IT Vulnerability Management

BROTIGHT

KEEP IT TIGHT WITH US

Minimizing Risk by Implementing Vulnerability Management Process

On time – On Budget – On demand

Classified document, not allowed to distribute.

Agenda

- 1. Need for Vulnerability Management
- 2. Vulnerability Management Process
- 3. Capabilities Overview
  - 3.1 Overview
  - 3.2 Software as a Service Model: Security & Coverage
- 4. Summary
  - Advantages & Benefits

Classified document, not allowed to distribute.

1. Need for Vulnerability Management

- **Vulnerabilities on a network are GOLD to cyber criminals:**
  - Provide unauthorized entry to networks
  - Can expose confidential information, fuel stolen identities, violate privacy laws, or paralyse operations
  - Exposure is extreme for networks with vulnerable devices connected by IP

Sources of Vulnerabilities

- ☒ Programming errors
- ☒ Unintentional mistakes or intentional malware in General Public License software
- ☒ Improper system configurations
- ☒ Mobile users sidestepping perimeter security controls
- ☒ Rising attacks through viewing popular websites

Classified document, not allowed to distribute.

1. Need for Vulnerability Management

- **Despite utilization of basic defenses, network security breaches abound**
  - TJX exposed 46M records
  - DSW exposed 1.4M records
  - Card Systems exposed 40M records
  - 215M+ reported record exposures since 2005
    (actual is significantly higher)

- **Automation is Crucial**
  - Manual detection and remediation workflow is too slow, too expensive and ineffective

Attack Trends

- ☒ Increased professionalism and commercialization of malicious activities
- ☒ Threats that are increasingly tailored for specific regions
- ☒ Increasing numbers of multistaged attacks
- ☒ Attackers targeting victims by first exploiting trusted entities
- ☒ Convergence of attack methods
- ☒ Shift from “Hacking for Fame” to “Hacking for Fortune”

Classified document, not allowed to distribute.

1. Need for Vulnerability Management

- **Did we learn our lessons?**
  - Most vulnerabilities are long known before exploited
  - Successful exploitation of vulnerabilities can cause substantial damage and financial loss
  - A few vulnerable systems can disrupt the whole network
  - System misconfiguration can make systems vulnerable

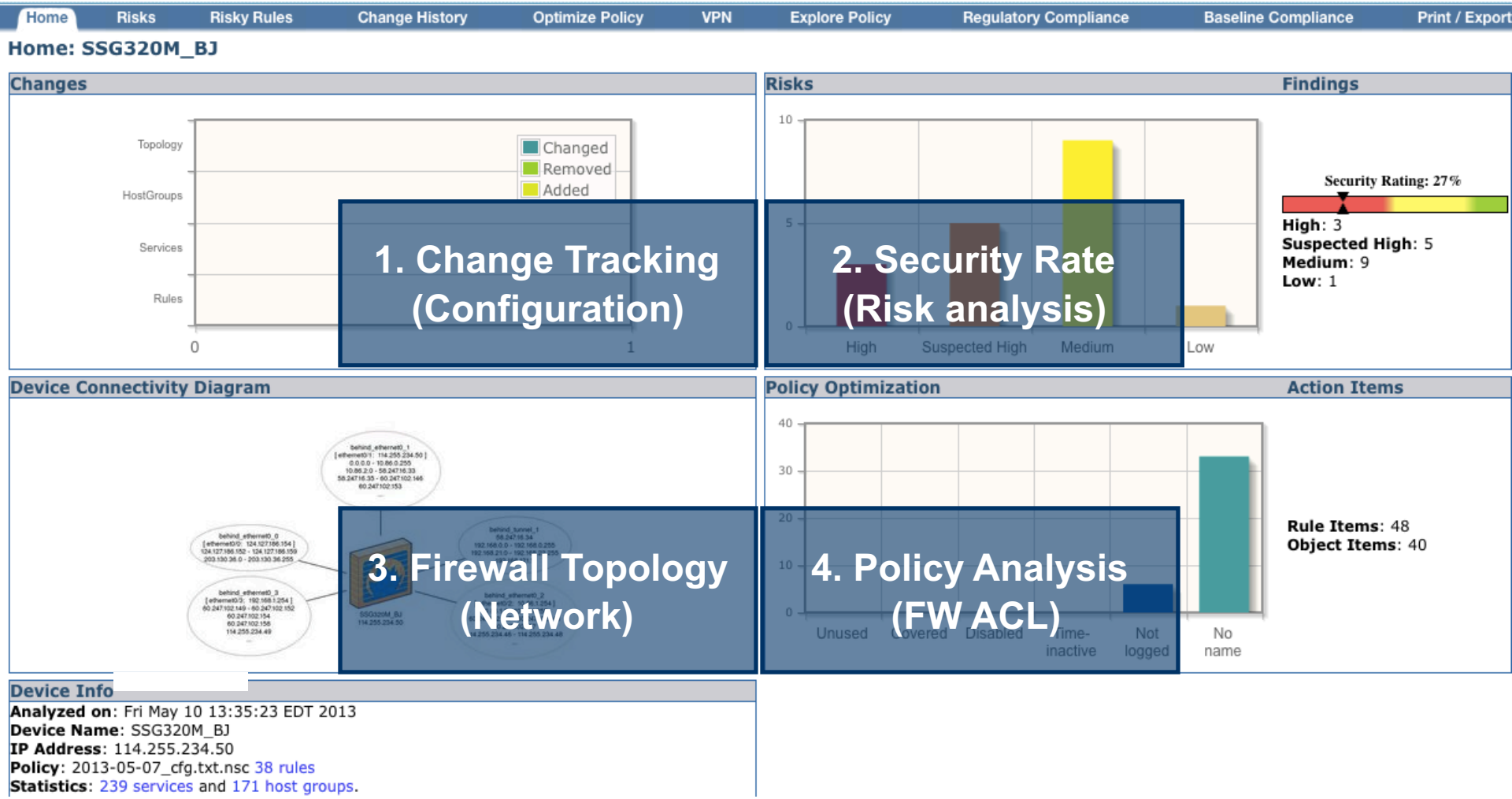
Challenges IT Security Face

- ☒ NOT enough TIME, PEOPLE, BUDGET
- ☒ Prioritization of efforts for minimize business risks and protecting critical assets. We can't fix all problems - what can we live with?
- ☒ Reduction of operational & capital expenses
- ☒ Adapting to accelerating change in sophistication of attacks and increasing number of regulations

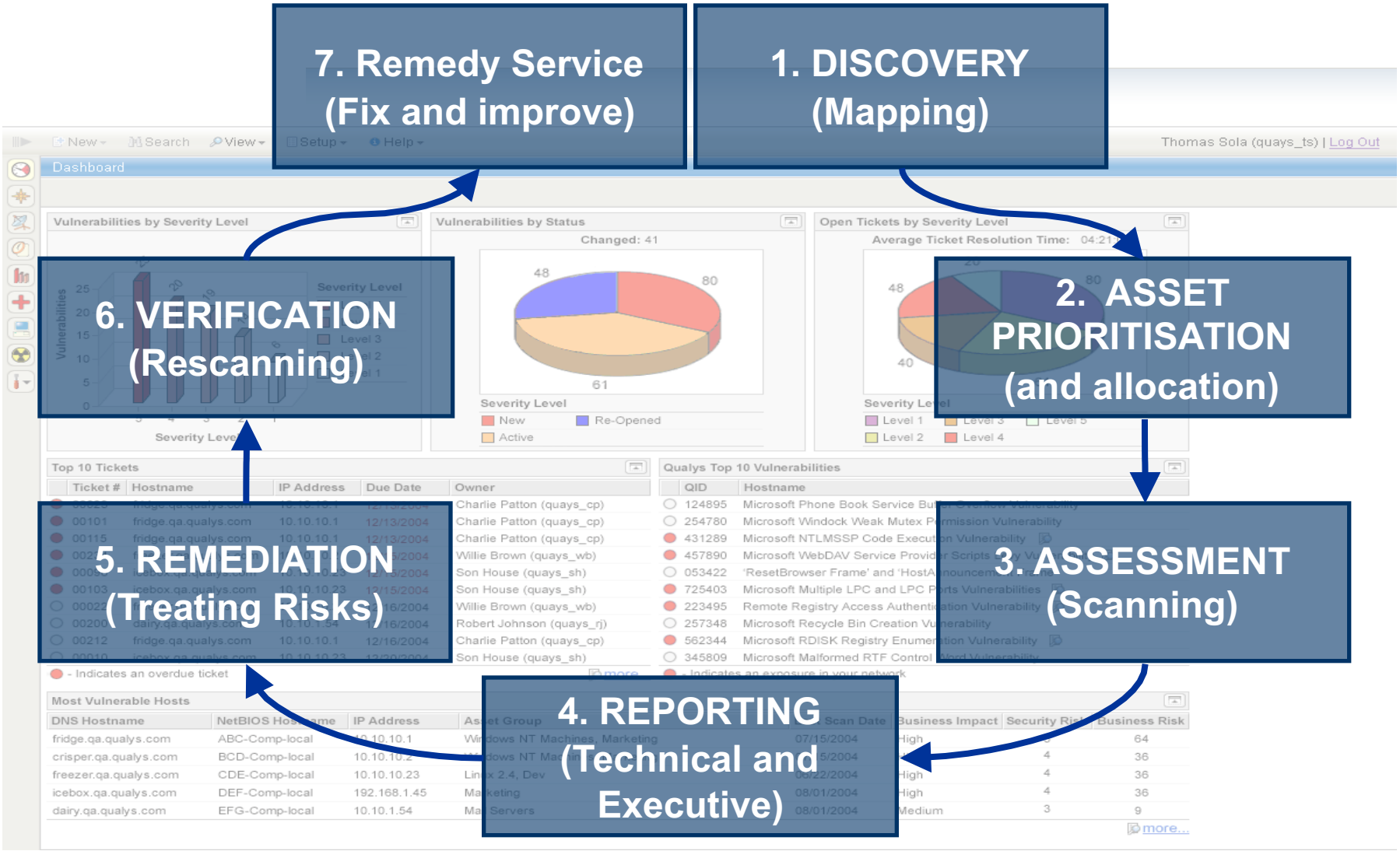
Classified document, not allowed to distribute.

1. Firewall Configuration Analysis

Report example

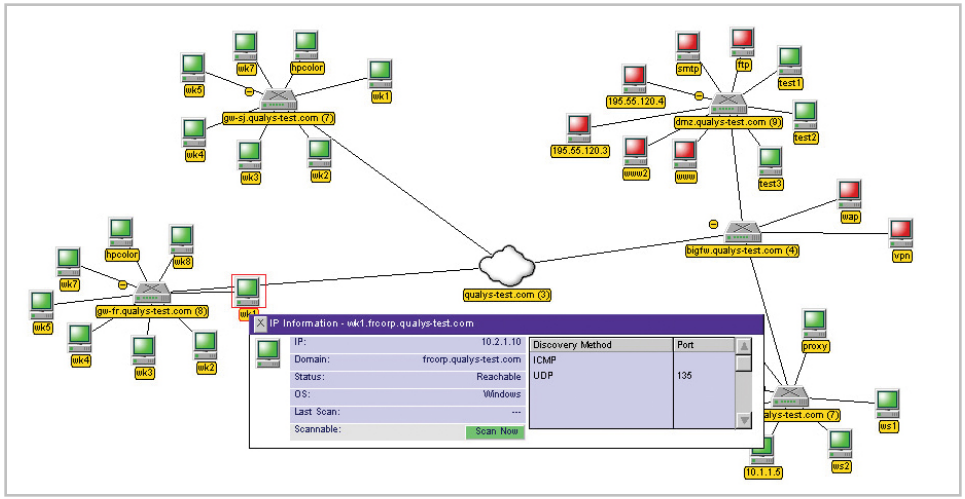


2. Vulnerability Management Process



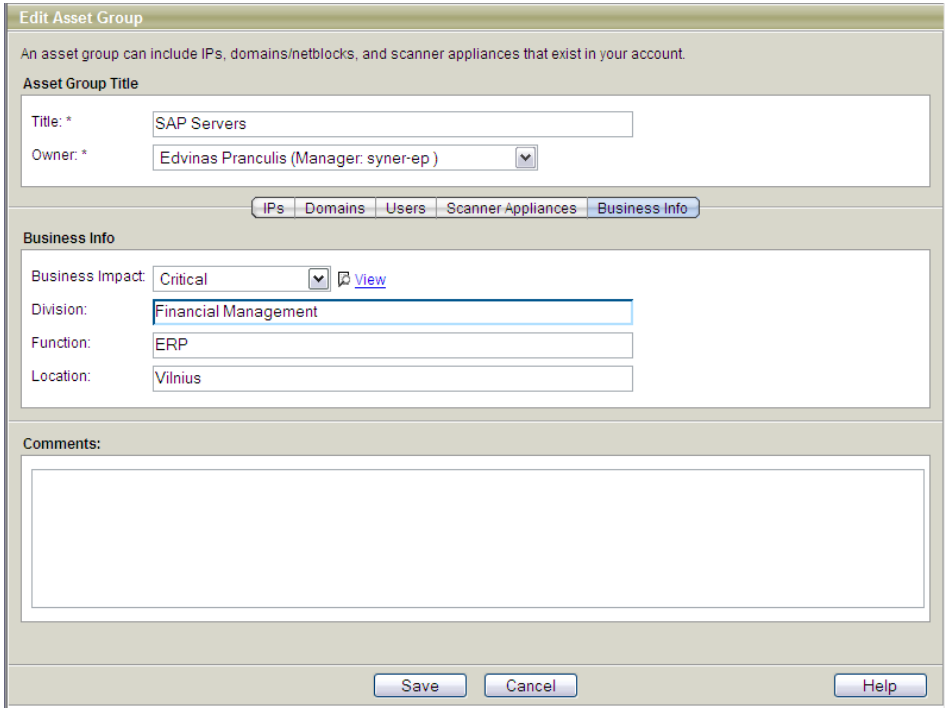
2.1 Discovery

- **Mapping**
  - Gives hacker's eye view of you network
  - Enables the detection of rogue devices (Shadow IT)



2.2 Asset Prioritisation

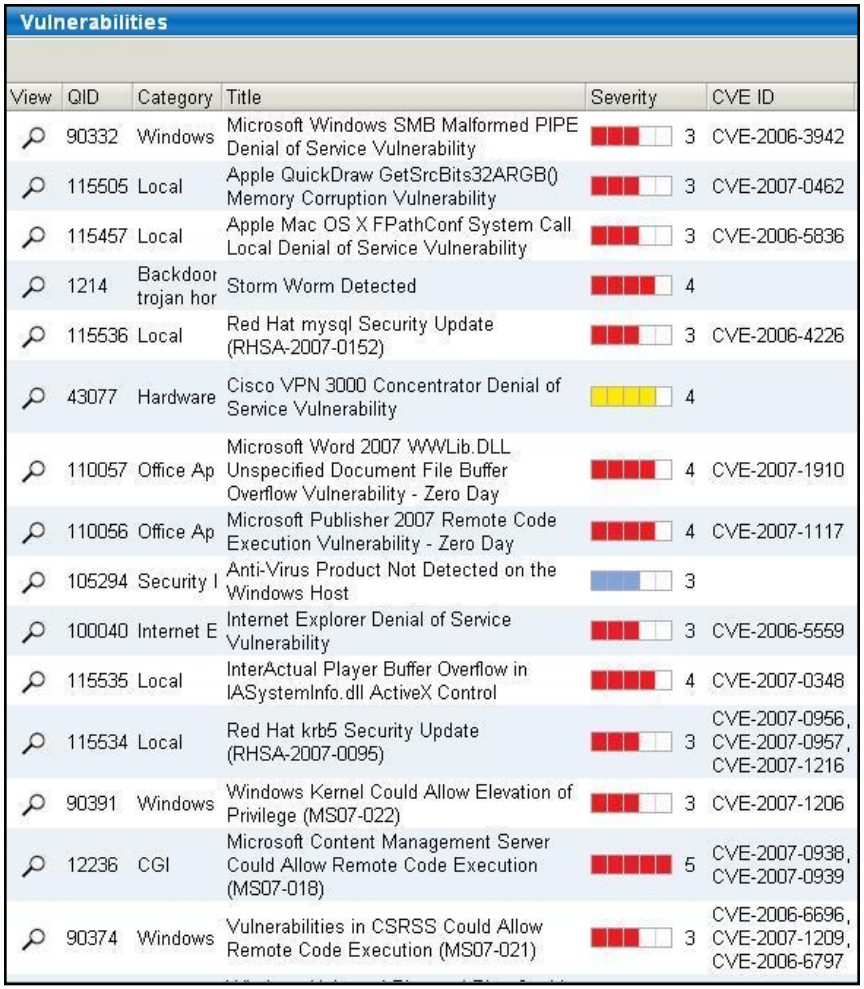
- **Asset Prioritisation**
  - Some assets are more critical to business then others
  - Criticality depends of business impact
- **Asset Allocation**
  - Each asset should have an owner



2.3 Assessment

- **Signature Classification**
  - Vulnerability Signatures
  - Application Fingerprints
  - Service Signatures
  - Device / OS Fingerprints
  - Configuration Signatures
  - Compliance Signatures

- **Timely Signatures**
  - 725+ Devices/OS
  - 250+ Remote Services
  - 5800+ Vulnerability Signatures
  - 950+ Vendors
  - 2000+ Products



Vulnerabilities

View	QID	Category	Title	Severity	CVE ID
	90332	Windows	Microsoft Windows SMB Malformed PIPE Denial of Service Vulnerability	3	CVE-2006-3942
	115505	Local	Apple QuickDraw GetSrcBits32ARGB() Memory Corruption Vulnerability	3	CVE-2007-0462
	115457	Local	Apple Mac OS X FPathConf System Call Local Denial of Service Vulnerability	3	CVE-2006-5836
	1214	Backdoor trojan hor	Storm Worm Detected	4	
	115536	Local	Red Hat mysql Security Update (RHSA-2007-0152)	3	CVE-2006-4226
	43077	Hardware	Cisco VPN 3000 Concentrator Denial of Service Vulnerability	4	
	110057	Office Ap	Microsoft Word 2007 WWLib.DLL Unspecified Document File Buffer Overflow Vulnerability - Zero Day	4	CVE-2007-1910
	110056	Office Ap	Microsoft Publisher 2007 Remote Code Execution Vulnerability - Zero Day	4	CVE-2007-1117
	105294	Security I	Anti-Virus Product Not Detected on the Windows Host	3	
	100040	Internet E	Internet Explorer Denial of Service Vulnerability	3	CVE-2006-5559
	115535	Local	InterActual Player Buffer Overflow in IASystemInfo.dll ActiveX Control	4	CVE-2007-0348
	115534	Local	Red Hat krb5 Security Update (RHSA-2007-0095)	3	CVE-2007-0956, CVE-2007-0957, CVE-2007-1216
	90391	Windows	Windows Kernel Could Allow Elevation of Privilege (MS07-022)	3	CVE-2007-1206
	12236	CGI	Microsoft Content Management Server Could Allow Remote Code Execution (MS07-018)	5	CVE-2007-0938, CVE-2007-0939
	90374	Windows	Vulnerabilities in CSRSS Could Allow Remote Code Execution (MS07-021)	3	CVE-2006-6696, CVE-2007-1209, CVE-2006-6797

Classified document, not allowed to distribute.

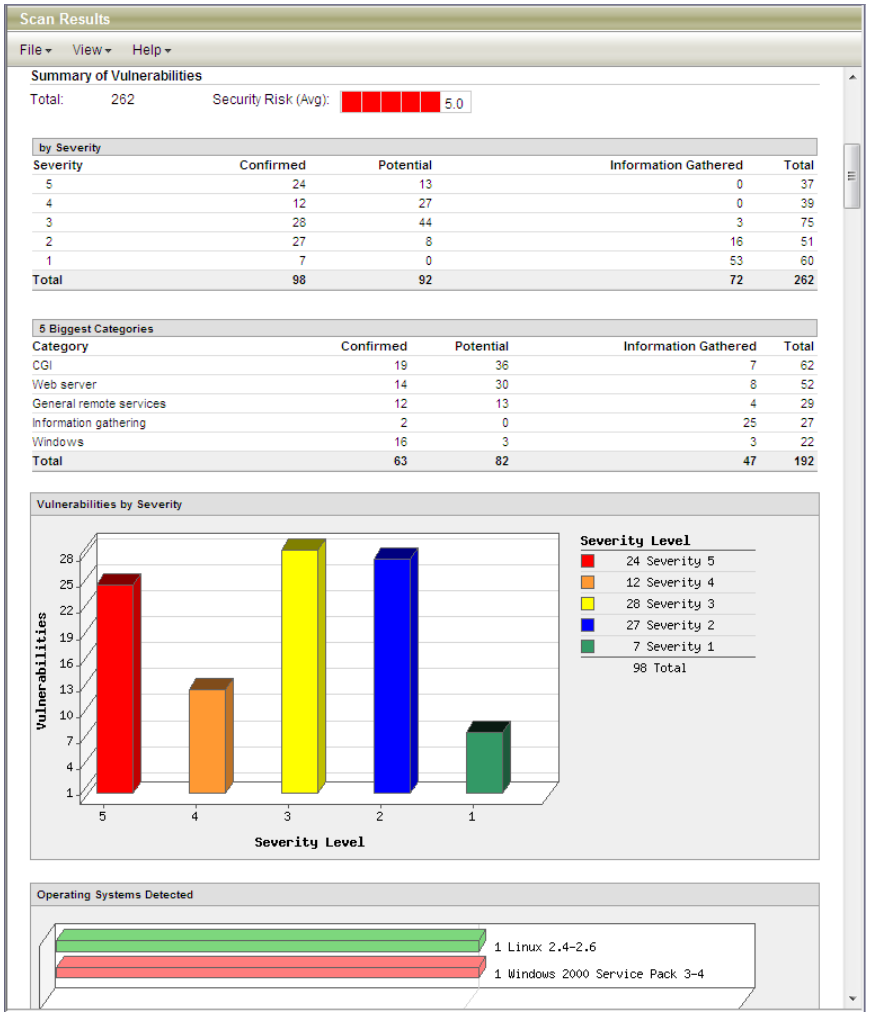
2.4 Scanning

- **Scanning:**
  - takes an “outside-in” and “inside-in” approach to security, emulating the attack route of a hacker
  - tests effectiveness of security policy and controls by examining network infrastructure for vulnerabilities
  - Provides tools for untrusted and authenticated scanning

“With this product, we gained the ability to automatically scan everything we own for vulnerabilities. And it provides us with a documentation path for all servers including best security practices, vulnerability ranking and patches.”

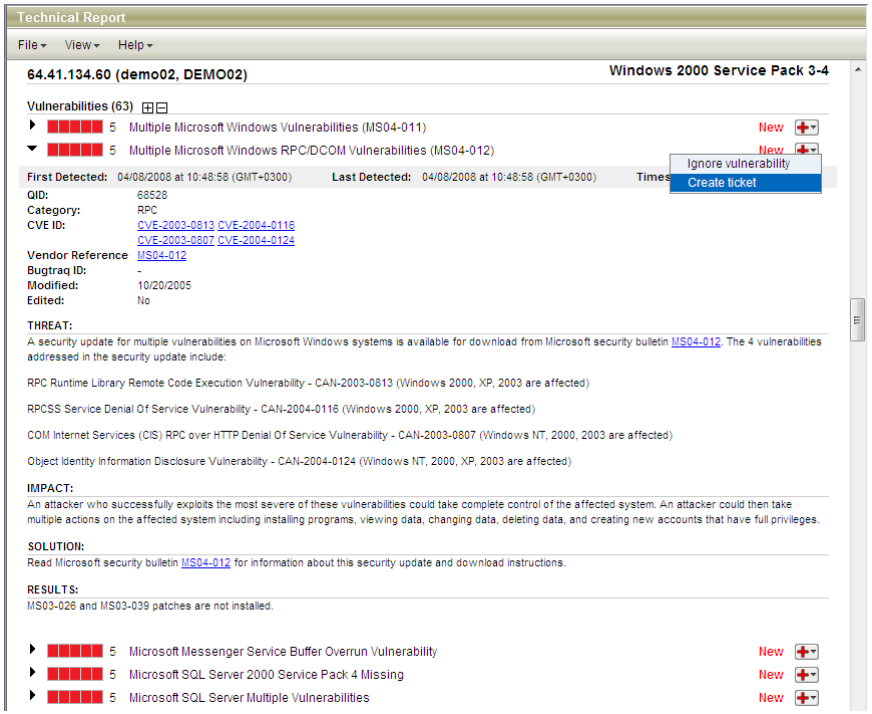
Bureau Chief, Strategic IT

Florida Department of Health

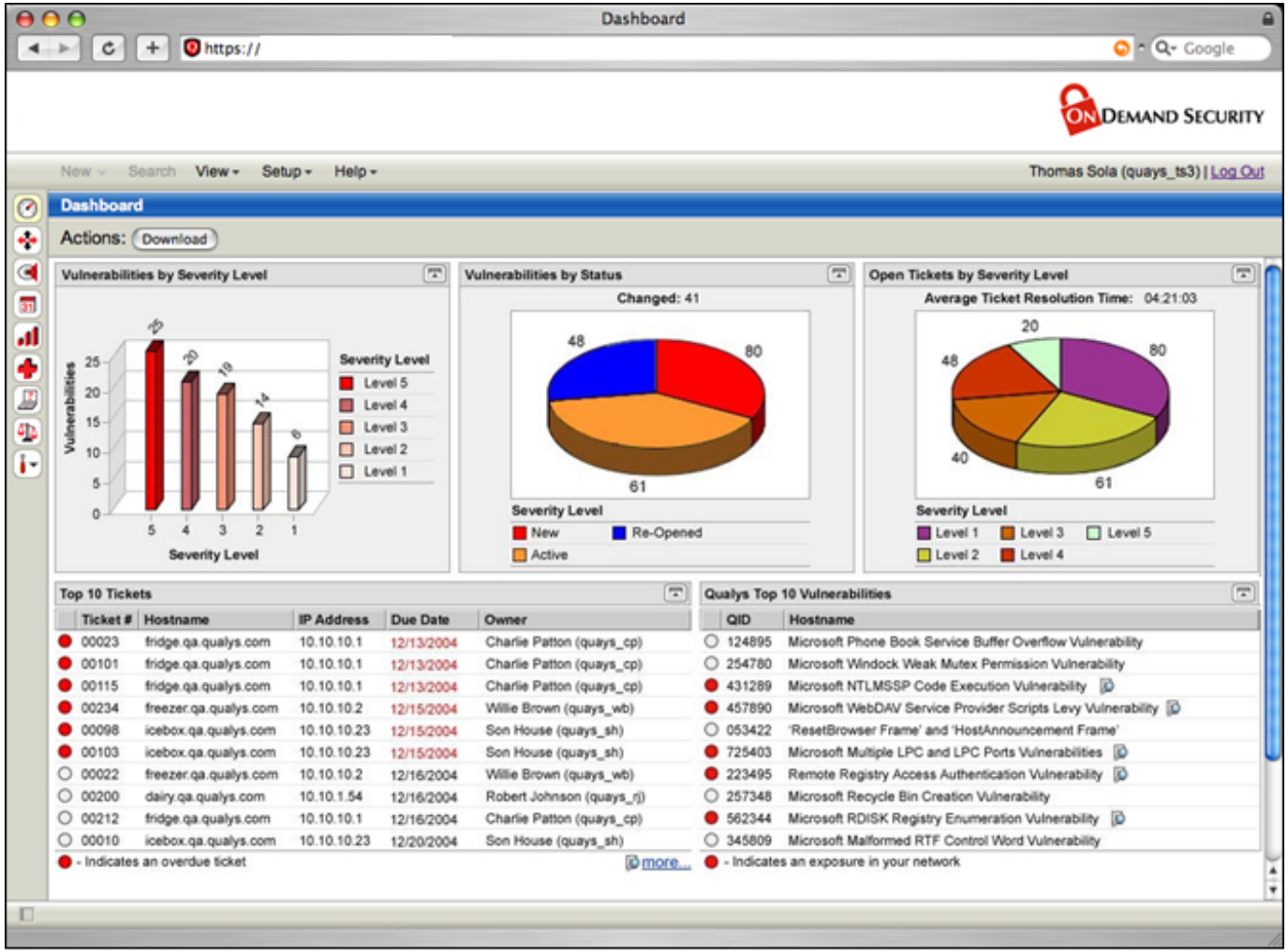


2.5 Reporting

- **Reporting:**
  - Allows for generation, storage and distribution of reports for large enterprise networks
  - E-mail notifications allow users to review reports upon completion
  - Reports can be generated for various compliance initiatives and security requirements:
    - Business Policy, **PCI, SOX, HIPAA, Basel II,** etc.
    - Security trend over a period of time
    - Business risk or CVSS scoring
    - Share reports with auditors, operation staff, security & network managers, executives



2.5 Reporting



2.5 Reporting

- **Reporting:**
  - Reporting by business units or asset groups
  - Security trend over time

"If you can't measure security, you can't manage it. Qualys lets me measure and manage my network security. Their reports demonstrate ongoing security improvement in working with IT suppliers."

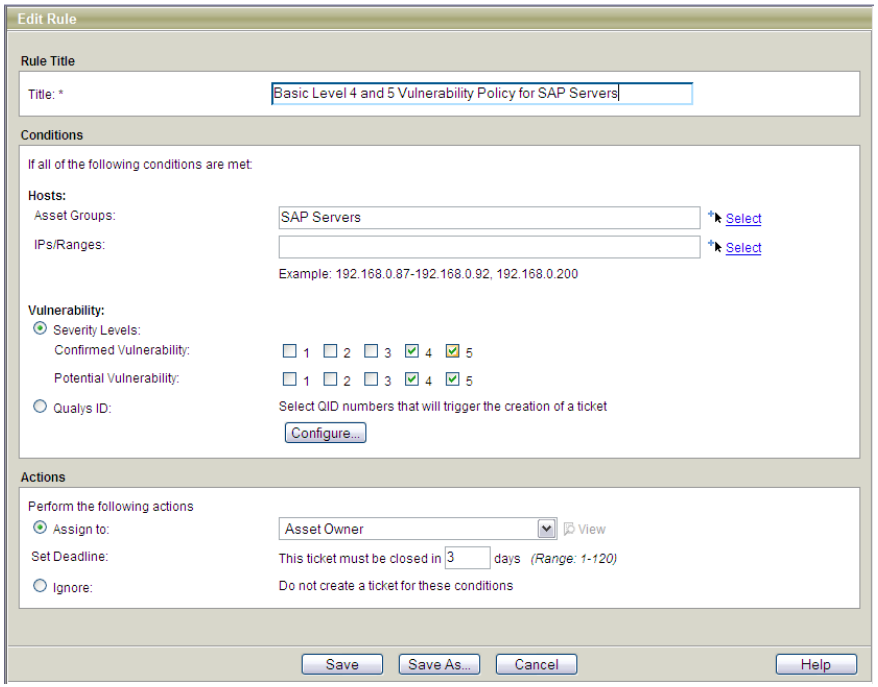
Director of Global Information Security
ICI

2.6 Remediation

- **Remediation**
  - Tickets are either generated automatically upon scan completion based on polices or on demand by users from any report
  - Trouble tickets capture complete audit trails and history of a vulnerabilities on hosts
  - QualysGuard scanners verifies the ticket after its closed
  - Integration with other helpdesk solutions is available through API

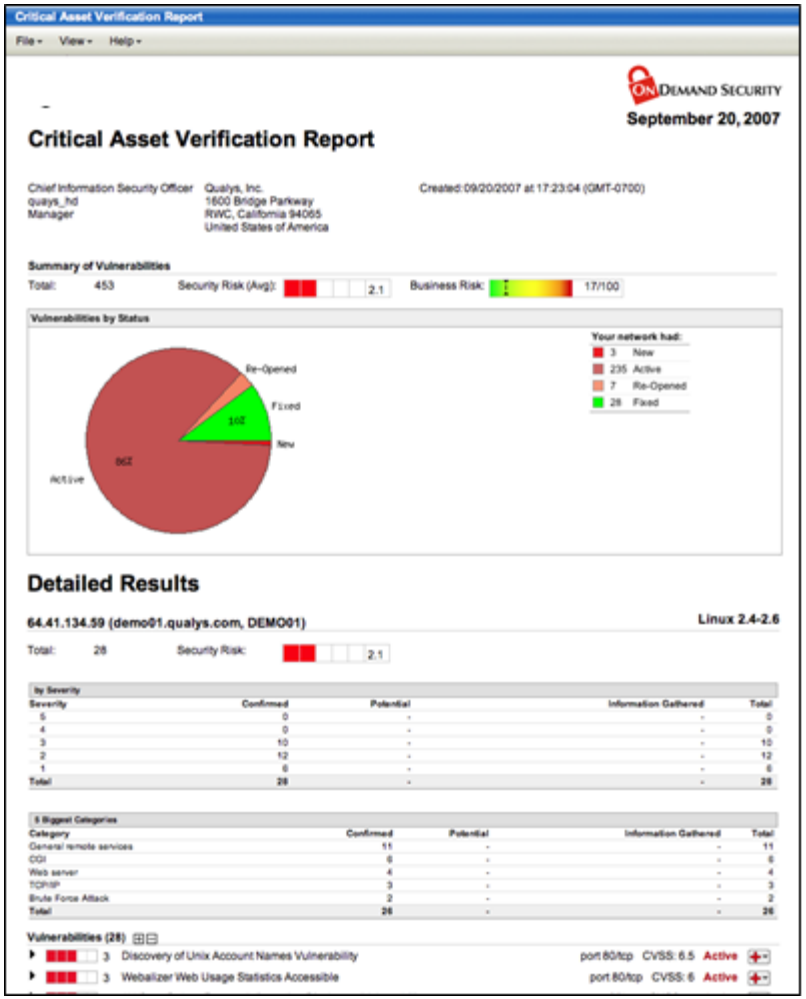
"In vulnerability management, it's all about response time. Qualys' remediation agent directly assigns tickets to fix things to my network technicians. The system then tracks those fixes."

Director of Enterprise Security
Wescorp



2.7 Verification

- **Re-scanning:**
  - Verifies applied patches and confirm compliance
  - Verifies the tickets after they are closed

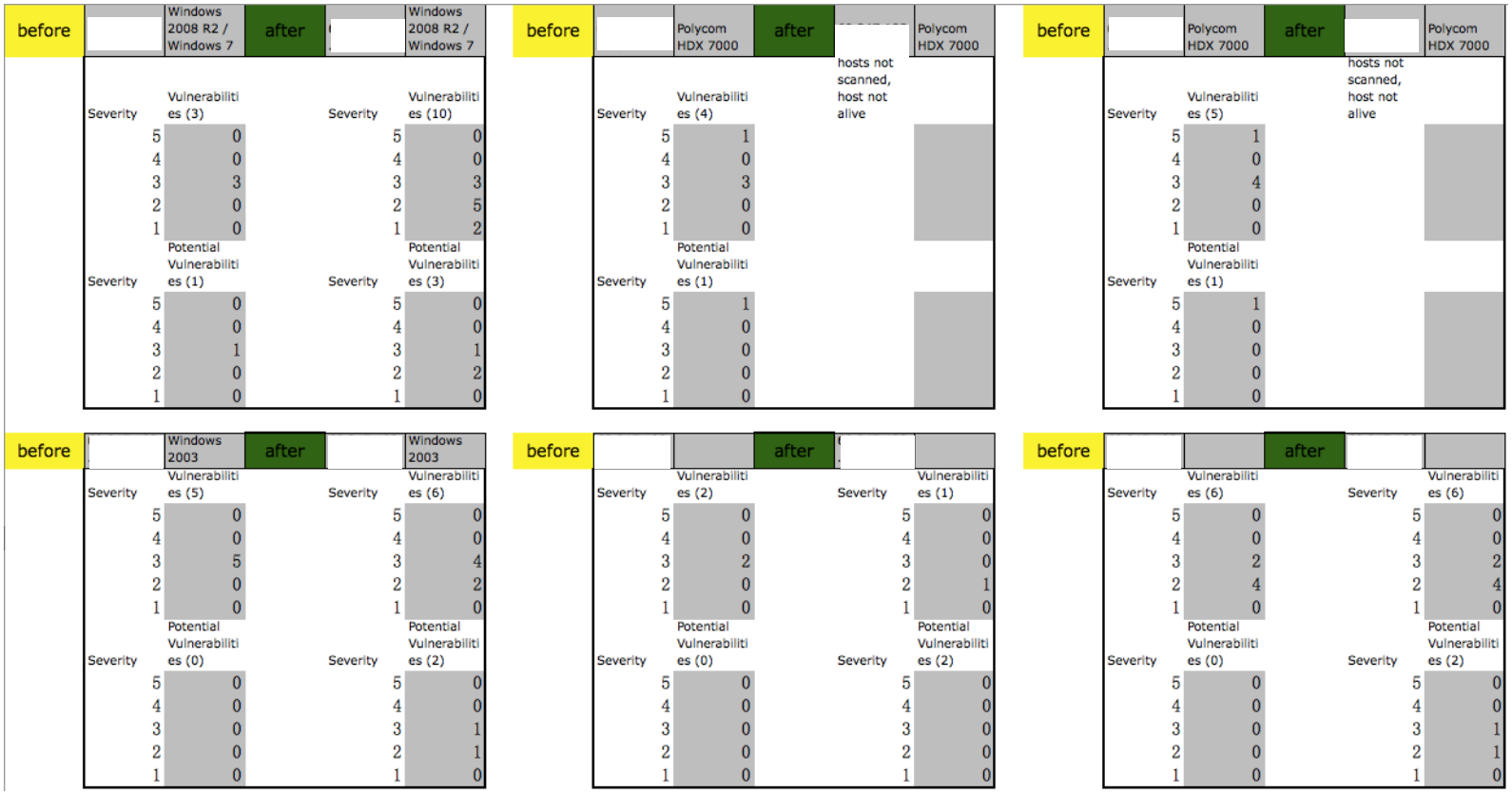


"Before QG we had an ad hoc process; QG brought much stronger control and visibility into our processes. QG gives us the ability to detect our vulnerabilities across our network and really ensure that we have the level of security and compliance we need."

Chief Information Protection Officer
CIGNA

2.8 Remedy Service

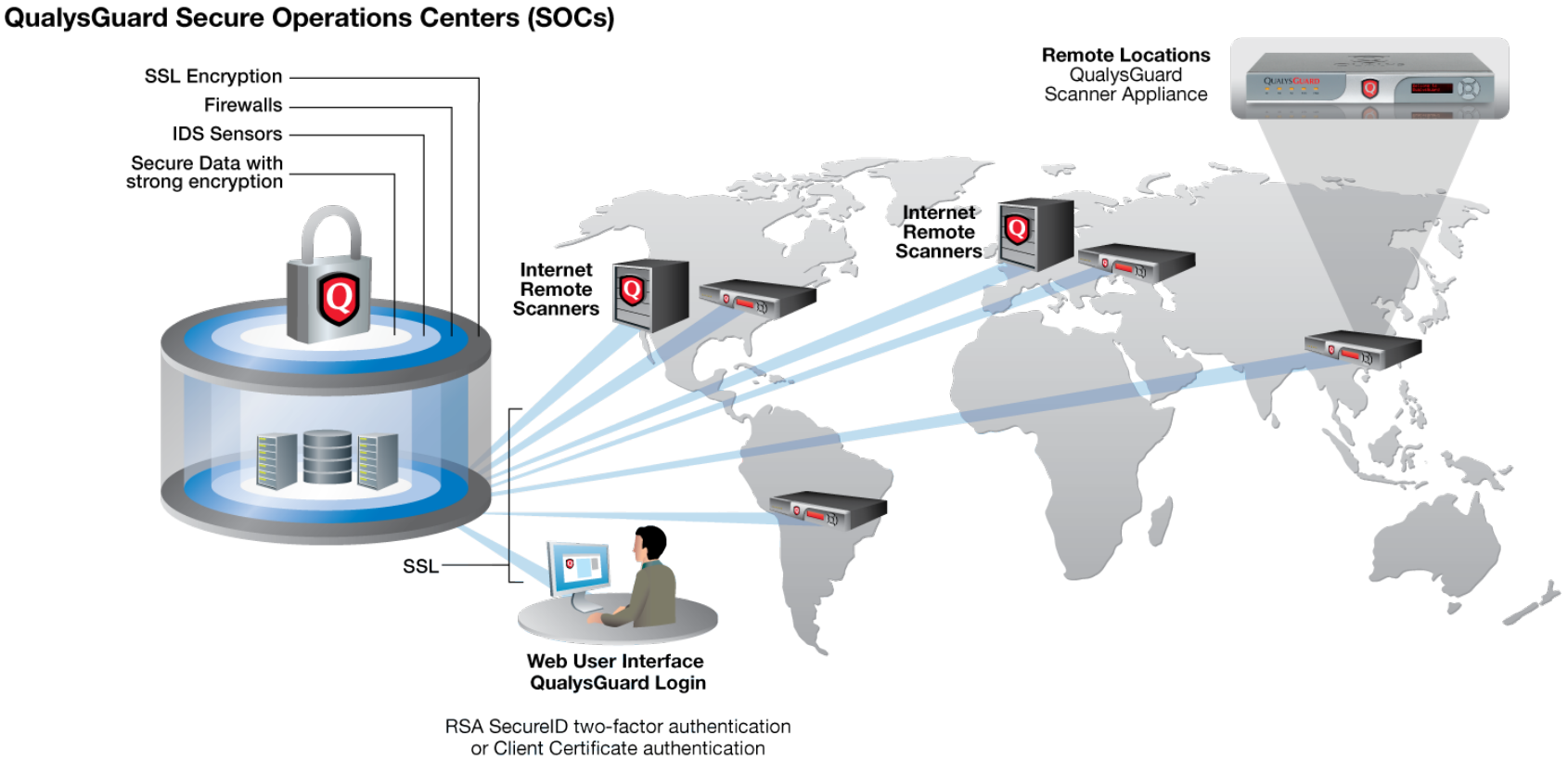
- **Before & After**
  - **Network Facilities**
  - **Host Servers**
  - **Firewall Policies**
  - **Virtualization Environment**



3. Benefits of Vulnerability Management

- **Vulnerability management gives you control and visibility to manage your networks security effectively and document compliance**
- **Vulnerability management is PROACTIVE approach to security**

3.1 QualysGuard (SaaS mode)



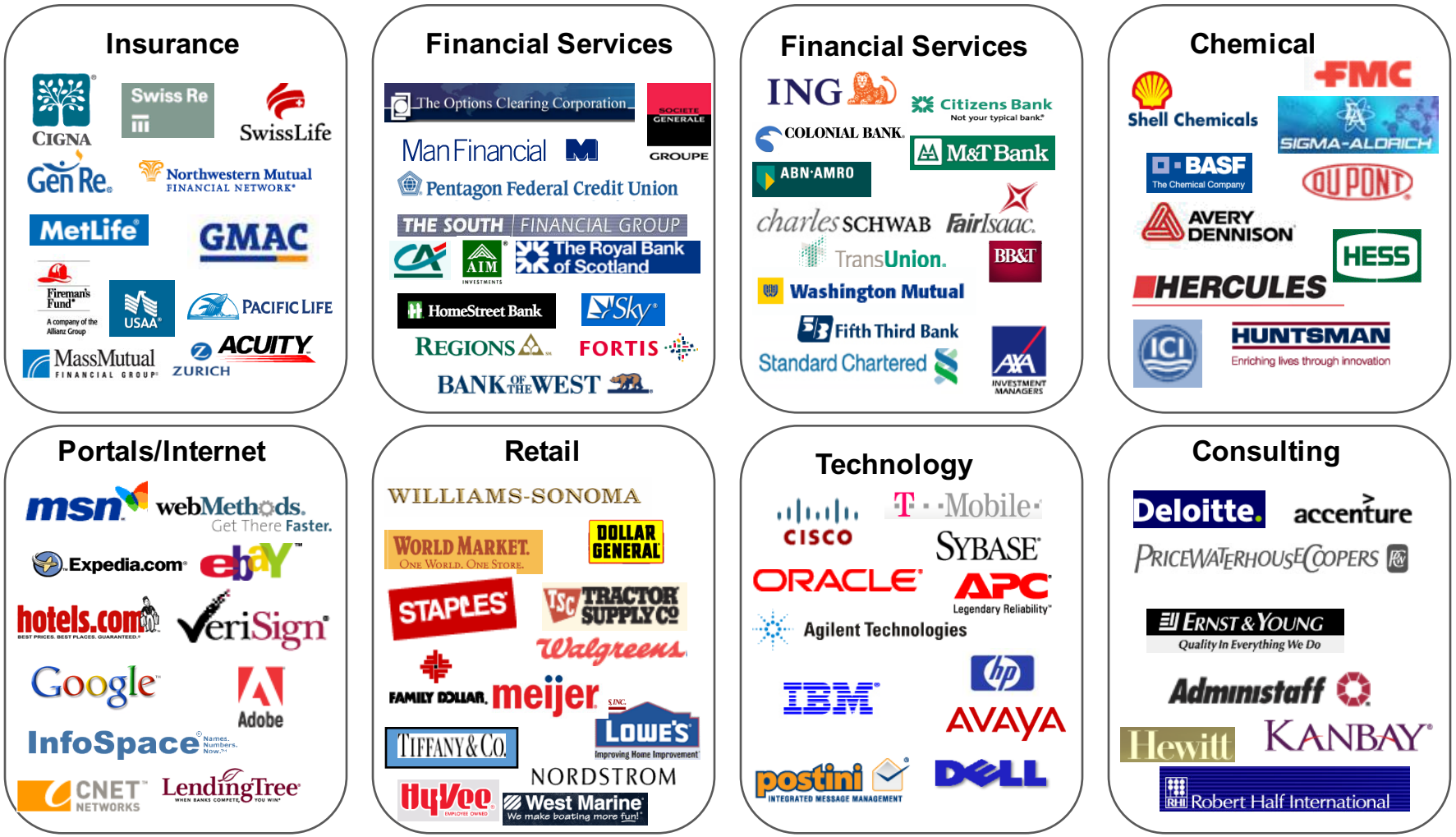
Deployability
- 6 000+ Appliances Deployed in >65 Countries
- Largest Single Enterprise Deployment: 223 Appliances in 52 Countries

Scalability
- 200+ Million IP Audits Per Year

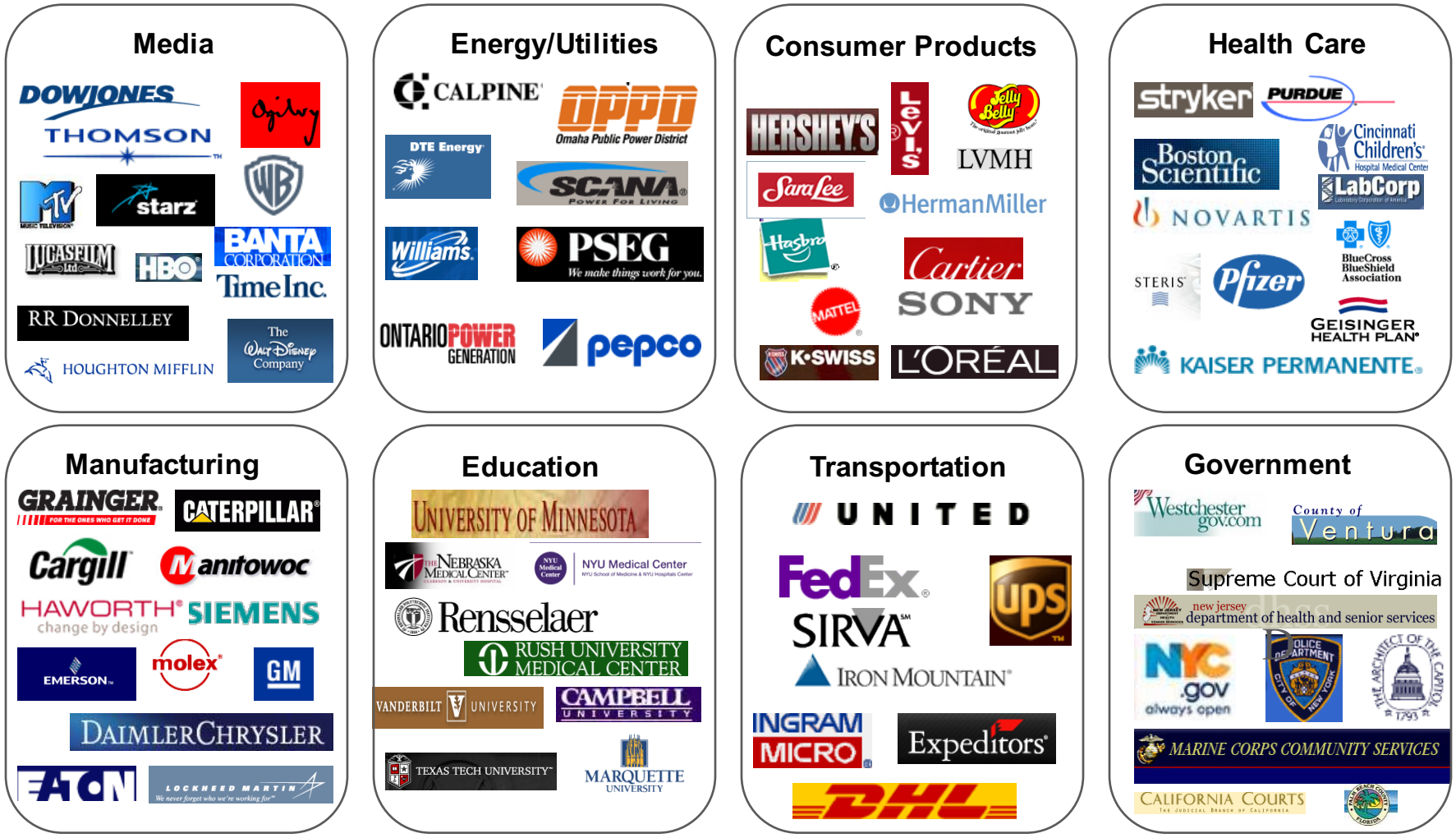
Reliability
- Six Sigma (99.99966%) Accuracy: <3.4 Defects per 1 Million Scans

Classified document, not allowed to distribute.

3.2 Case Study by Industries



3.2 Case Study by Industries



4. Summary

- **The Benefits of BROTIGHT Vulnerability Management Service & QualysGuard Platform:**
  - Gives you control and visibility to manage your networks security risks effectively and document compliance
  - Automates most elements of Vulnerability Management in an efficient, cost-effective manner
  - Enables you to cut your vulnerability management expenses by 50-90% when compared to traditional enterprise-software VM solutions
  - With BROTIGHT professional service, you could reduce the risk of IT infrastructure via periodicity site/cloud service and keep your infrastructure running on manageable risk control.

Classified document, not allowed to distribute.

Classified document, not allowed to distribute.