Open Source in the Government and Industry

Bill Vass
President/COO
Sun Microsystems Federal, Inc.

“Recovering CIO”
bill.vass@sun.com
blogs.sun.com/BVass

Recent Press on Open Source

- **CIO Magazine:** "The Recession will lead CIO's to move to open source"
- **eWeek:** "10 things IT organizations will do during The Recession"..."#1 Move to Open Source"
- **GCN:** "OSD Guidance Memo to move to Open Source"
- **GCN:** "Defense Appropriations language advocates a move to Open Source"

Why the Fed's Move to Open Source?

Enterprise IT Requirements

- ✓ Increased Security
- ✓ Reduced Procurement Time
- ✓ No lock-in or lock-out
- ✓ Reduced cost
- ✓ Increased quality

Developer Requirements

- ✓ See the source code
- ✓ Contribute fixes & features
- ✓ Fix bugs themselves
- ✓ Work together with each other to create solutions
- ✓ Government can engage to evolve the product - FMAC

Security:

- All proprietary software is written globally: Microsoft, Oracle, IBM, ...
  - Primary development locations:
    - India
    - China
    - Russia
  - Open Source and open development processes enhance overall security and visibility
  - Open Source, there is no place to hide

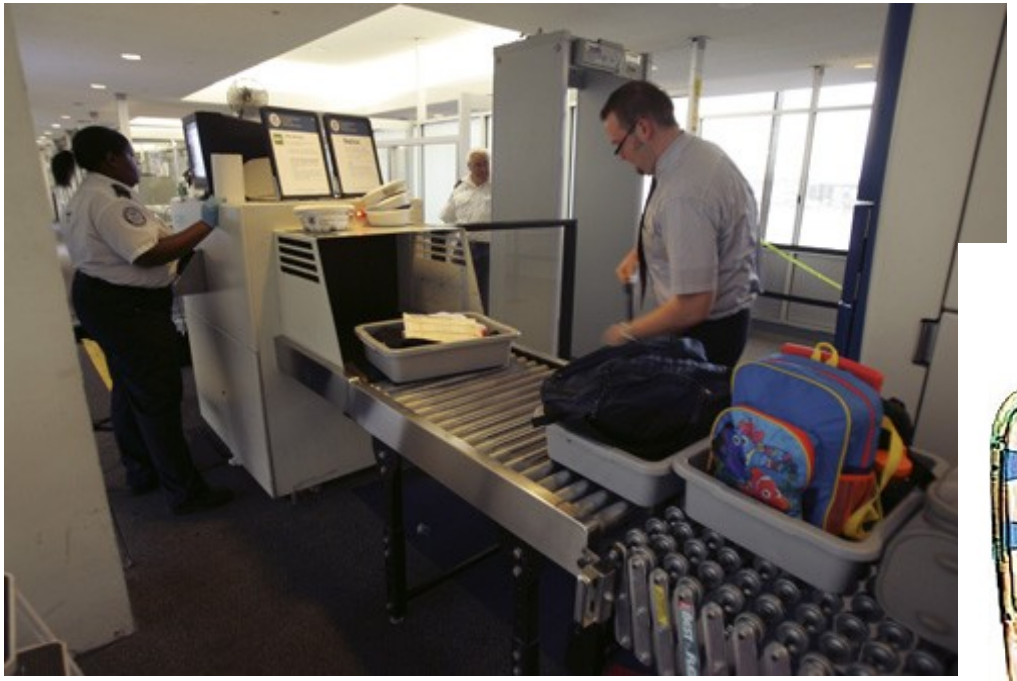
Security:

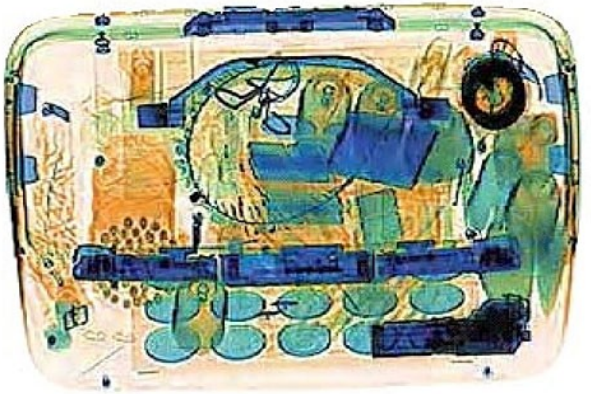
- Proprietary software may be reviewed and even certified by “Experts”**...However**
- A small number of experts can't compete with a community (160K – Solaris, 3M - Java)
  - Every time a Proprietary package is opened up, new vulnerabilities are found quickly (Solaris, Java,...)
  - Community vulnerabilities are usually fixed **before** they are exploited

>

Security:

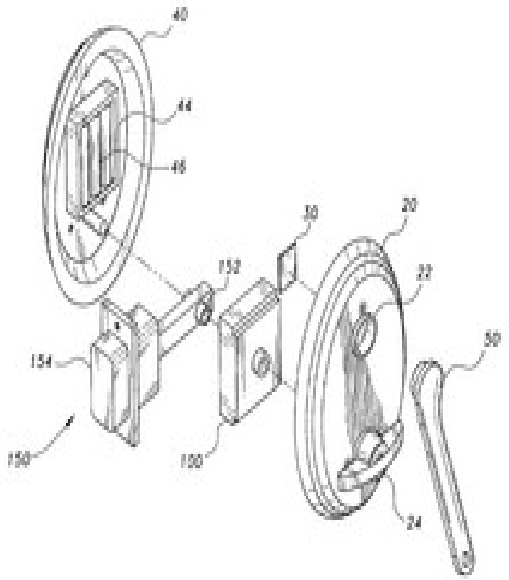
- Public / open source can be scanned with tools to improve overall security
- Proprietary vendors say “trust us”, Open Source code can be verified with third party tools

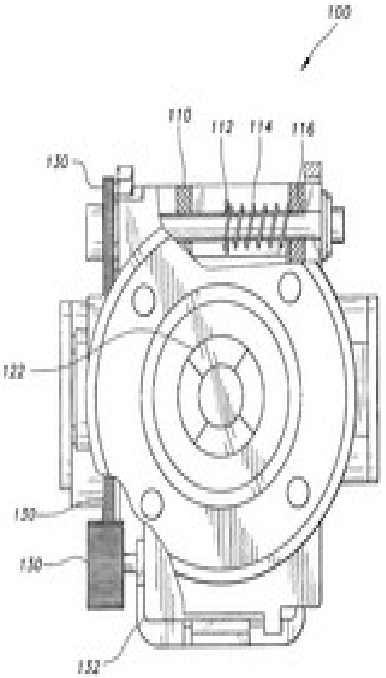


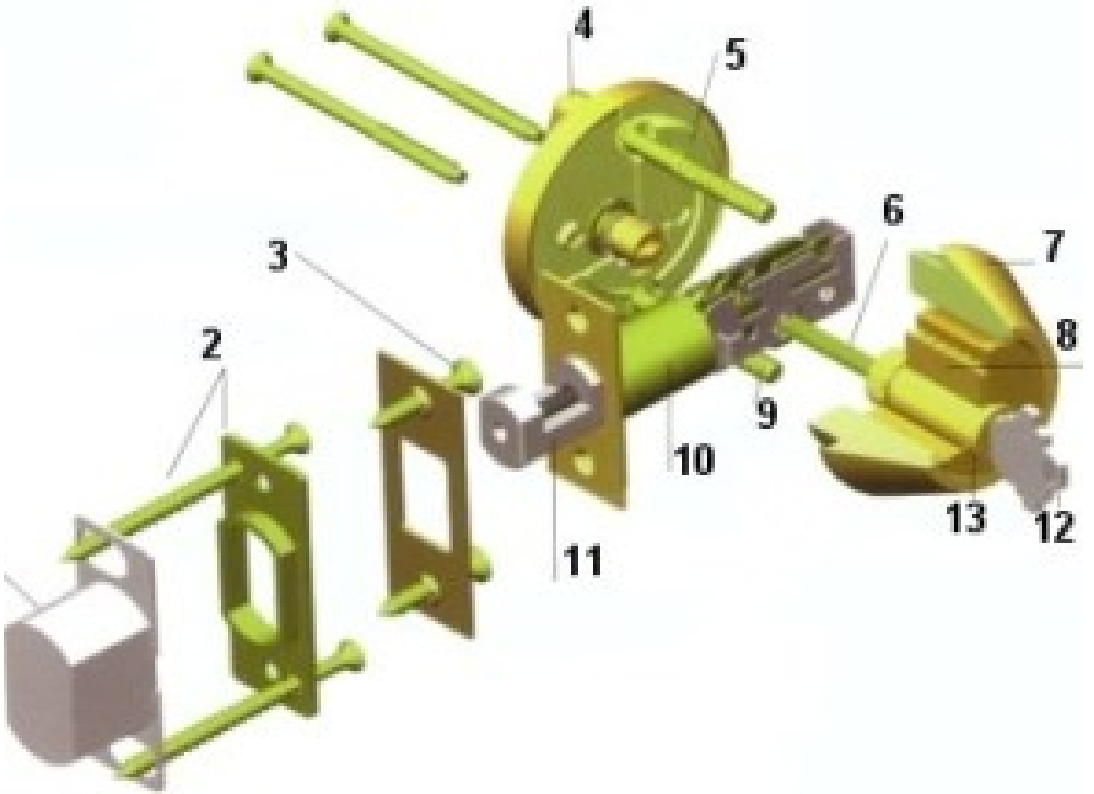


Security:

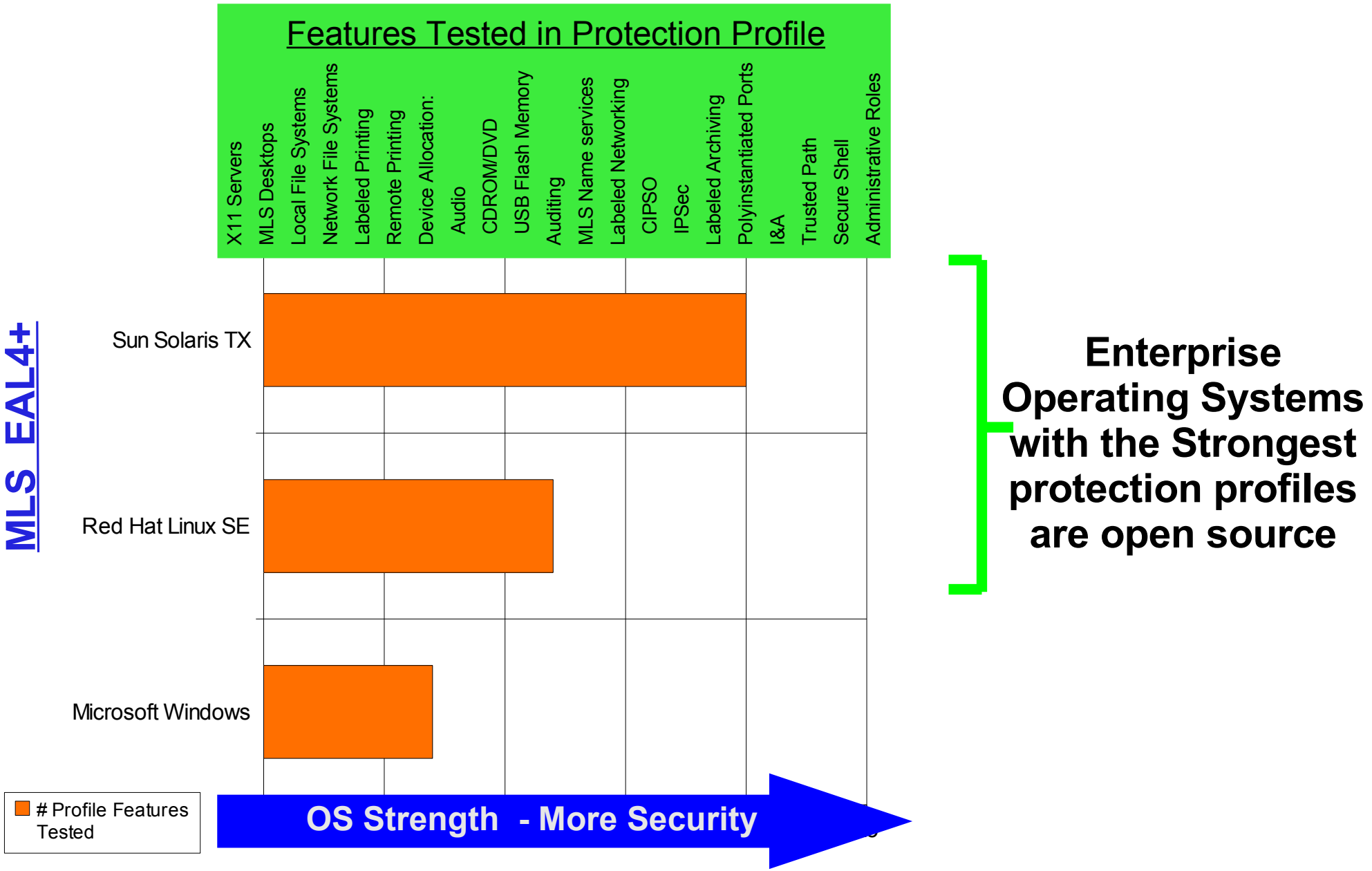
- Good Physical / Cyber Security is done in the open
  - Open Development means the security secret can't be in the code, it must be managed outside the code
  - Security through obscurity, isn't
  - Cryptography examples: RSA vs. Clipper Chip





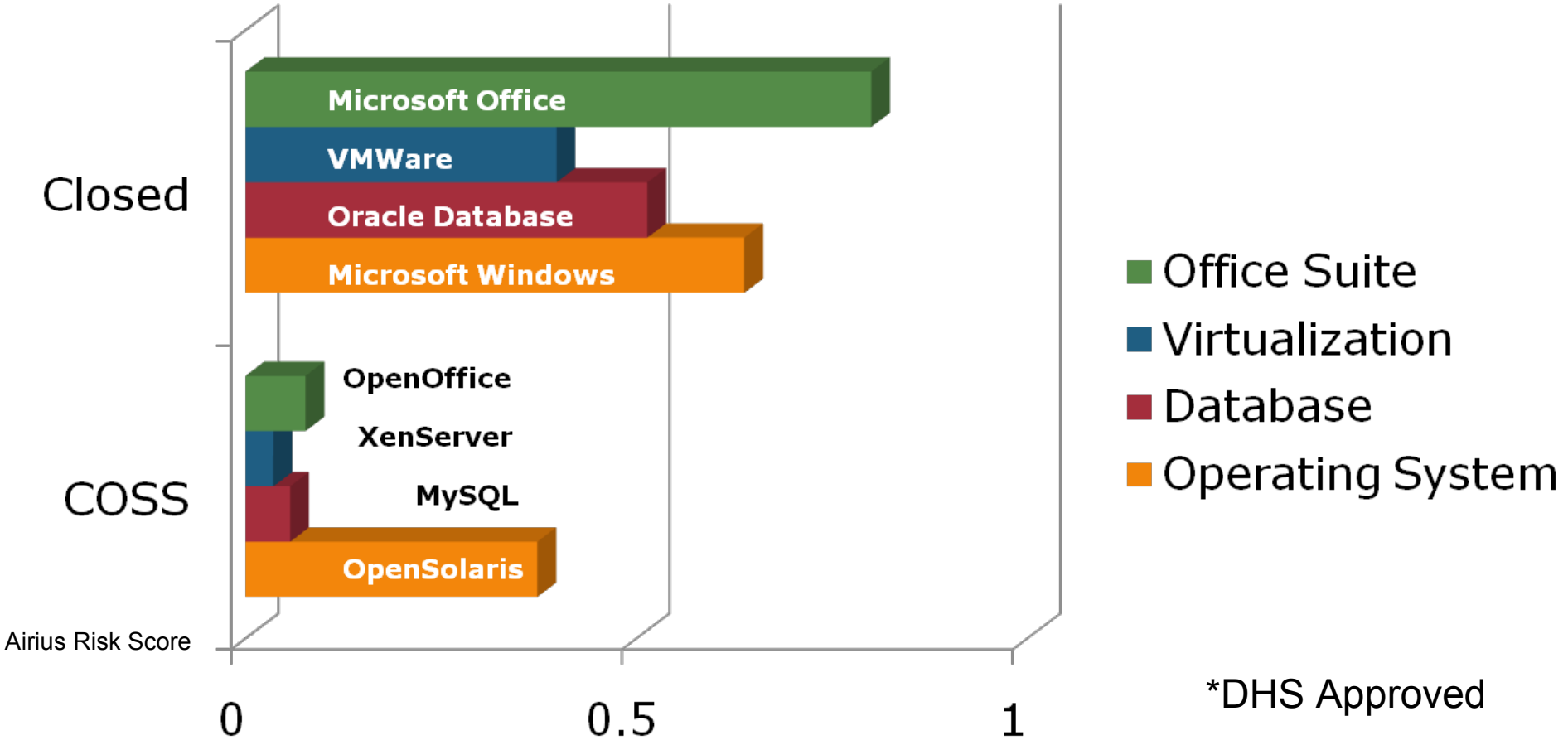


Common Criteria Certified Operating Systems



Software Vulnerability Data

National Vulnerability Database Cumulative Total
http://nvd.nist.gov/nvd.cfm + CPE + CBSS/CBE (Vulnerability Score)



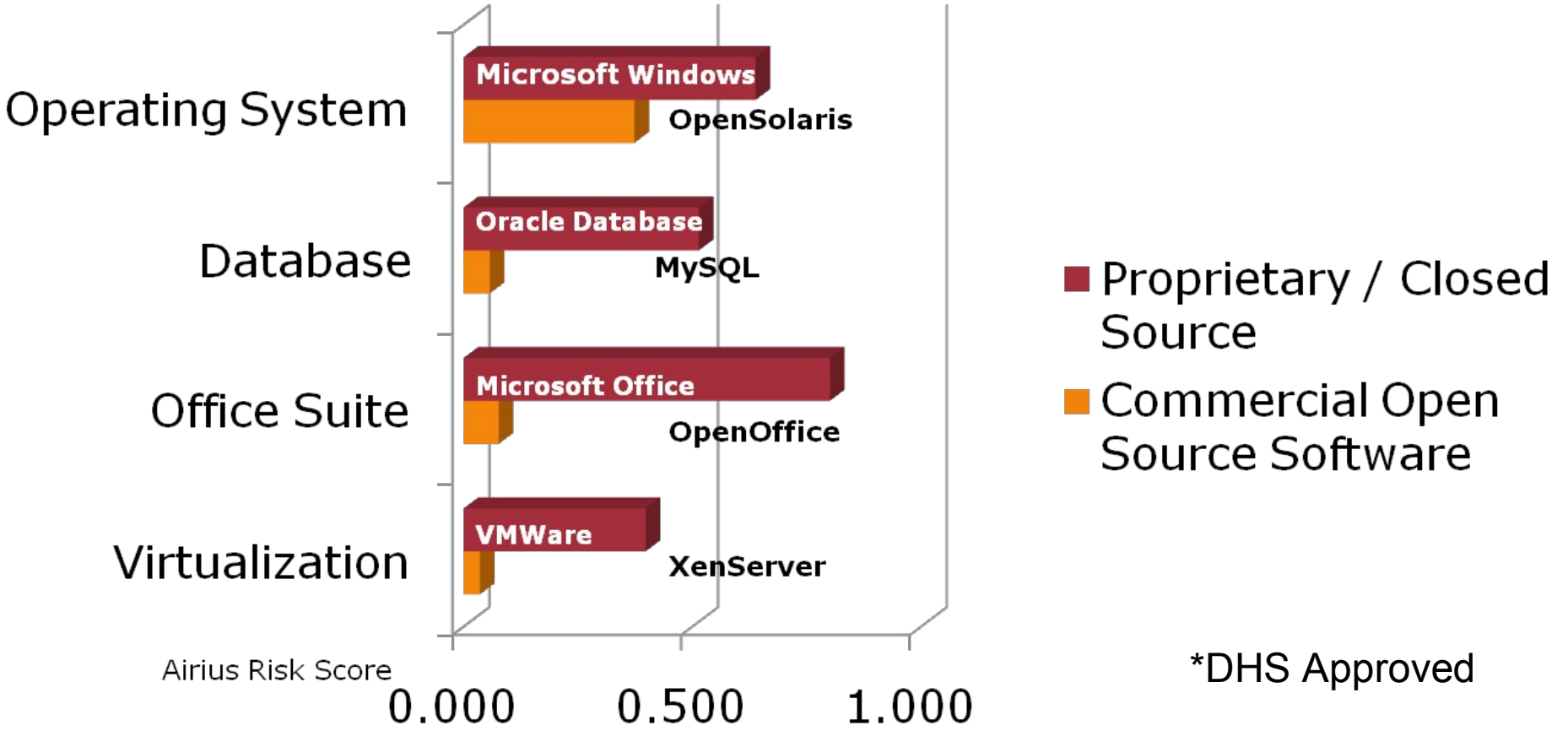
*DHS Approved

Source - Airius Risk Report: 12/31/08

Relative Risk: COSS v. Closed

Software Vulnerability Data

National Vulnerability Database Cumulative Total
http://nvd.nist.gov/nvd.cfm + CPE + CBSS/CBE (Vulnerability Score)



*DHS Approved

Source - Airius Risk Report: 12/31/08

Sorted by Solution Type

Reduced Procurement Time:

- Download, Verify, and Go
  - Don't have to wait for vendors to pilot
  - Don't need to go through a long procurement
  - Recent Examples:
    - HHS - ESB
    - CANES - ESB
    - Hours vs. Years
  - Can scale quickly when needed
  - Not held back by process

No Lock-in or Lock-out:

- Interfaces are usually open, but always publicly exposed
- Public interfaces allow interoperability
- Public code means support from:
  - Multiple vendors can provide support
  - Systems Integrators can provide support
- If vendor EOSL, others can support
- Investment protection beyond one vendor

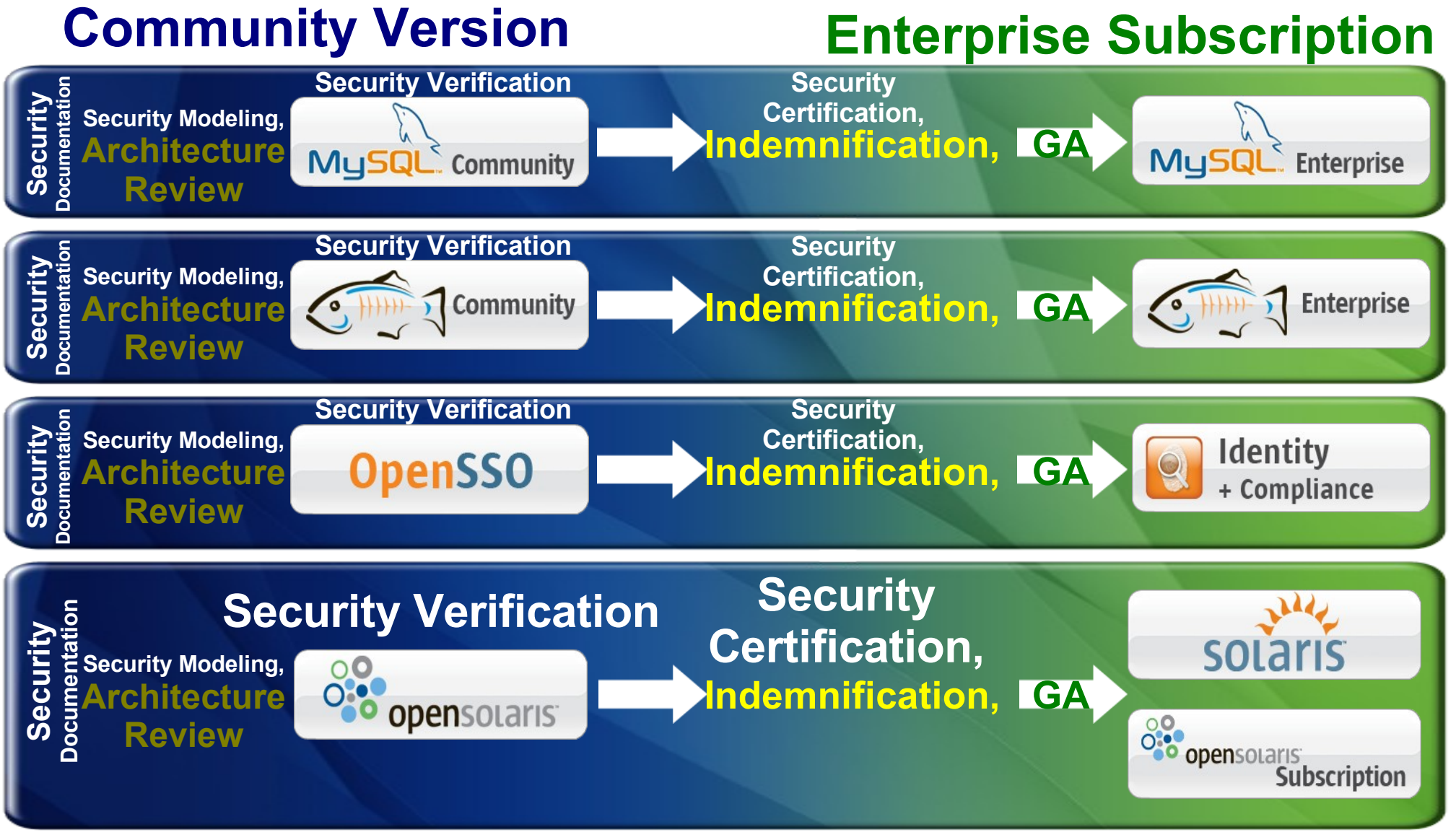
Reduced Cost:

- Zero cost of acquisition, but **NOT FREE**
  - Open source Enterprise applications are available on nearly all operating system kernels, including Linux, Open Solaris, Apple OS X, and even MS Window
  - There are Enterprise Ready Open Source applications for almost any need: OS, Middleware, Database, and Desktop
- **Often can be 90% of the functionality for 10% of the Cost**
- Faster acquisition and deployment also save cost
- Bottom Line: **Do more with less**

Increased Quality:

- Public and Community inspection improves the code
- Supported open source code goes through multiple inspections:
  - > Community inclusion / critical review
  - > Architecture review
  - > IP infringement / Indemnification review
  - > Backward compatibility check
  - > Security review
  - > QA /Test
  - > Productionalization / GA

Commercial Open Source Software Development



Government Engaging with Community to Develop or Influence Products:

- FMAC Project with Open Source Solaris
- SAM /QFS ILM extensions
- HHS /ESB – NetBeans Health objects
- SE Linux
- TE in FreeBSD / BSD
- TE in Java and MySQL
- Label aware ODF / OpenOffice
- World Wind 3D Java
- Many other programs

We want the work we do to be public domain

Sun microsystems

DoD Open Technology Conference

Open Source in the Government and Industry

Bill Vass
President/COO
Sun Microsystems Federal, Inc.

"Recovering CIO"
bill.vass@sun.com
blogs.sun.com/BVass

Risk/Time Score metrics

- Considers TIME as a critical element when considering "current risk", or risk as of right now.
- Provides a weighted metric to sort issues, riskiest being highest, relative to NOW
- Sorts DANGER messages in a prioritized order of relevance. Cuts through the noise and makes sense of CVEs

Using Time To Understand Risk

- What is the Risk Report?
  - The Risk Report is dynamic risk analytic data product generated by Airius Internet Solutions using public protocols and verified data from the National Vulnerability Database.
  - Uses in order from NVD -> CVE, CPE, CVSS, OVAL -> information is imported to MySQL database for query.
  - The risk metrics are collected automatically and sorted. Members of the Airius team correct discrepancies introduced by bad data, and then the results are generated using automated statistical queries on MySQL.
  - http://nvd.nist.gov is the official datasource for the risk information.
- Airius Risk/Time Score
  - The ordered output is generated by an algorithm that scores a weighted value for each CVE based on the risk and age of that CVE, and then totals all the weighted CVEs across the life of a product. Such total scores are then compared one to another. In this way, an application that has been out for a very short time could make the top of the list if it had more security issues of high criticality over its release life than most applications. This differs from the usual method of just tracking total issues over the life of a product.
  - The Risk/Time scoring system is a distinct creation of Airius Internet Solutions
- Acceptance of Data Aggregation and Scoring System
  - The Risk Report is being presented at DHS Software Assurance Forum on March 12, 2009
  - **"The Risk Report: Using SCAP Data to Output Time Sensitive Risk Analytics for FOSS"**
    Ernest M. Park, Chief Scientist, Airius
- References
  - https://buildsecurityin.us-cert.gov/swa/forum/agenda.html
  - Joe Jarzombek, PMP
    Director for Software Assurance
    National Cyber Security Division
    Office of Assistant Secretary
    for Cyber Security & Communications
    Department of Homeland Security
  - http://nvd.nist.gov/validation.cfm
  - http://nvd.nist.gov/
  - http://gpl3.blogspot.com
  - http://nvd.nist.gov/scap.cfm
  - http://fossbazaar.org/blogs/ernestpark

Behind the Risk Report

Airius Internet Solutions – 203-354-8800, risk_report@airius.com