QUALYS®

Sicherheitsaspekte im Betrieb eines "Software as a Service" Systems – Beispiel QualysGuard

Wolfgang Kandek

CTO - Qualys, Inc

Frankfurt, 20. November 2009

ON DEMAND SECURITY

Our Understanding of Cloud Computing

- IaaS, PaaS, SaaS
- Better Performance in the service's area of competence enabling you to focus on core areas
  - AWS – elasticity, availability
  - AppEngine, Sforce, Azure – foundation, robustness
  - Salesforce – functionality, accessibility, scalability
- Qualys
  - Updated Vulnerabilities, Catalog of Policy Checks, Comprehensiveness of Web Application Checks, Reporting
  - Uptime
  - Ability to scan/evaluate large number of Devices

Trust

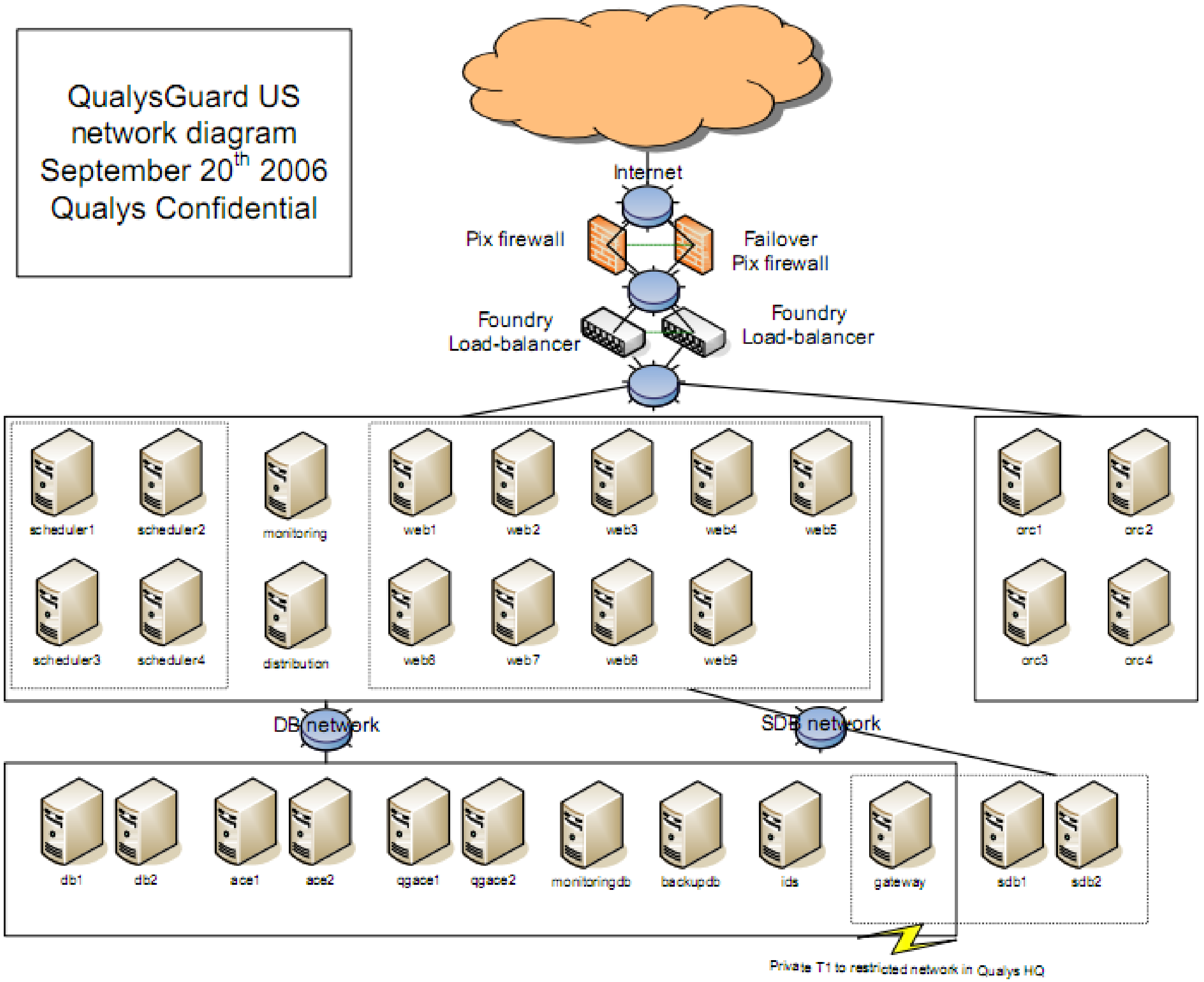
- Confidence that a service will get executed to the expected degree and under certain conditions
- Phone Lines – Availability and Privacy
- Data lines – Availability and Privacy
- Software
  - Operating System
  - Communication software
  - Compiler
  - Anti Virus Software

Gaining Trust

- Transparency in our setup and operations

Gaining Trust – Transparency

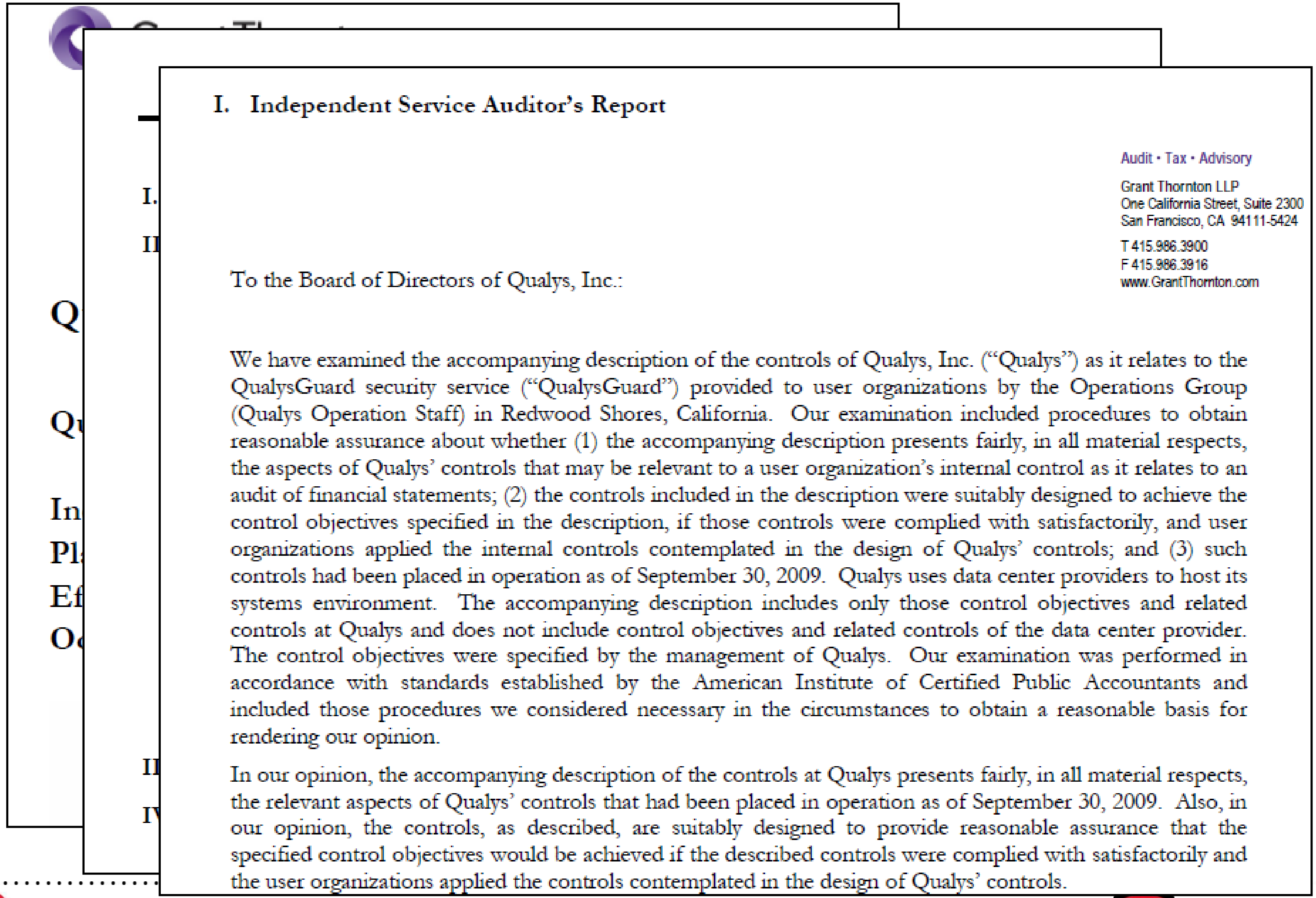
QualysGuard US
network diagram
September 20th 2006
Qualys Confidential



Gaining Trust

- Transparency in our setup and operations
- External certifications
  - SAS70 Type II for last 4 years

Gaining Trust – Certifications



I. Independent Service Auditor's Report

Audit • Tax • Advisory

Grant Thornton LLP
One California Street, Suite 2300
San Francisco, CA 94111-5424

T 415.986.3900
F 415.986.3916
www.GrantThornton.com

To the Board of Directors of Qualys, Inc.:

We have examined the accompanying description of the controls of Qualys, Inc. ("Qualys") as it relates to the QualysGuard security service ("QualysGuard") provided to user organizations by the Operations Group (Qualys Operation Staff) in Redwood Shores, California. Our examination included procedures to obtain reasonable assurance about whether (1) the accompanying description presents fairly, in all material respects, the aspects of Qualys' controls that may be relevant to a user organization's internal control as it relates to an audit of financial statements; (2) the controls included in the description were suitably designed to achieve the control objectives specified in the description, if those controls were complied with satisfactorily, and user organizations applied the internal controls contemplated in the design of Qualys' controls; and (3) such controls had been placed in operation as of September 30, 2009. Qualys uses data center providers to host its systems environment. The accompanying description includes only those control objectives and related controls at Qualys and does not include control objectives and related controls of the data center provider. The control objectives were specified by the management of Qualys. Our examination was performed in accordance with standards established by the American Institute of Certified Public Accountants and included those procedures we considered necessary in the circumstances to obtain a reasonable basis for rendering our opinion.

In our opinion, the accompanying description of the controls at Qualys presents fairly, in all material respects, the relevant aspects of Qualys' controls that had been placed in operation as of September 30, 2009. Also, in our opinion, the controls, as described, are suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls were complied with satisfactorily and the user organizations applied the controls contemplated in the design of Qualys' controls.

Gaining Trust

- Transparency in our setup and operations
- External certifications
    - SAS70 Type II
    - ISO 2700x under evaluation
- Openness to Customer Audits

Gaining Trust – Customer Audits

ACME®

Qualys Discussion Questions

Acme – Internal Audit Autumn 2009

Detailed Questions:

1. Where are the Secure Operations Centers located that store Acme credentials (please include all onshore and offshore locations)?
2. Who has access to Acme credentials (please include all onshore\offshore employees, third parties, vendors and consultants)?
3. Who manages and has access to the encryption keys that encrypt Acme credentials?
4. When the credentials are used to perform a scan, how long are the credentials cached in any system? Are the cached credentials purged?
5. As noted in the QualysGuard Architecture and Data Security Overview, where is user information, account information, registered IP's, registered domains, assets groups, scan profiles, activity logs and global "anonymized" vulnerability statistics stored (in plain text)? And who has access to this information?
6. Who has access to the vulnerability database (please include all onshore\offshore employees, third parties, vendors and consultants)? Where is the vulnerability database located (please include all onshore and offshore locations)? What type of data is stored in the vulnerability database?
7. Is any Acme information (credentials, IP addresses, vulnerability DB's) stored offsite on backup tapes?
8. Who performs your annual SAS 70 audit? Does the scope of the audit explicitly include where Acme credentials are stored and utilized?

General Topics Related to:

- Information Security Policy
- Physical Security
- Human Resource Procedures (on boarding and off boarding)
- Incident Response Policy and Procedures

Gaining Trust – Customer Audits

How does Qualys prevent or identify software updates from occurring that are malicious in nature or not intended?

All automated software updates made available for download by the Scanner Appliance are rigorously tested in comprehensive Quality Assurance processes. Erroneous, malicious or unintended software updates should be detected at this stage before being released into the production environment where the Scanner Appliance would automatically download and apply the updates.

Qualys have defined procedures for troubleshooting anomalies when a Scanner Appliance is placed in Debug Mode. All activity conducted by Qulays Technical Support or Operations staff is monitored within an audit trail which is regularly reviewed. Appropriate action is taken if deviance is noted from standard procedures.

How does Qualys monitor if an exception has occurred?

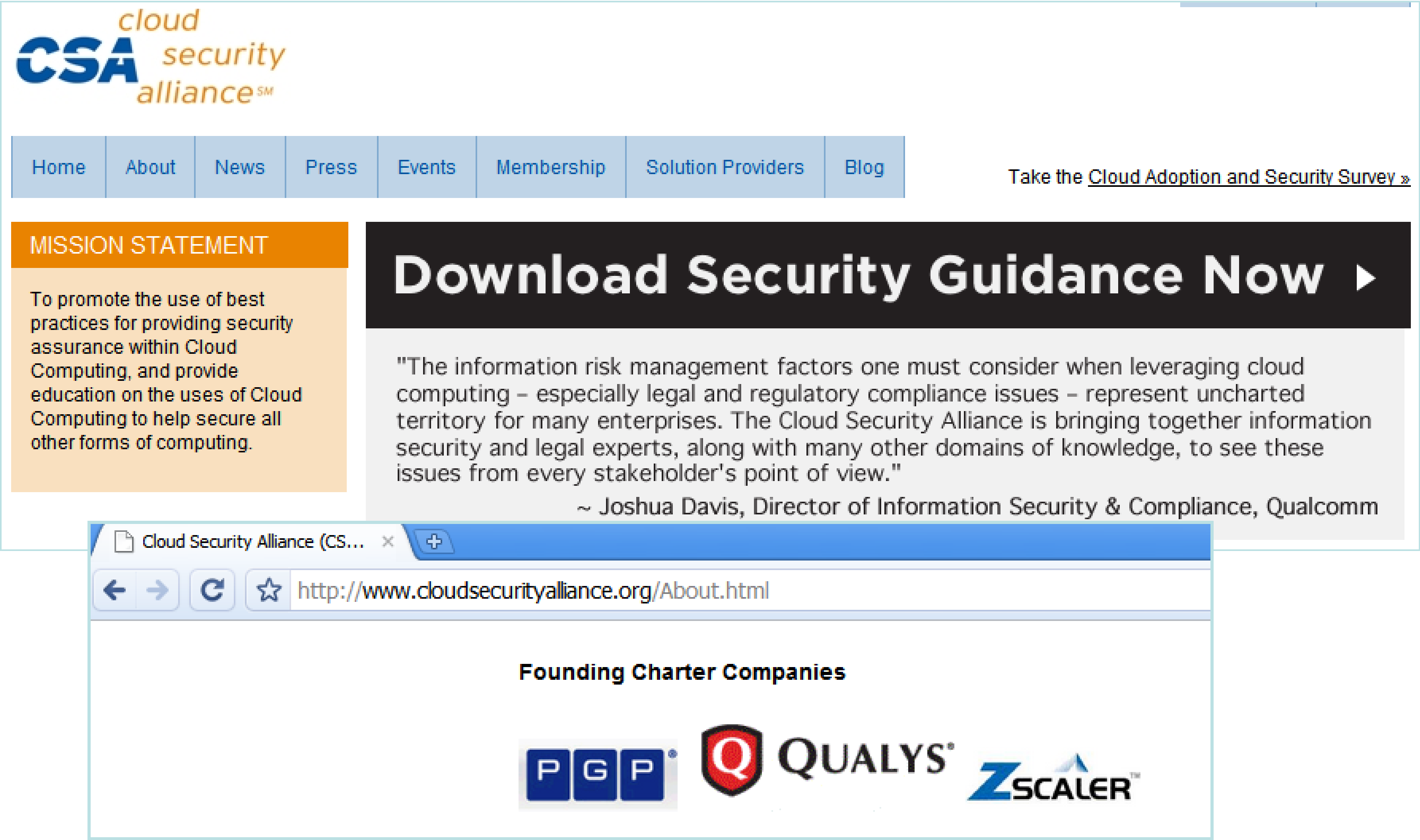
Qualys Operations Team has a daily process to review all Scanner Appliances operating within a Debug Mode. Any Scanner Appliance found to be in Debug Mode without valid approval will be investigated. In the event of a Scanner Appliance being in Debug Mode without the necessary approval, the end user is notified and appropriate steps will be taken.

In addition, a daily process of audit trail review is made to identify Scanner Appliances which have been placed in Debug Mode and are returned to normal operations. Any results are correlated with approval records and exceptions are dealt with accordingly.

Gaining Trust

- Transparency in our setup and operations
- External certifications
  - SAS70 Type II
  - ISO 2700x under evaluation
- Openness to Customer Audits
- Thought leader in the SaaS Security market
  - Cloud Security Alliance

Gaining Trust



Take the Cloud Adoption and Security Survey »

MISSION STATEMENT

To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.

"The information risk management factors one must consider when leveraging cloud computing – especially legal and regulatory compliance issues – represent uncharted territory for many enterprises. The Cloud Security Alliance is bringing together information security and legal experts, along with many other domains of knowledge, to see these issues from every stakeholder's point of view."

~ Joshua Davis, Director of Information Security & Compliance, Qualcomm

Cloud Security Alliance (CS...
http://www.cloudsecurityalliance.org/About.html

Founding Charter Companies

Security – Secure Design

- Engineering Team Leads specialized in Security
  - All Engineers Background checked
- Security Architecture
  - Multi tenant architecture
  - Data isolation between customers using encryption and database mechanisms
- Security Features
  - Access Control
    - 2-factor authentication - SecurId, Client certificates, VeriSign VIP
  - Role based access levels for Users
  - PDF encryption/signing for outside data sharing

Security – Secure Design

- Structured Software Development Lifecycle
  - Best practices
    - Examples: Input sanitation, prepared SQL statements, CSRF
  - Automated build system
    - Source Code Control System
    - Hourly and Daily builds
    - Automatic static source code checking
    - Integrated bug tracking system
    - Automatic acceptance testing
- Engineering and Operations are separate Organizations
    - No Engineering access in Production
    - No Production data in Development and QA

Security - Operations

- Dedicated Team of Specialists
  - Background checked
  - System and Database Administration
  - Network and Security Engineering
- Management Architecture
  - Individual user accounts
  - 2-factor authentication
  - Monitoring systems
  - 10+ platforms

Security – Operations - Physical

- Datacenters
  - Outsourced – Tier 4 TIA- 942
  - Independent security Certifications
    - US – SAS 70 Type II
    - Europe – ISO 27001
- Office
  - Separated with biometric authentication
  - Dedicated Management Network
  - Thin client Management Stations
    - Air Gap from normal workstations
      - All data transfers logged
    - 2-factor authentication with Smartcards

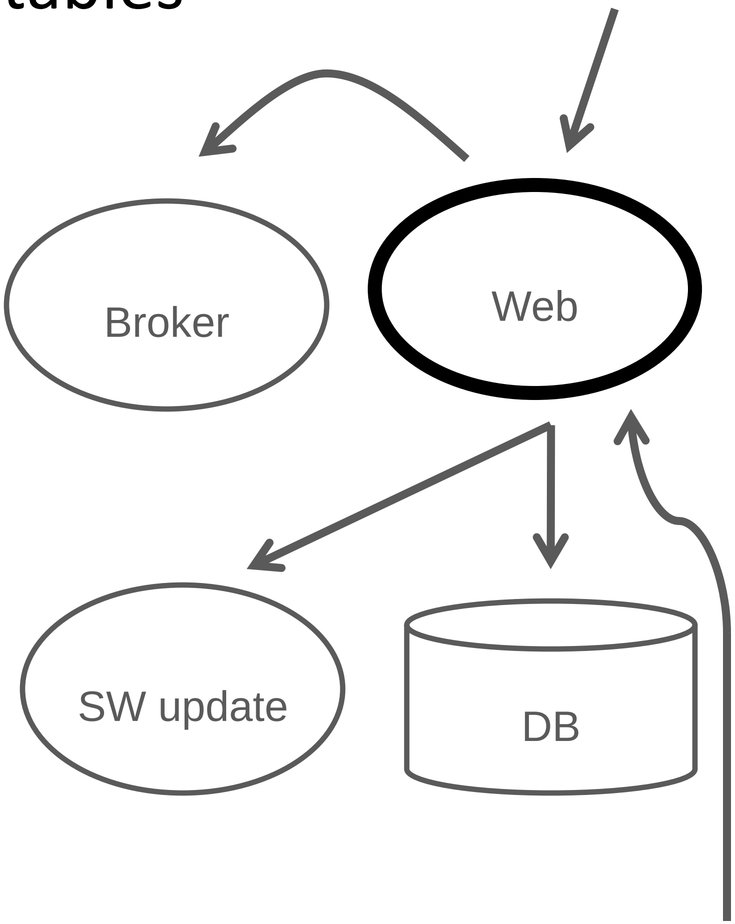
Security – Operating System Level

- Core Operating System
  - Linux
  - Red Hat Linux – Support
  - Expertise
- Hardening
  - Minimal installation
  - Host Firewalling – ingress, egress
  - SELinux
  - Minimal Access Rights and strong authentication
    - Dedicated user accounts, sudo and key based authentication

Security – Operating System Level

- Strict local stateful Firewalls – iptables

1. Deny all incoming and outgoing
2. Allow incoming HTTPS
3. Allow outgoing to Scan Broker
4. Allow outgoing to DB
5. Allow HTTPS to SW update server
6. Allow incoming SSH from Management server



Security – Web Server Level

- Web Server Software Version
  - Apache and SSL
  - PHP with hardening extensions
- Web Server Configuration
  - Content owner user <> Web Server user
  - SELinux policies in enforcing mode
- PHP application code
  - Encoded, no source
  - Configuration files in separate package under Operations control

Security – Database Level

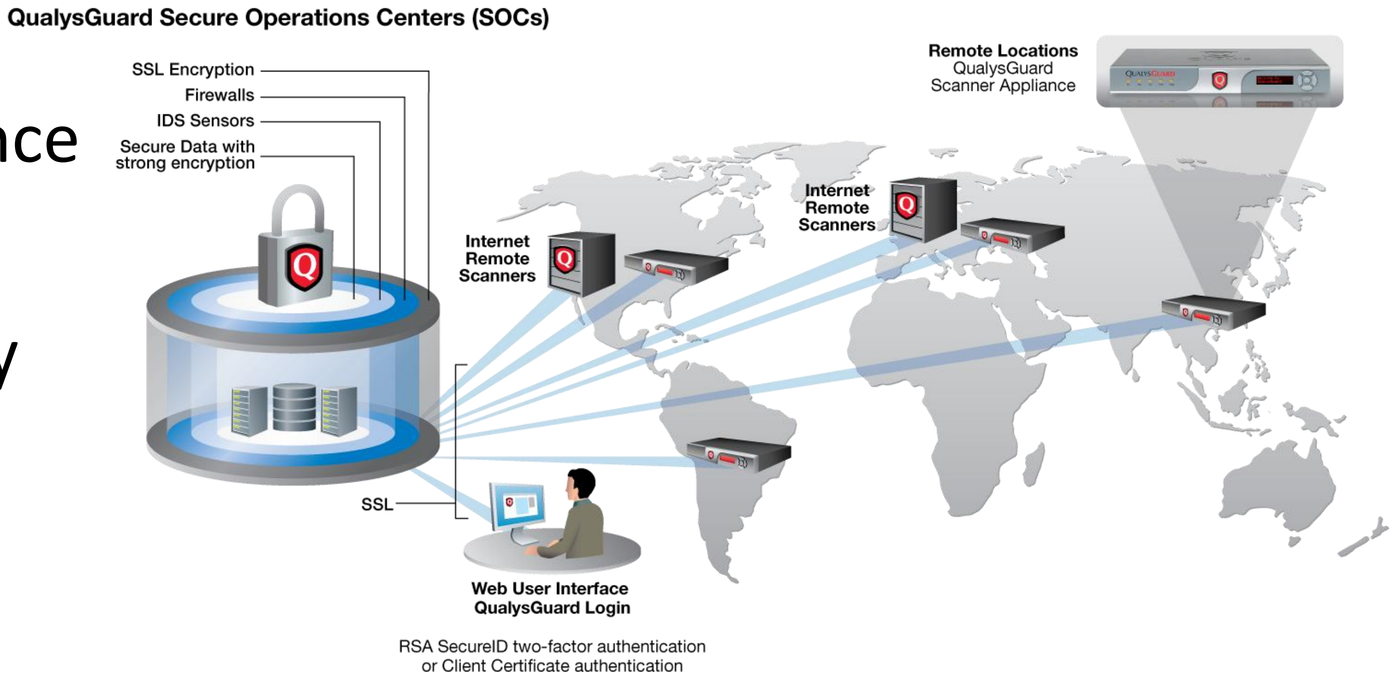
- Database Software Version - Oracle 10g
- Database Configuration
  - Minimal installation
    - Components
    - Package access
  - Schema owner <> Application user
    - Multiple Application Users with different access rights
- Use of Virtual Private DB and Encryption
- Prepared and Dynamic SQL monitoring

Security – Network Level

- Routers with BGP
  - Qualys IP space
- Network Firewalls – Cisco ASA
- Switches with VLANs - Cisco
- VeriSign SSL certificates
  - SSL Termination at the server
- Snort IDS Systems
- Centralized logging
  - Syslog, Open Source Alerting
  - Splunk

Qualys Infrastructure

- Performance
- Reliability
- Availability
- Scalability
- Security



Thank you

wkandek@qualys.com