SWID Tags – Foundation for Automation

Data Model for Software Identification Data

AGENDA

Problem Space – why do we care/what are tags

Focus Areas – what can we impact

Market Impact – how can we leverage

Cybersecurity Guidance – how can you use

What do you get with normalization

Problem Space
3rd party ID/Normalization will always have issues

- Humans are bad about consistency and normalization
- Different discovery tools = different approaches to naming, grouping, normalization
- Tools have differing focus areas – accuracy and data inclusion varies
- Too many publishers
- Too many platforms
- Too many releases
- Typically patch details are not included
- Expecting consistency from anything other than a single source of truth (the publisher) is the definition of insanity.

What Are SWID Tags

- Most authoritative SWID ID data
  - Provided by publisher
  - Digitally signed
  - Certified
  - Unique tag ID
  - **No lag time in support**
- Additional security requirements
  - **Starting point to chain of trust**
  - Payload for install files
  - **Payload for runtime files**
- Application structures (BOM)
  - Suites, components, plug-ins, **patches**
- May also be created by
  - Open source software publishers/distributors
  - 3rd party organizations (i.e. nsrl.nist.gov)
  - In-house IT operations as software is on-boarded

Tag Data	Birth Certificate Data
Product Name	Name of child
Version	Date of Birth
tag Creator	Gov Organization
Publisher	Mother
Licensor	Father
tagID	Birth certificate number

SWID tags – the starting link for the chain of trust

How Software ID Tags Help

Improve Accuracy

Consistent, normalized and secure data, Unique Tag ID

Reduce Noise

Remove unknown, but related files – focus on product

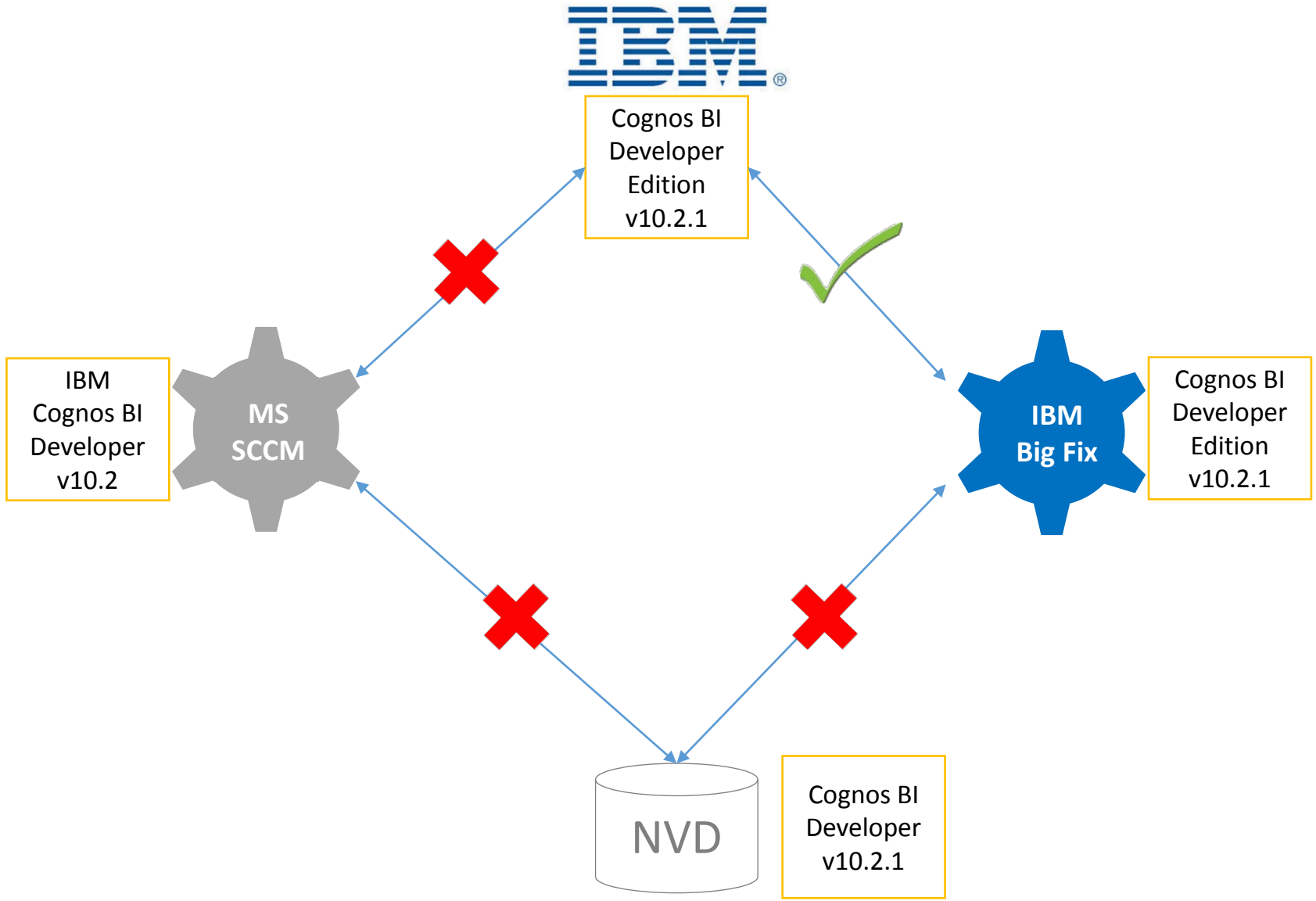
Lower Costs

Automate, automate, automate

Automation of Normalization

An ISO based approach

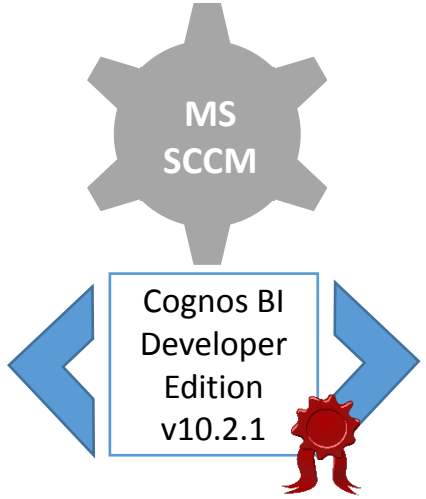
TODAY

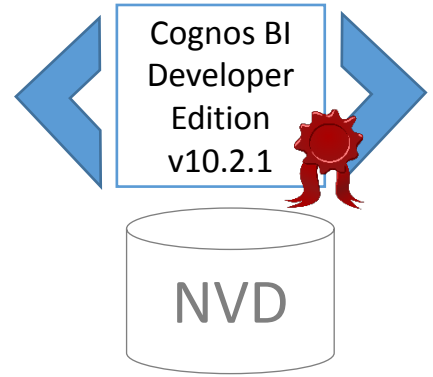


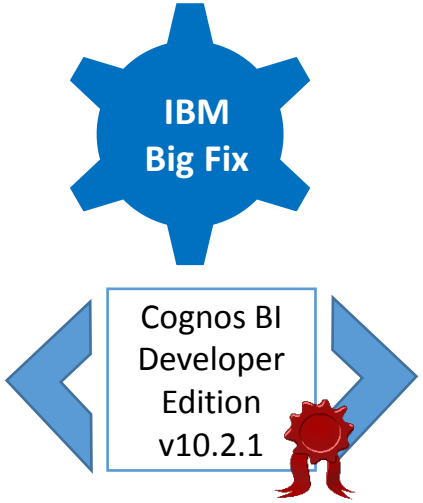
Automation of Normalization

An ISO based approach

Desired State







Automation of Normalization

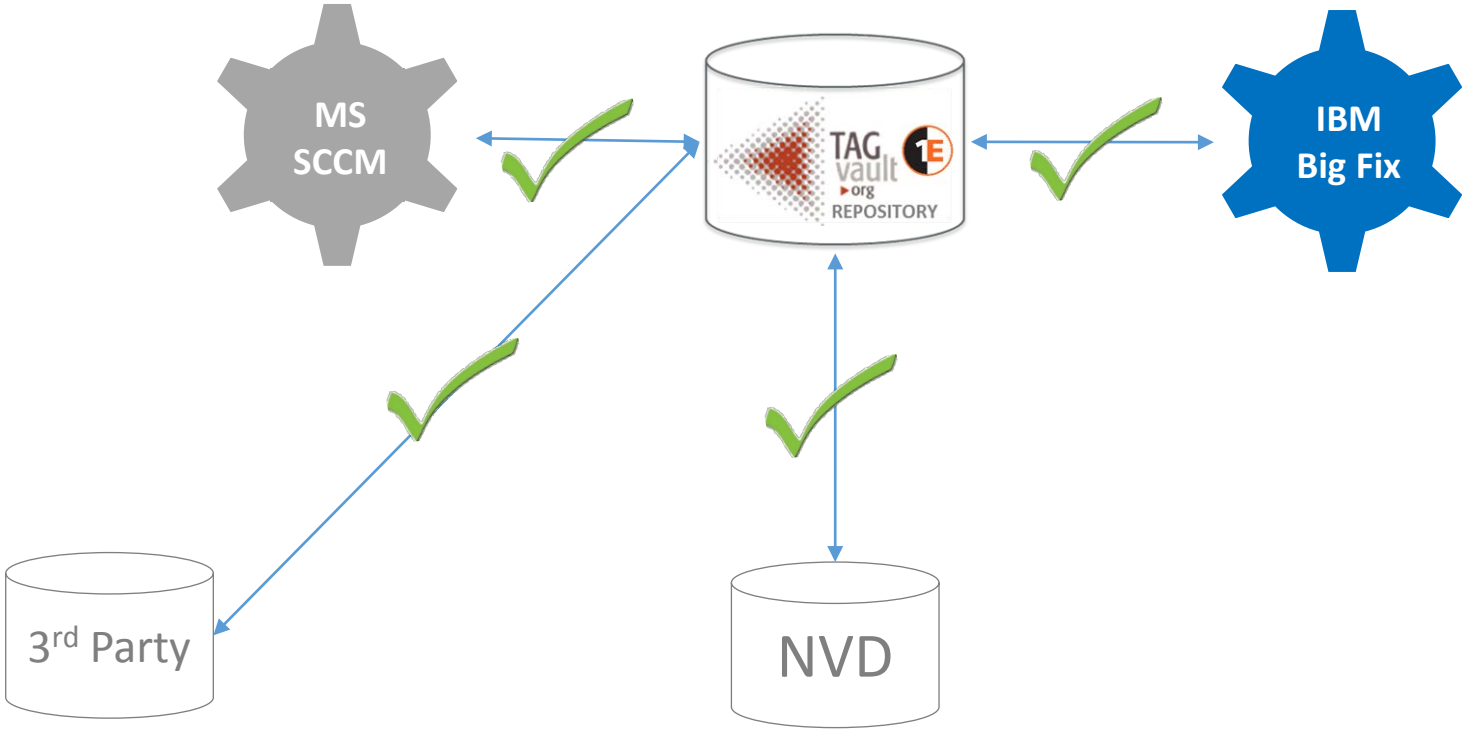
An ISO based approach

Interim Approach

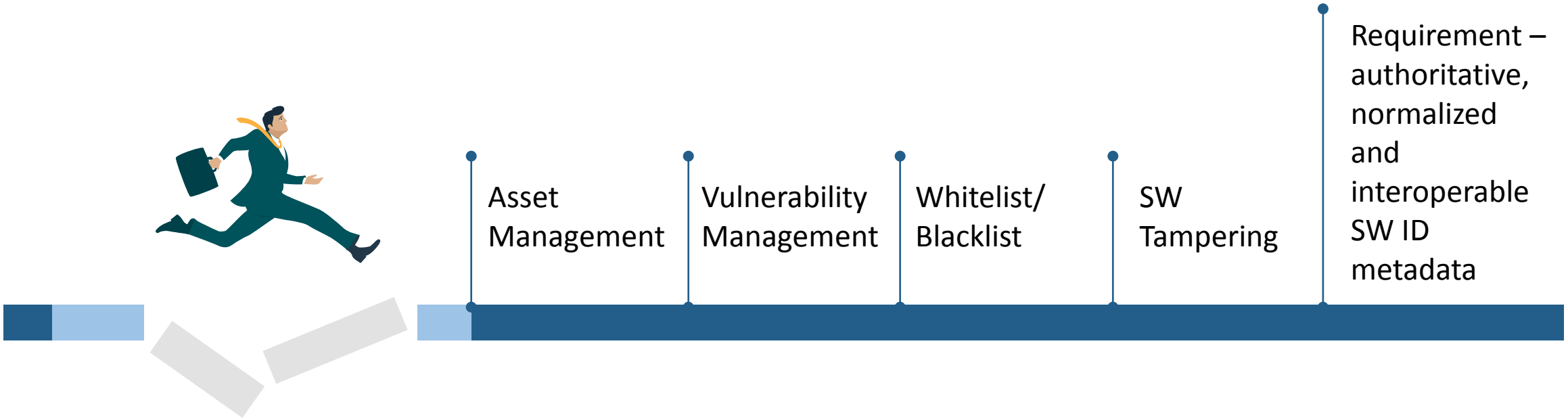
1E Catalog

IBM

Cognos BI Developer Edition v10.2.1



Focus Areas for authoritative SW ID



Market Impact

Most discovery tools support 2009 SWID tags

3 primary Windows Installer tools support creation of 2009 SWID tags

WiX supported 2015 SWID tags before the standard was finalized

1E providing support for SWID Tag Repository for TagVault.org

Standard bodies recognize the need as well and must work in an interoperable environment

- DMTF – incorporating SWID tag data into CIM model
- TCG/TNC – including SWID tag data in IF-M standard
- IEEE Anti-Malware Support Services AMSS – Clean File Metadata Exchange (CMX)
- ISO/IEC – integration with entitlement and usage data
- NIST-IR 8060 – Guidelines for the creation of Interoperable SWID Tags

Market Players

SDO Involvement

IEEE
ISO JTC1 IEC INFORMATION TECHNOLOGY STANDARDS
TRUSTED COMPUTING GROUP
NIST National Institute of Standards and Technology
DMTF

Consumers

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
Anglepoint
GSA
MITRE
NIST National Institute of Standards and Technology
U.S. ARMY

Tool Providers

iQuate
Scalable
hp
IBM
Eracent
Symantec
Microsoft
ModusLink GLOBAL SOLUTIONS
ca technologies
OpenIT

Commercial Publishers

EMC²
Microsoft
Wix
Symantec
hp
IBM

Starting to hear from

Walmart
OPTUM
BEST BUY
DHL
Schlumberger
Roche
BlueCross BlueShield

Companies with logos are members of TagVault.org
SDO's are independent and work with TagVault but do not necessarily endorse TagVault.org

Clean File Metadata eXchange (CMX)

Provides timely information about clean files

Metadata provided by publisher – filename, hash, path, signature data

Data for CMX can be provided by SWID tags that include payload data and are digitally signed

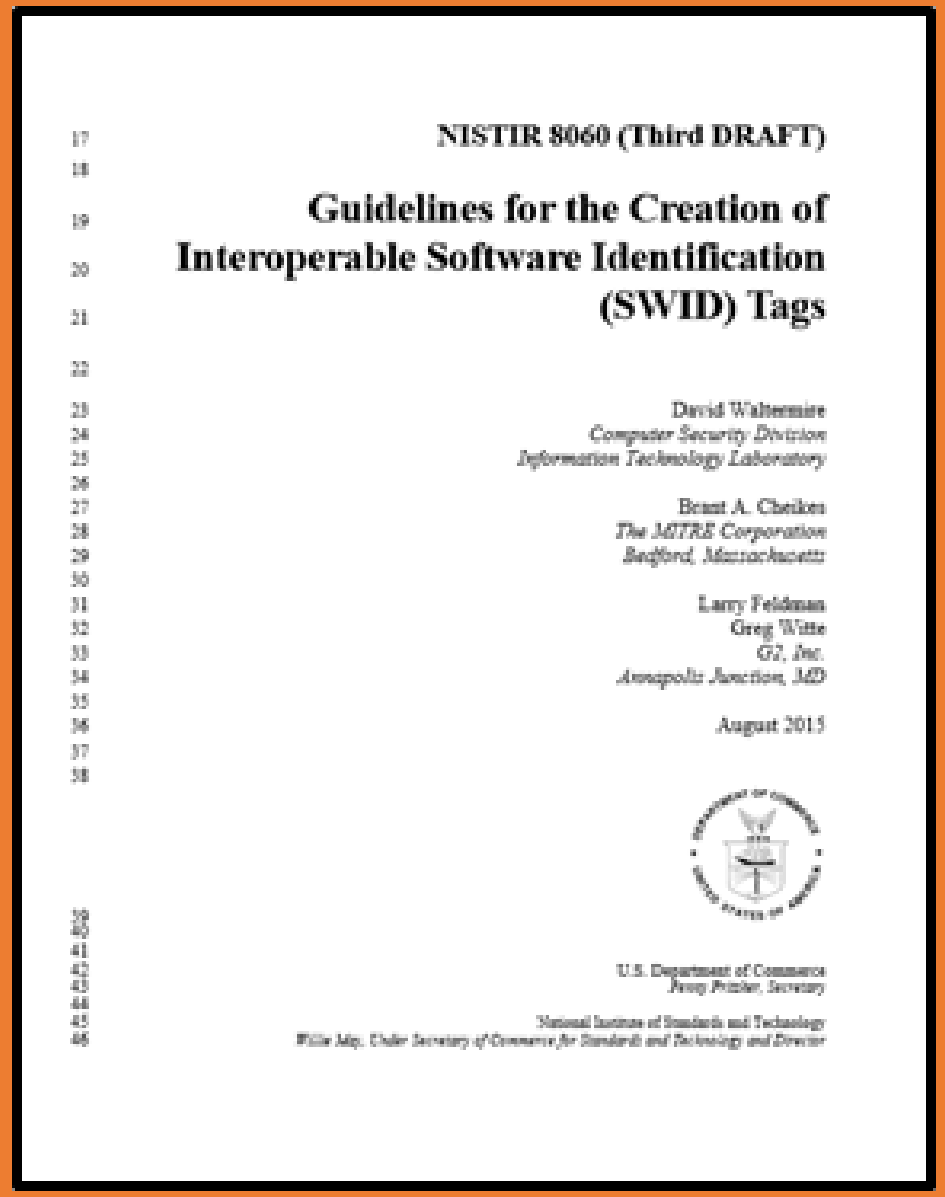
NISTIR 8060

Guidelines for the creation of SWID tags

Based on use cases for tag data

Desire to ensure interoperability

Available for public review - strong request to provide feedback



NISTIR 8060 (Third DRAFT)

Guidelines for the Creation of Interoperable Software Identification (SWID) Tags

David Waltermire
Computer Security Division
Information Technology Laboratory

Brant A. Cheikes
The MITRE Corporation
Bedford, Massachusetts

Larry Feldman
Greg Witte
G2, Inc.
Annapolis Junction, MD

August 2015

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

Cybersecurity Guidance

Utilize industry normalized names/details

1. Signed SWID tag (with trusted signature)
2. Unsigned SWID tags provided by vendor
3. Industry normalized data accessed from trusted industry org
4. SW identified by tool, but not normalized by the vendor, nor trusted third party

---

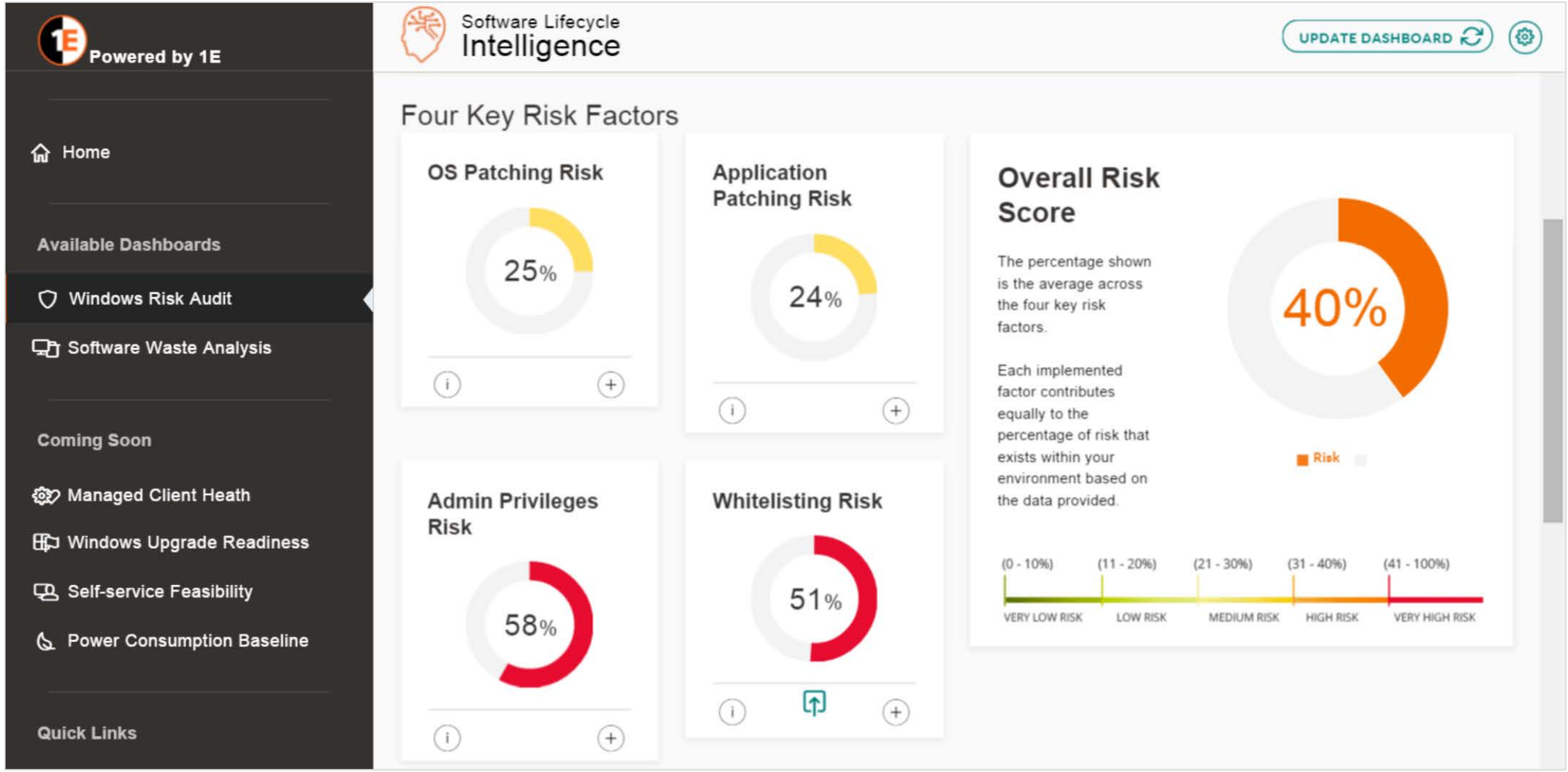
Require SW ID Meta data from all vendors (Walmart is starting to do this)

Customers - require and validate interoperability – only way to get to normalized names

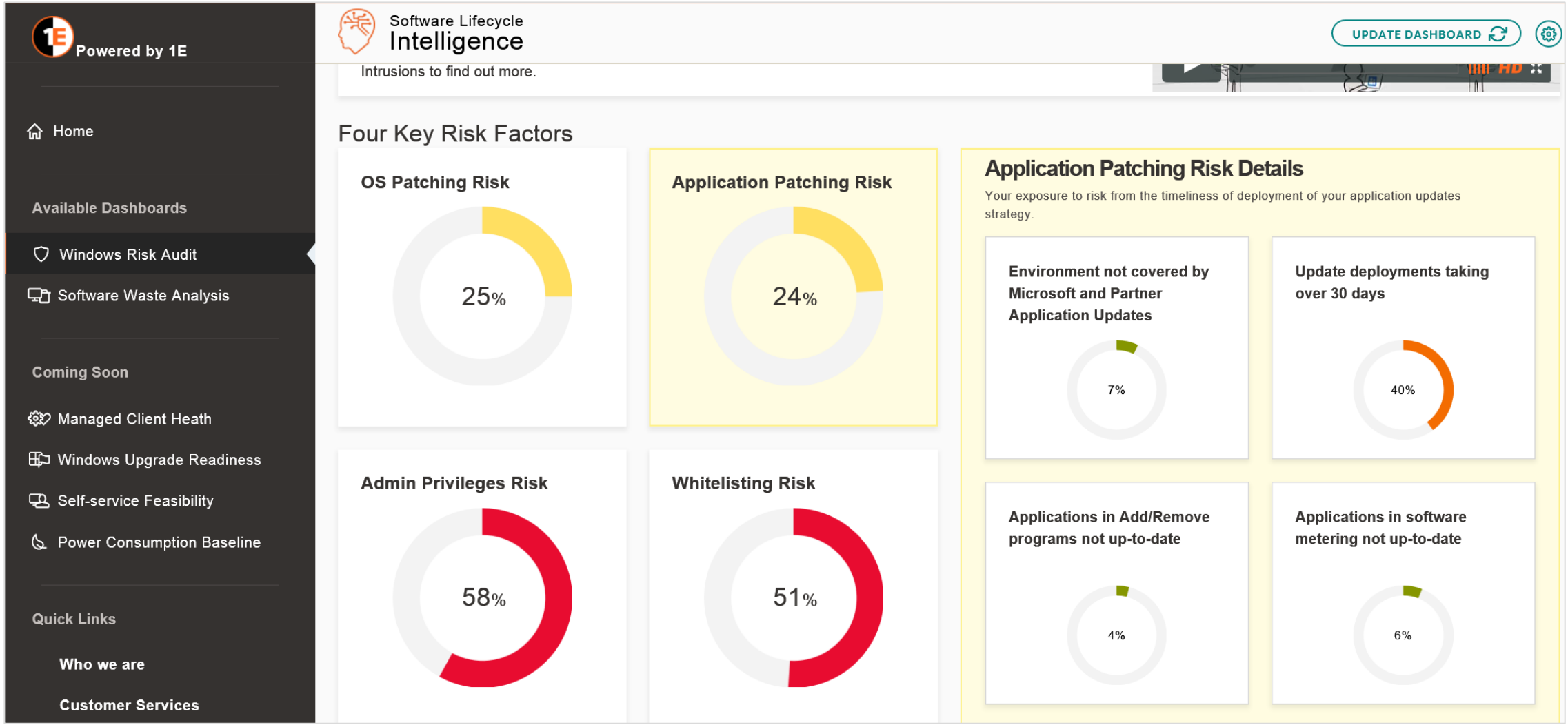
---

Work with others in the field – ensure interoperability

What does Interoperability get us?



What does Interoperability get us?



Thank you

QUESTIONS