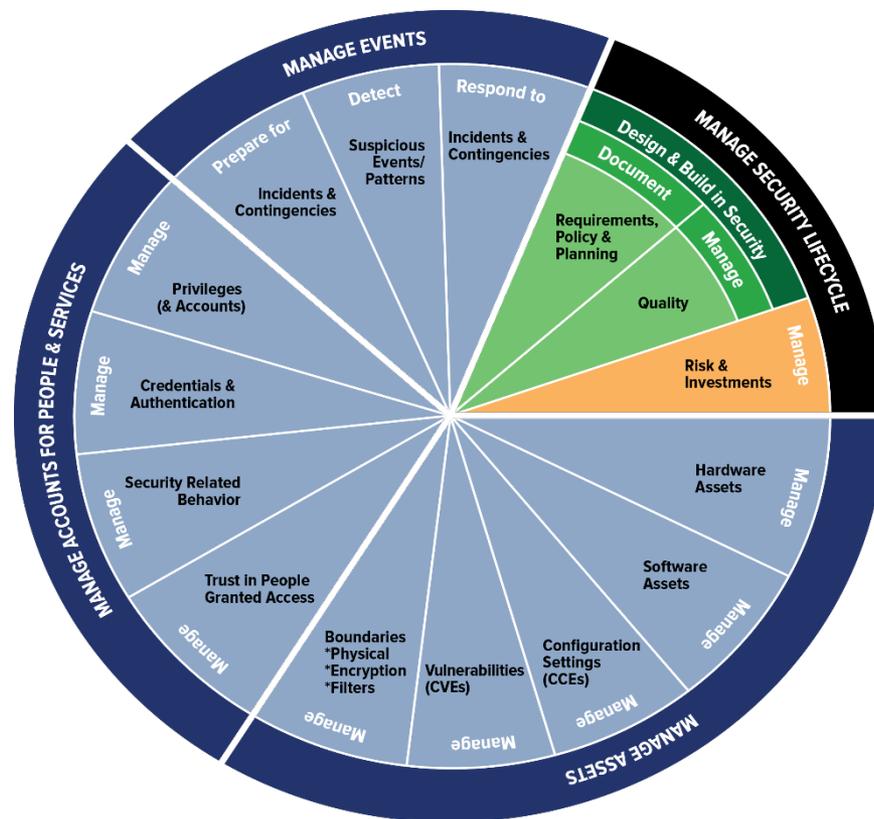
According to the CSIS report:

- 75% of the attacks use known vulnerabilities that could be patched;
- More than 90% of successful attacks require only the most basic techniques; and,
- **96%** of successful breaches **can be avoided** if the victim puts in place simple or intermediate controls.

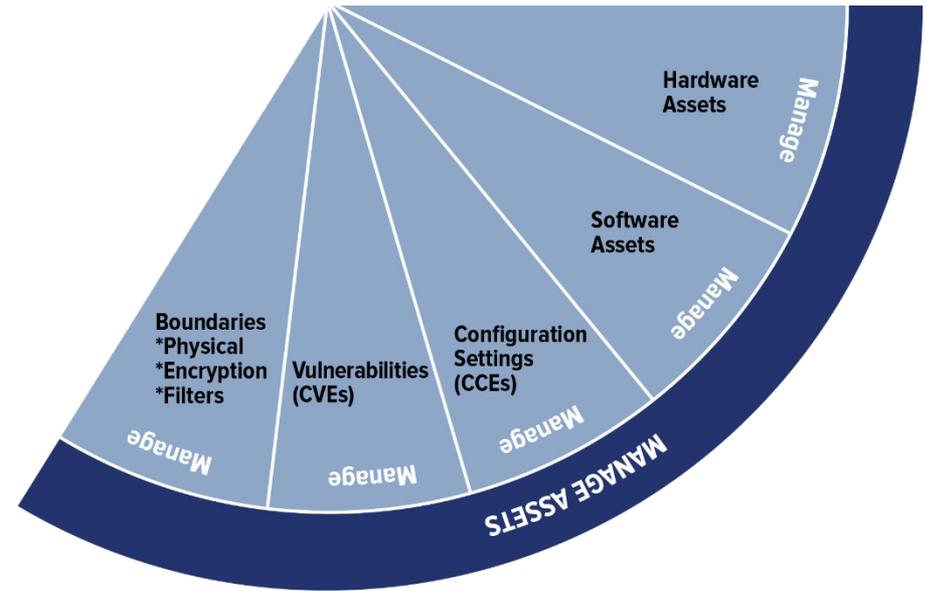
CDM Implementation Phases

3 + 1 Implementation Phases

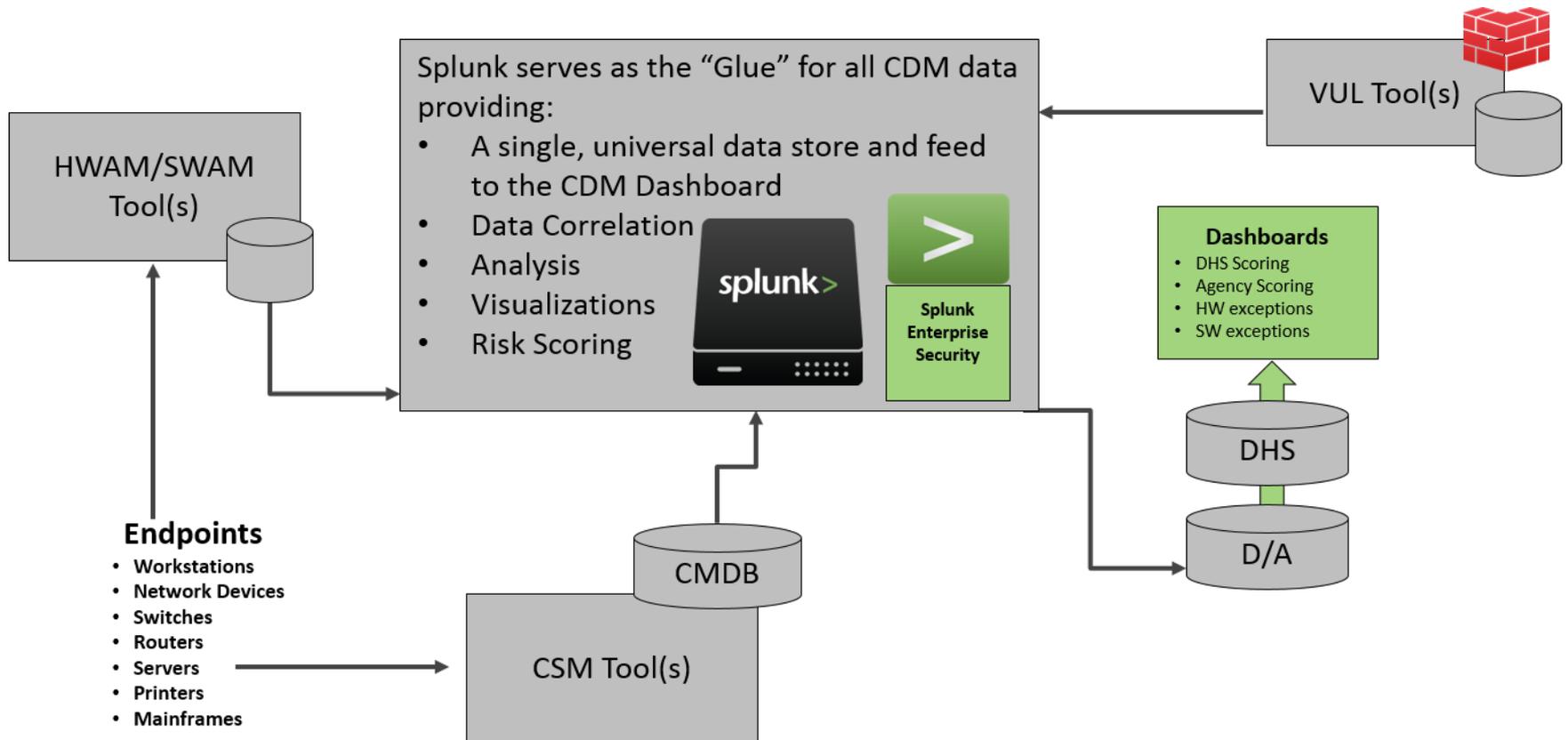
- Manage Assets
- Manage Accounts for People and Services
- Manage Events
- Manage Security Lifecycle



CDM Phase One: Manage Assets

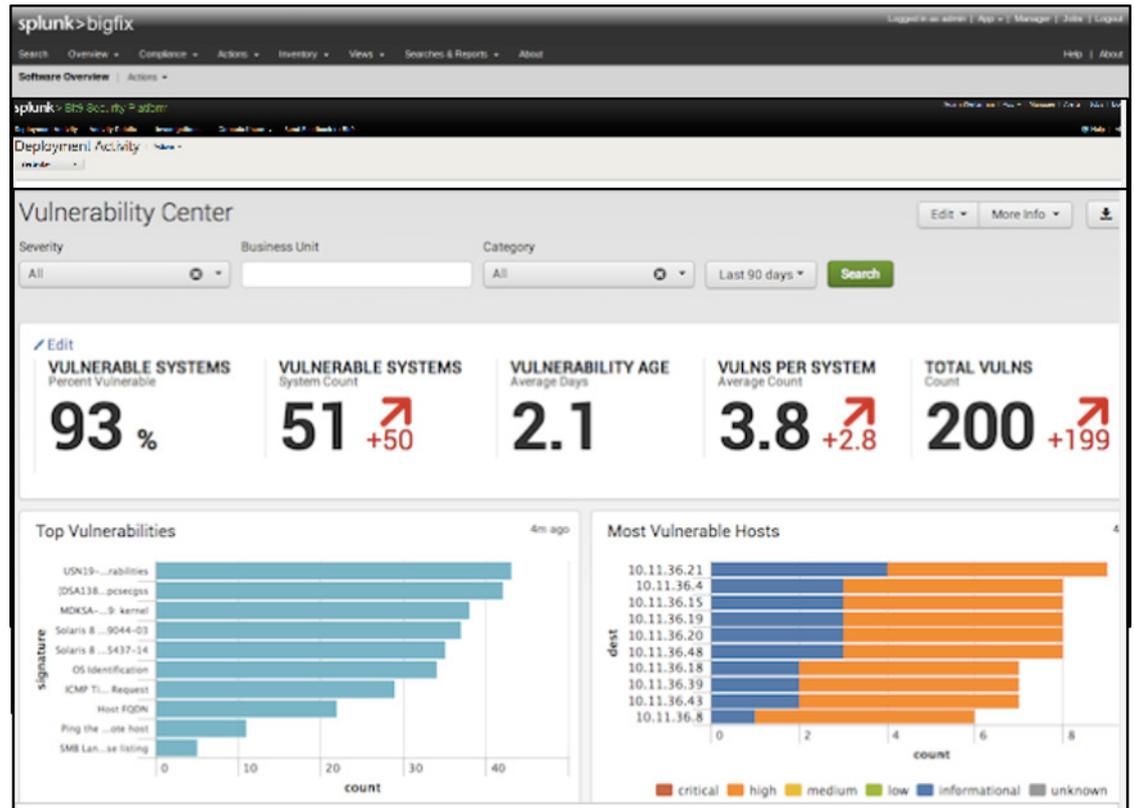


Splunk's Suggested (basic) Phase 1 CDM Architecture



Splunk Apps Available – Phase 1 Support

- Splunk App for BigFix
- Splunk Add-on for McAfee
- ForeScout CounterACT App
- Splunk App for Windows
- Splunk App for Unix
- Splunk App for Bit9 Security Platform
- Splunk App for Symantec
- Splunk for Nessus



Breakout Room Discussion Topics

- What has been the biggest challenge your department/agency has had to deal with during the SWAM implementation or operational stage?
- If you had a challenge, how did you resolve it?
- Do you have any best practices or lessons learned that you can share with the community regarding SWAM implementation or operations?
- Do you have any recommended topics for future webinars and learning community events?



Best Practices and Lessons Learned

- Presentation of any best practices and lessons learned that came from the breakout room discussions



Event Conclusion

Thank you for attending today's
CDM Learning Community Event!

- A certificate of attendance will be available to download on the CDM Learning Program website at www.us-cert.gov/cdm/training, within one week of today's event
- Visit our website to learn more about the CDM Learning Program and upcoming events at www.us-cert.gov/cdm
- For any questions, comments, or suggestions for future topics, please email us at cdmlearning@hq.dhs.gov
- Please take a moment to fill out our 4 question survey



The CDM Learning Program

CDM Learning Program – What’s in it for you:

- Monthly Learning Community Event (CDM-LCE)
 - CDM leaders and implementers discuss relevant CDM topics in-depth, either in a live face-to-face session or using a virtual platform such as AvayaLive!
- Monthly Webinars
 - CDM experts deep-dive into specific CDM topics and participants are able to ask relevant questions using a text-chat function
- Weekly CDM Bits & Bytes
 - Short email awareness tips that link to additional content posted to the CDM Learning forum on GovLoop
- Online Vignettes
 - Short video vignettes which allow the learner to develop foundational knowledge around key CDM concepts and topics

Resources Available: <https://www.us-cert.gov/cdm>



Homeland
Security

Federal Network Resilience

Sign up for our blog!

<https://www.govloop.com/groups/cdm-learning-bits-bytes/>

CDM LEARNING – BITS & BYTES



Group Admins



Public Group active 18 hours, 47 minutes ago

The CDM Learning Community is designed to enhance cybersecurity risk management by fostering a CDM learning environment that increases Departments and Agencies awareness and knowledge about the CDM program and offer a place to exchange best practices for implementing and maintaining the CDM program.

[Home](#)

RSS

Show: — Everything —



[Forum](#)

[Members](#)

11

FEATURED



CAREER

6 Tips for Keeping Your Cool During Difficult Conversations



CAREER

11 Tips to Keep You Motivated at the Office This Summer



CITIZEN ENGAGEMENT

Making the Case for Communications in the Cabinet



KNOWLEDGE NETWORK
FOR GOVERNMENT



Homeland
Security

Federal Network Resilience