"We are paying for What?!"

IT Asset Management: security, sanity and saving money.

Presented by David L. Morse, 28 Feb, 2017
ASQ Regional Software SIG Meeting, McLean, VA
Disclaimer

- This is a presentation of introductory material and early research. It is intended for education and to foster ongoing discussion.

- The opinions expressed do not represent those of the hosting or organizing entities, or of the speaker’s employer (MITRE, ASQ, etc.).

- The information provided is not intended to promote or otherwise evaluate products, services, vendors, or intellectual property.

- Referenced information may not be the most current available about specific vendors or products.

- Questions or comments regarding this presentation should be directed to:
  - David L Morse, dmorse[@]MITRE D0+ org
Agenda

- the challenge
- the academics
- the landscape
- the use case
- the future

Goals

- introduce topics
- get user stories, use cases
- get feedback on research ideas
- foster future discussion
- foment revolution
problem
enterprise (including government) does not know what it has
  - security and cost management depend on asset awareness
  - software, hardware, data and configuration – all need to be inventoried

legacy systems, siloed business units, funding
  - many factors complicate collection of asset info
stakeholders vary

- for software license management = finance and compliance
  - justification of license cost
    - based on installed and usage
  - preparation for audit by vendors
    - penalties and business down-time

- for vulnerabilities and threat response = IT/security operations
  - humans overwhelmed by the pace of threats, number of alerts
    - automating identification, assessment and management of assets.

“IT asset management (ITAM) provides an accurate account of technology asset lifecycle costs and risks to maximize the business value of technology strategy, architecture, funding, contractual and sourcing decisions.” Gartner

“SAM (software asset management) A process for making software acquisition and disposal decisions. It includes strategies that identify and eliminate unused or infrequently used software, consolidating software licenses or moving toward new licensing models.” Gartner
Figure 1. The Six SAM Tool Activities

Source: Gartner (November 2016)
Accurate data is priority

- "garbage in, garbage out"
  - discovery must be comprehensive and accurate
  - inventory must be normalized, de-duplicated

- real savings is from reclaiming under-used licenses
  - must have application usage data
  - aligned with entitlement
The landscape

“Key Findings”

- Complex software licensing options increase software license compliance audit risk and cost uncertainty.
- Evolving deployment models, including physical, mobile, virtual and cloud platforms, have made managing software licensing more cumbersome.
- The use of software asset management (SAM) tools has overtaken that of monolithic IT asset management (ITAM) tools.
- The SAM tool market can be confusing, complicated by the fact that some vendors focus on specific SAM activities, while others provide a broad-based approach.

differentiating tools

- discovery tools (agent / agentless)
  - identifies endpoints and attributes (traditional or virtual)
    - OS, version, patch level, installed applications
    - hardware – storage, peripherals, CPU, RAM, etc.

- configuration management tools
  - integrate with/contain configuration management database (CMDB)
  - analysis of inventory, change endpoint settings, deploy OS/applications/patches
  - integrate with authentication (e.g. MS Active Directory)
  - e.g. Microsoft SCCM and IBM BigFix

- compliance tools have ability to
  - incorporate entitlement data
  - analysis of inventory (internal or external)
  - set of rules to identify compliance status
    - client centric (e.g. MS platforms)
    - server centric (more complex, variable)

- 3rd party auditors may expect to use organization’s native tools
use case –
license management

“Global enterprise software waste today stands at 38%, totaling $28 billion of waste in the US alone, or $247 per user…”  

enterprise wants to measure cost of installed product
  ▶ need to discover all endpoints with installed product
  ▶ assess installed version against entitlement
  ▶ quantify product usage
    ▶ may determine some instances are underutilized
    ▶ gain savings by reclaiming (uninstalling) instances
  ▶ accurate metrics allow strategic planning
    ▶ do we need so many licenses? a different deployment?
use case – compliance

- compliance is more concerned with ensuring business continuity (less so with savings)
  - being in compliance means:
    - reduced risk of business interruption (e.g. due to audit)
    - reduced risk of unexpected costs (e.g. due to penalties from vendors)
- the asset data gathered for compliance also supports
  - vulnerability management
  - patch management
  - etc.
NCCOE mission - creating example solutions for commercial industry to use
  ▶ using today’s tech for today’s problems - not government focused
  ▶ solving basic issues like asset management
  ▶ using standards and NIST best practice
    ▶ after applying Risk Management Framework (RMF)
    ▶ then, map to Cybersecurity Framework (CSF) (business drivers)
  ▶ use open source when gap
    ▶ no vendor solution, or no vendor volunteered product for lab
  ▶ publish implementation details for public use / education

use case - Financial Services Sector, IT asset management

focused on the needs of the security analyst
  ▶ trying to bring them all they need in consolidated view
  ▶ move from siloed datasets to complete set, allow drill down
  ▶ can do analytics (e.g. within Splunk) and dashboard the metrics
    ▶ E.g. ? What are the current vulnerabilities across my assets?

https://nccoe.nist.gov/projects/use_cases/financial_services_sector/it_asset_management
the future

- improved recognition of products
  - normalization of naming and versioning
    - e.g. publishers releasing all products with tags
    - note, a current example, IBM does this now
  - this increases accuracy of usage and vulnerability metrics

- automation of all processes including remediation
  - expansion of existing product functions
    - e.g. from discovery and inventory to full SAM
  - expect established players will consolidate market
  - current offerings will increase integrations
    - e.g. orchestration products (NOC/SOC/IT-ops oriented) will expand their ability to connect to and control other devices and tools, enabling increasingly complex “playbook” responses to alerts
One approach to solving normalization – publisher defined data.

Example SWID tag - “.swidtag” – unique ID and name for product. Very basic example, this tag does not show optional elements, such as payload hashes or digital signature.

```
<?xml version="1.0" encoding="UTF-8"?>
<SoftwareIdentity name="IBM Endpoint Manager for Patch Management - 9.2.0"
uniqueId="69647496a81546c6ab20892a00014ede-9.2.0"
version="9.2.0"
versionScheme="multipartnumeric"
xmlns="http://standards.iso.org/iso/19770/-2/2014-CD1/schemaxsd"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
Meta persistentId="69647496a81546c6ab20892a00014ede"/>
<Meta taxonomyCode="SSKLK5"/>
<Meta taggingProcess="4-1-20140704"/>
<Entity name="IBM" regid="regid.1986-03.com.ibm"
role="licensor publisher tagcreator"/>
</SoftwareIdentity>
```

Multiple publishers (i.e. IBM, Microsoft, Symantec, Adobe, etc.) are producing SWID tags with some or all of their software products. Some discovery tools are able to ingest SWID tags.

Note: The SWID specification has the optional `<SoftwareIdentity> @version` attribute with a default value of “0.0”. If the publisher uses versioning (e.g. in accordance with the SemVer standard) this attribute should be filled in appropriately. This is critical for most SAM/ITAM and security functions.
Traditional Discovery Approach

Note: discovery typically requires an agent

License Estimate
N x Browsers
1 x App Server
2 x Transaction Svr
2 x Database

5 apparent licenses (possibly more for browsers)
Discovery with SWID Tags

More accurate results with normalized metadata from SWID tags.

**Note:**
discovery can be agent, or agentless (supporting cloud & virtual systems)

License Estimate
2 x Transaction Svr
2 Licenses

Copyright TagVault.org, 2014
Example IBM metrics tag “.slmtag” – local logging of app usage-time for auditing.
we discussed the need for accurate discovery and normalized data – tags are one approach

what is necessary for success with tags?

is there a “critical mass” point?

- enough products are tagged by publishers
- tools are built to ingest and evaluate tags

will digitally signed SWID tags provide sufficient:

- authenticity (publisher, distributor, tag creator...)
- integrity (trusted product payload and file hashes)
- ease of use in automation (PKI infrastructure and crypto requirements, repositories for vendor “gold tags”)

How will this work in cloud with VMs, containers...?
References

- NCCOE ITAM Solution for Financial Services, https://nccoe.nist.gov/projects/use_cases/financial_services_sector/it_asset_management
- Semantic Versioning Specification (SemVer), http://semver.org/spec/v2.0.0.html
This is a presentation of introductory material and early research. It is intended for education and to foster ongoing discussion.

The opinions expressed do not represent those of the hosting or organizing entities, or of the speaker’s employer (MITRE, ASQ, etc.).

The information provided is not intended to promote or otherwise evaluate products, services, vendors, or intellectual property.

Referenced information may not be the most current available.

Questions or comments regarding this presentation should be directed to the author:

- David L Morse, dmorse[ AT ]MITRE D0+ org