QUALYS®

Ensuring security for an enterprise cloud-based managed security service

Wolfgang Kandek
CTO - Qualys, Inc

Open Group Conference – San Diego – February 4, 2009

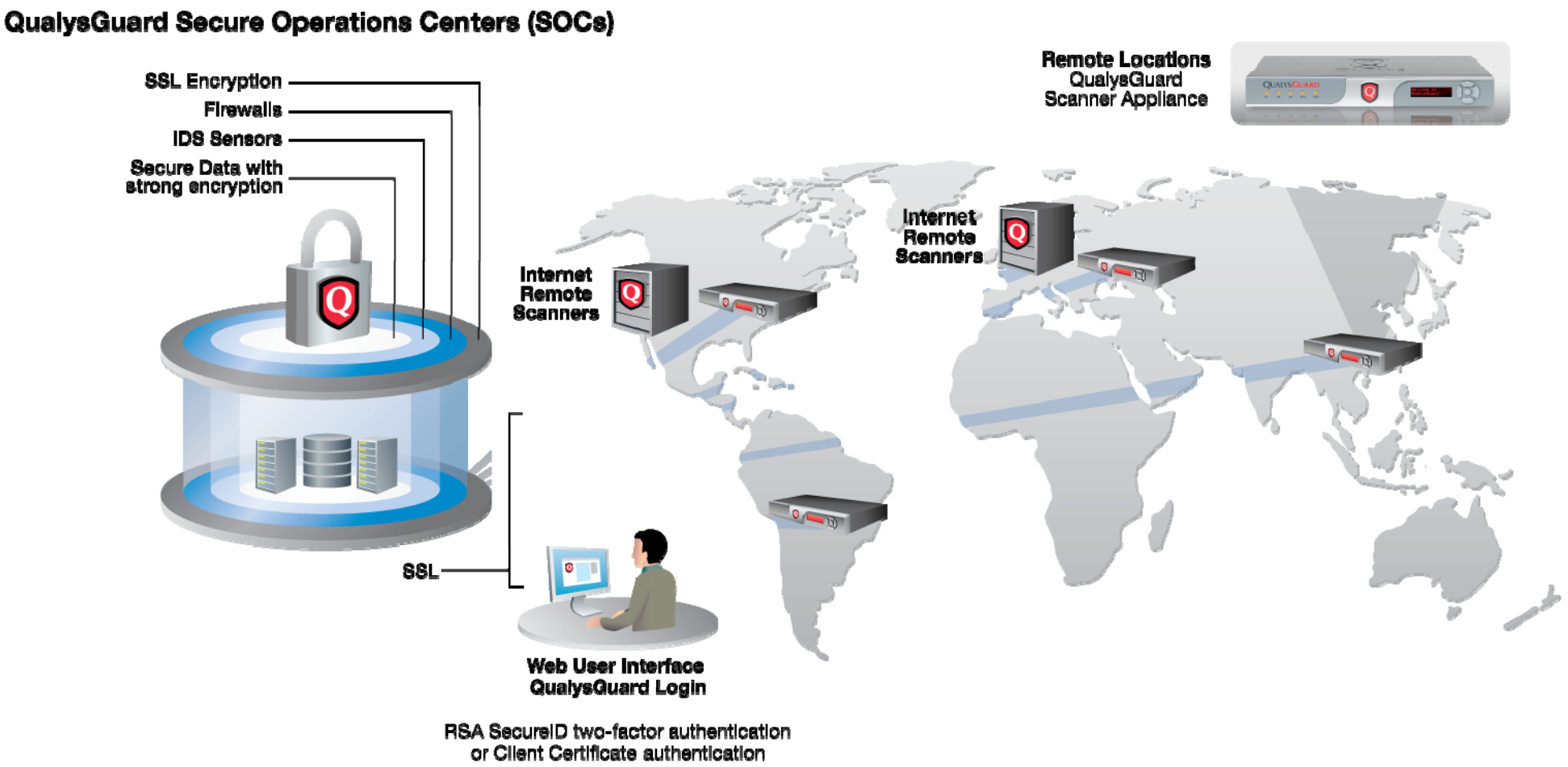
ON DEMAND SECURITY

Qualys

- Software as a Service in the Security Space
- Founded 1999
- 3,500 customers – 50,000 users
  - 35 % of Fortune 100, 20 % of Fortune 1000
- 100 Million+ IPs scanned
- 200+ employees, 100+ in engineering
- Services
  - Vulnerability Management
  - Policy Compliance
  - Web Application Scanning
  - PCI

  - Scanning
  - Data Management and Workflow

QualysGuard Infrastructure



Why Qualys ?

- Need for Vulnerability Management, Policy Compliance and Web Application Scanning
  - Security
  - Regulatory
- Data Quality
  - Vulnerability and Control Catalog
  - False Positive rate (Saas advantage)
- Simple to deploy

- Barriers: Data Storage - Trust

Gaining Trust - Architecture

- System purpose built for one application - QualysGuard
- Single standard Operating System and software stack
  - Linux 2.6 – RedHat based hardened/minimal
  - SELinux
  - Apache hardened/minimal
  - PHP with Security patches
  - Host based firewall ingress/egress
  - Integrity checking
- Data encrypted at rest and in transit
  - AES and SSLv3
- Single-Sign On and Full REST API
- Structured development process with clear handoffs

Gaining Trust - Architecture

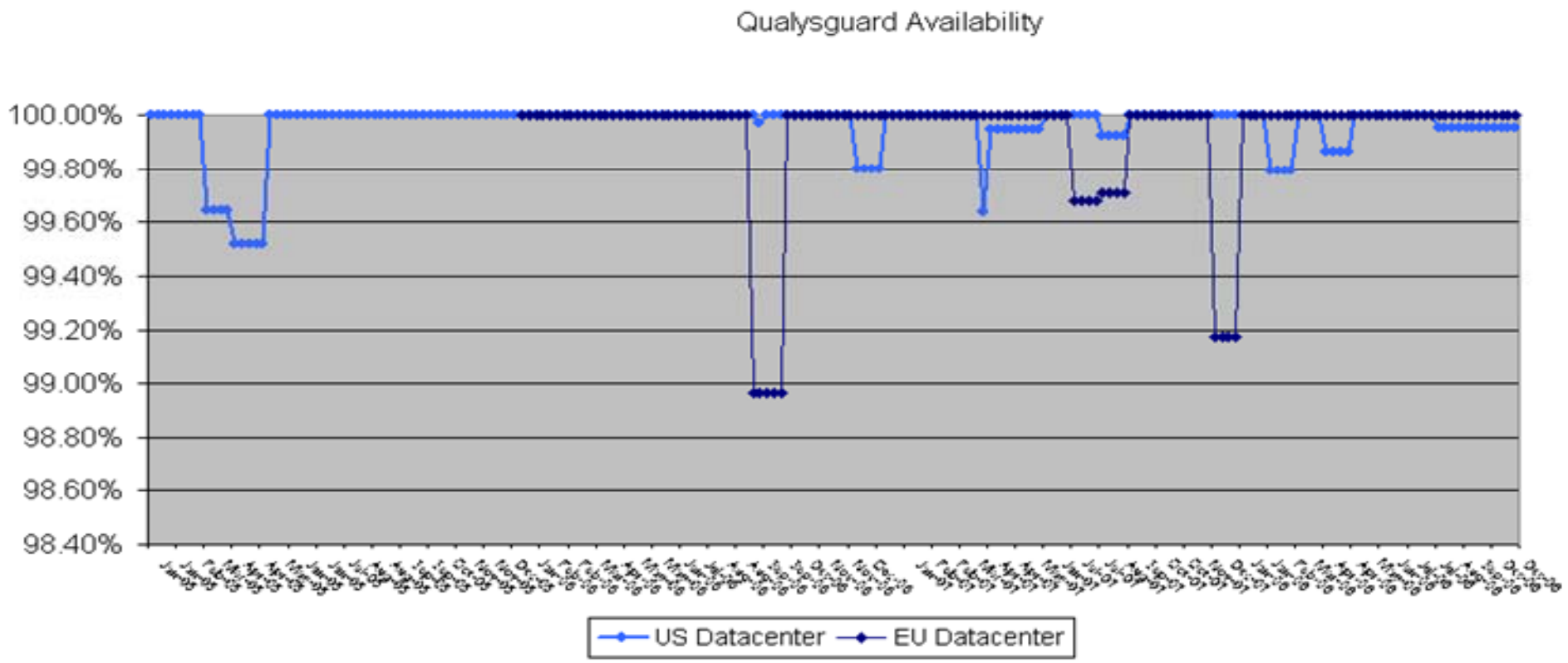
- Dedicated QualysGuard Operations team
  - System Administrators, DBAs, Security Engineers (15)
- String Access Control:
  - Separate physical area for Operations
  - Separate physical network for Operations
  - Stateless workstations for access – Sun SunRay
  - SmartCards and username/password, escalation through sudo
  - Centralized logging of all actions
- Enterprise-grade networking equipment and firewalls
  - Ingress/egress
- Automated build and deployment system
  - Development, QA, staging, production

Gaining Trust - Transparency

- Explain Architecture
- External Security Audit
  - SAS70 Type II
  - Source Code Review
- Hosting center with Security Audit (SAS70 Type II/ISO)
- Publish Uptime statistics
- Publish False Positive data
- Open to customer audits
  - 1-2 a quarter, discuss suggestions
- Continuous improvement in Operations and Engineering

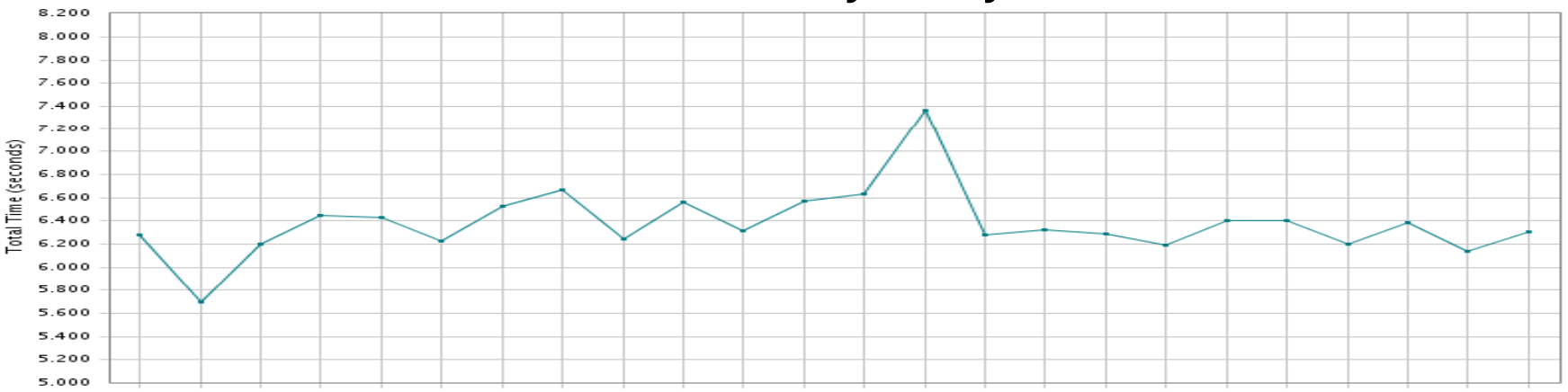
Gaining Trust - Transparency

QualysGuard – Internal Availability

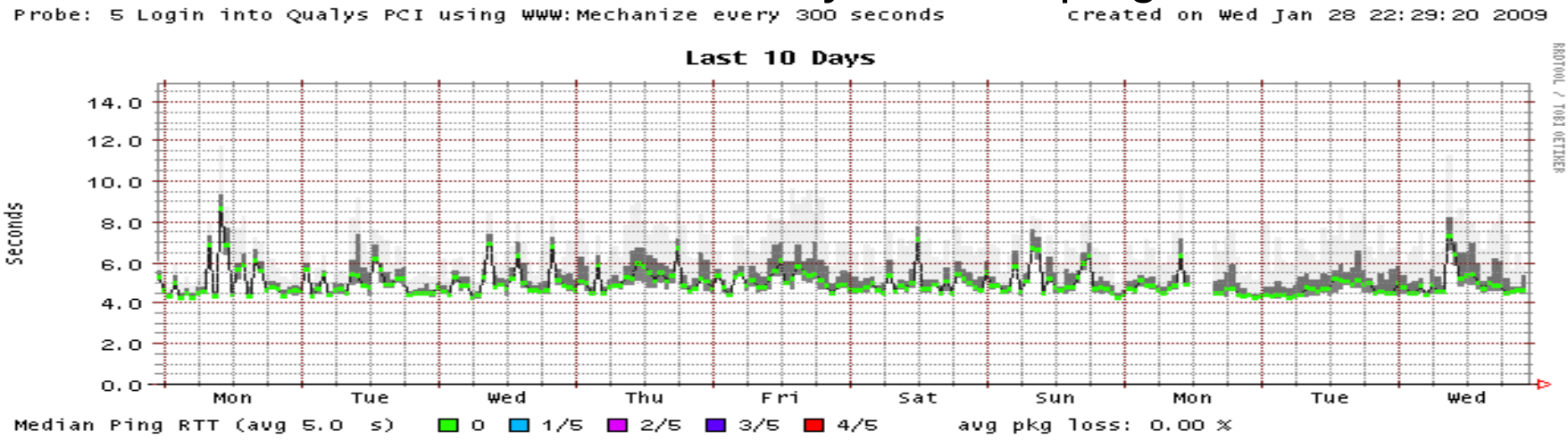


Gaining Trust - Transparency

External Performance and Availability - Keynote



Internal Performance and Availability - Smokeping



ON DEMAND SECURITY

QUALYS®

QualysGuard – next steps

- Architectural improvements
- Platform for security related applications
  - Developed Internally
  - Partners
- Platform for external Security and Audit data
  - Accept upload of Questionnaires and Scan results
  - Digital signing as 3rd party steward
- Hardware encryption devices
- Data separation via Oracle (VPD)
- External Security Audit – ISO

Questions