Security from the Cloud

Achieving Security & Compliance in the Cloud…

Samer M. Omar, CISSP, CISA, CRISC, CISM
Qualys Managing Director – Middle East

MENA ISC 2011, September 19th, 2011

QUALYS®

ON DEMAND SECURITY

E-Era…

- The ever increasing need to connect digitally with customers and suppliers and the rapid pace of technical innovation, the task of maintaining the security and compliance posture of one's network has become a daunting, one could even say impossible, task.

Increase Revenue

Regulatory Compliance

Improve Profitability

Customer Confidence

Secure Data

Downtime

Failed Audits

Lost / Stolen Data

Negative Publicity

Threats

Fraud

QUALYS®

ON DEMAND SECURITY

Changing Perceptions …

In Order for Cloud Computing – Security to grow in the MENA region – we must learn to change the way we think about two simple paradigms of the security industry:

- Data onsite is safer than data offsite.
- Something running on a system is safer than something coming from outside the system.

The paradigm of the industrial age

"Trust is good, control is better"

Joe Stalin

Works fine in a centrally controlled society

QUALYS®

ON DEMAND SECURITY

The paradigm for the information age

"Trust, but verify"

Ronald Reagan

For managing situations beyond your direct control

QUALYS®

ON DEMAND SECURITY

Cloud Computing
(Managed Services)

- Cloud computing / Remote Managed Services are a major departure from traditional networks and applications. Cloud computing service offerings have at least four of these seven traits:
  - Internet (or intranet) accessible
  - A massively scalable, user-configurable pool of elastic computing resources (such as network bandwidth, compute power, memory, etc.)
  - Multi-tenancy (one large software instance shared by many customer accounts)
  - A broad authentication scheme
  - Subscription or usage-based payment (pay as you grow)
  - Self-service
  - Lack of location specificity (anywhere / anytime)

Terminology

The chairman of the Cloud Summit Executive 2008 conference reportedly started the event by joking that he asked 20 people to define cloud computing, and got 22 different answers.

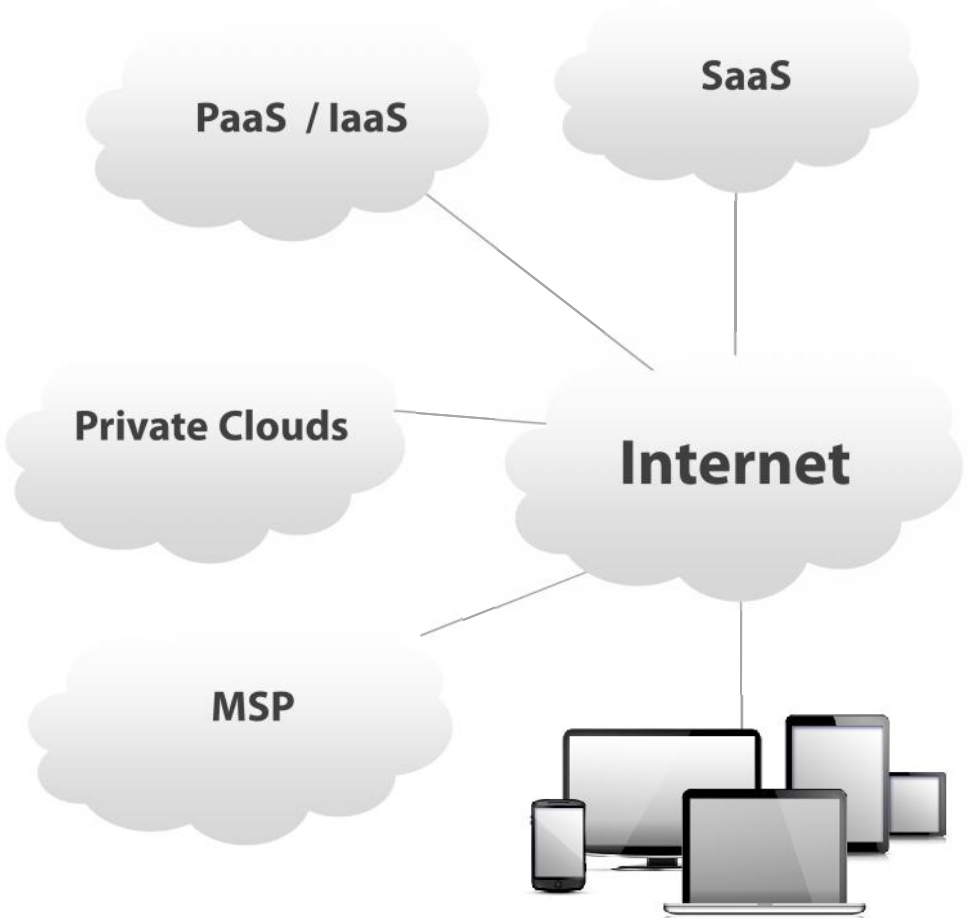
- ”Something that will “profoundly change the way people work and companies operate.” (The Economist)
- “Reliance on the Internet for satisfying the computing needs of the users.” (Wikipedia)
- “We’ve redefined cloud computing to include everything that we already do. I can’t think of anything that isn’t cloud computing with all of these announcements.” (Larry Ellison, Oracle)

Terminology

- Public Cloud - are created by one vendor and offered to the general public
- Private Cloud - Private clouds are hosted by the same organization that utilizes the service (which in general does not support multi-tenancy)
- SaaS – Software as a Service -providers deliver software functionality through the browser, without the end-user having to install software locally.
- PaaS – Platform as a Service - providers give developers complete development environments in which to code, host, and deliver applications.
- IaaS – Infrastructure as a Service - provides massively scalable, elastic computing resources via the Internet.
- Managed Services – remotely managing a clients infrastructure (Security, Applications, Networks, etc) based on a Service Level Agreement and not staffing

Security in the Cloud Computing Era

A dual challenge: Securing the old and the new environment



Cloud Security

- A global & independent 3'rd party view of the security & compliance posture at the device, network and application level

QUALYS®

ON DEMAND SECURITY

The Clouds are Soaring

- "Nearly 90 percent of organizations surveyed expect to maintain or grow their usage of software as a service (SaaS), citing cost-effectiveness and ease/speed of deployment as primary reasons for adoption.“ - Gartner
- “By 2011, early technology adopters will forgo capital expenditures and instead purchase 40 percent of their IT infrastructure as a service,” - Gartner.
- By 2013, 12% of world software market will be Internet-based forms of SaaS and cloud computing - Merrill Lynch.

Market Trends

Figure 10 Different Drivers Exist For Outsourcing Security Versus Other Applications

10-1 Better protection drives adoption of managed or SaaS security services

"How important were the following in driving your firm's adoption of managed or SaaS security services?"

Base: 715 North American and European enterprise IT security decision-makers (multiple responses accepted)

Source: Forrsights Security Survey, Q3 2010

Market Trends

Figure 10 Different Drivers Exist For Outsourcing Security Versus Other Applications

10-2 Speed of implementation and low cost drive interest in SaaS

"Why is your firm interested in software-as-a-service (SaaS)?"

Base: 140 North American and European enterprise IT software decision-makers (multiple responses accepted)

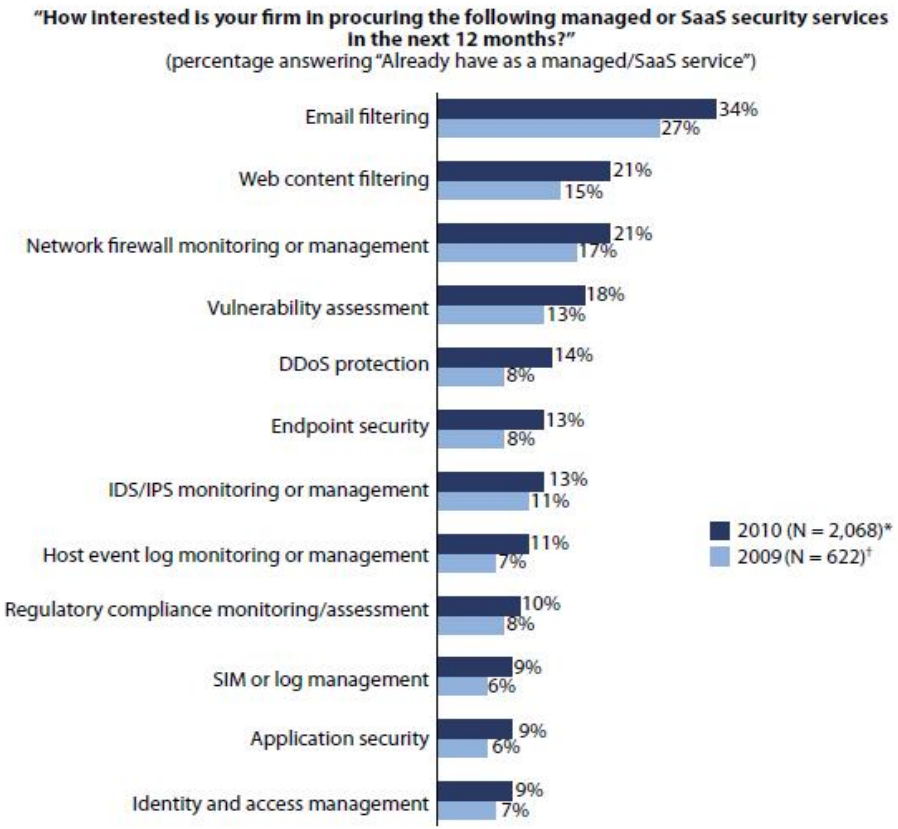
Source: Enterprise And SMB Software Survey, North America And Europe, Q4 2009

56886

Source: Forrester Research, Inc.

Market Trends

Figure 8 Managed Security Solutions Show Robust Uptake



Base: North American and European enterprise and SMB IT security decision-makers

*Source: Forrsights Security Survey, Q3 2010
†Source: Enterprise And SMB Security Survey, North America And Europe, Q3 2009

56886

Source: Forrester Research, Inc.

QUALYS®

ON DEMAND SECURITY

Managing Security – The Challenge

Reputation

" How do I guarantee my customers that their confidential information is safe with me? "

Operations

" What is the next threat that could compromise my company's business?"

Compliance

" How can I ensure my company is meeting compliance requirements in a cost effective way?"

Security is a major undertaking…. It spans Process, Procedure, People, Technology and Business and is concerned with Confidentiality, Integrity, Availability, Privacy, and Compliance

QUALYS®

ON DEMAND SECURITY

Overwhelming Challenges – Argh..

Cyber Crime

Malware Infection

Denial of Service

Phishing

Identity Theft

Criminal Attacks

Credit Card Fraud

Data Leakage

Employee Theft

QUALYS®

ON DEMAND SECURITY

CxO's Nightmare

- Budgets are getting squeezed
- Attracting and retaining security specialists is becoming more difficult
- Number of connected devices is growing (with devices including iPhones, iPads, Android devices, etc.)
- The security landscape is rapidly being turned on its head.
- This is becoming apparent with the barrage of security breach disclosures published in this weeks news, even at leading companies with security measures in place.
- Here's where cloud computing comes in.

Source: www.privacyrights.org

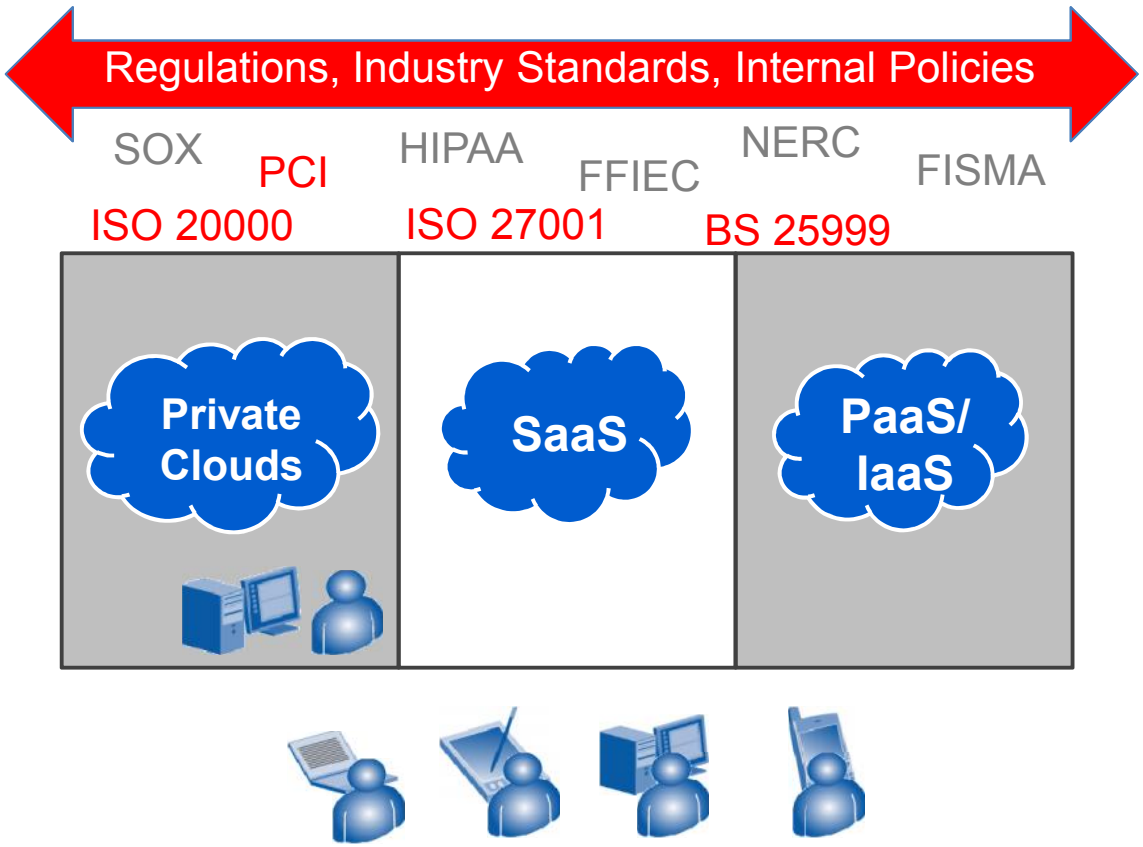
Source: CSI Survey 2010/11 2009 Internet Crime Report

QUALYS®

ON DEMAND SECURITY

Security & Compliance Conundrum

Having to Address both New and Old Challenges



- New and multiplying attack vectors
- Internet based Business Collaboration
- Authentication still an unresolved issue
- Security & compliance silos, fragmented tools & data
- Hard and costly to provide enterprise wide visibility and policy enforcement
- Budget constrains
- A more strategic role for CSOs

Status Quo… Not Sustainable

- Continue to acquire hardware & software to build their computing environments
- Carry the burden of securing those increasing complex environments
- Continue to buy patchwork of security solutions that integrate poorly, and are difficult and costly to deploy and maintain
- Rely on infrastructure and application vendors to provide patches to remediate vulnerabilities found in the wild which the introduced in the first place

Myth …

- We can do it better
- Our environment is more secure
- Our employees can be trusted
- It costs more money over time for SaaS
- We will lose control or visibility of our resources
- We will lose our jobs or career enhancement

Reality…

- Security is complex and cumbersome; very few organizations globally ever really achieve their goals due to budget restrictions, resource availability, etc.
- Most organizations lack the necessary security controls to achieve comprehensive 24x7 security for their entire environment.
- Employee's are the single biggest risk to insider threats which represents 70-80% of all cyber attacks.
- TCO, ROI, TEI are often misrepresented or miscalculated because they are missing key data or hidden costs.
- Cloud Security typically gives more control and opportunities to clients because they are presented security information in a useable and actionable format.

Advantages of a Cloud Computing Approach

- **Low start-up costs make cloud computing especially attractive to small businesses and entrepreneurs.**
- **Low cost for sporadic use**. TurboTax online is free for “standard” taxpayers. Similarly, some cloud-based business services, such as Google Apps, do not need to be purchased for one-time or infrequent computing.
- **Ease of management**. No need to worry about keeping licenses current or purchasing additional hardware.
- **Scalability**. High-growth companies can easily expand the number of users and locations at modest cost.
- **Device and location independence**. The way you access a cloud could be your desktop. It could be someone else's computer. It could be a smart phone.
- **Rapid innovation**. Because vendors are able to roll out new features incrementally, they can respond to user needs more rapidly.

Qualys at a Glance

- Software-as-a-Service (SaaS) since inception
  - Founded in 1999 to a SaaS Vulnerability Management Service
  - Expanded the service as suite of SaaS Security and Compliance offerings
  - Last round of funding in 2004
  - 250 employees (130 in R&D, Support and Operations)
- 5,000+ global customers
  - 47% of Fortune 100
  - 29% of Fortune 500
  - 16% Forbes Global 2000
  - US 65%, EMEA 30%, Asia 5%
  - 7,000+ scanner appliances in 85 countries

Gartner

Highest possible rating of "Strong Positive"

Largest market share

FORRESTER

Highest possible rating of "Leader"

IDC
Analyze the Future

"The leading vendor"

FROST & SULLIVAN

"Market Share Leadership 2010"

Qualys Platform
Software as a Service (SaaS)

- Provides scalable delivery of security services with no additional software or infrastructure to deploy over time:

QualysGuard Vulnerability Management

- *Globally Deployable, Scalable Security Risk and Vulnerability Management*

QualysGuard Policy Compliance

- *Define, Audit, and Document IT Security Compliance*

QualysGuard PCI Compliance

- *Automated PCI Compliance Validation for Merchants and Acquiring Institutions*

QualysGuard Web Application Scanning

- *Automated Web Application Security Assessment and Reporting that Scales with your Business*

QualysGuard Malware Detection (New)

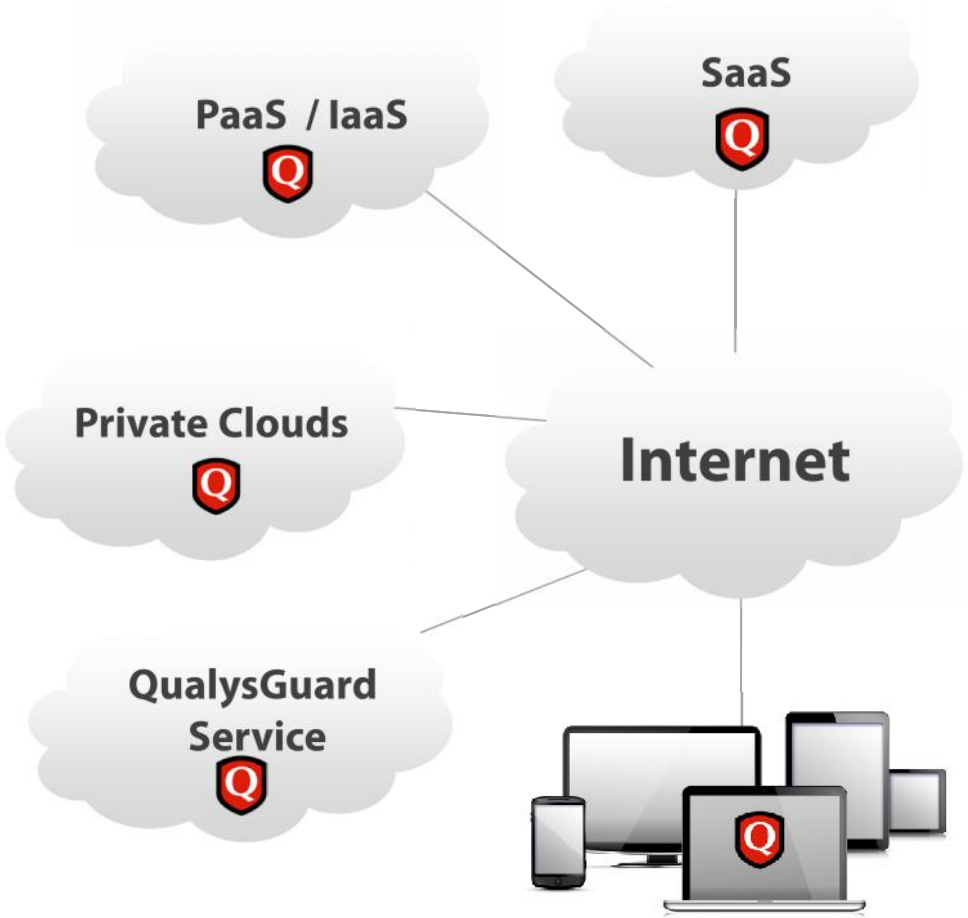
- *Free Malware Detection Service for Web Sites*

Qualys GO SECURE (New)

- *Web Site Security Testing Service and Security Seal that Scans for Vulnerabilities, Malware and SSL Certificate Validation*

Security in the Cloud Computing Era

A dual challenge: Securing the old and the new environment



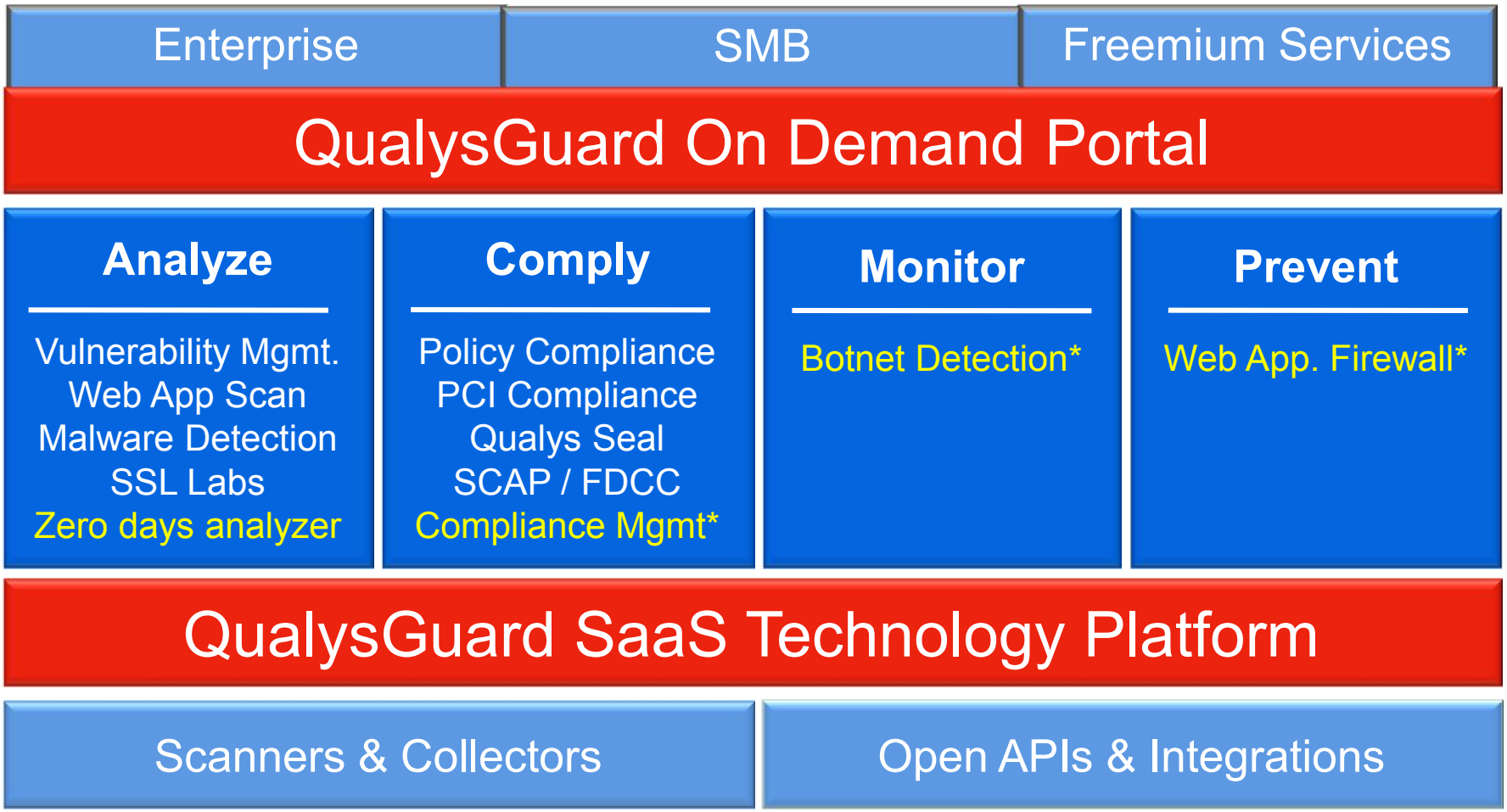
QualysGuard SaaS Platform and Application

- A global & independent 3'rd party view of the security & compliance posture at the device, network and application level
- Now expanding to real-time monitoring and protection

QUALYS®

ON DEMAND SECURITY

QualysGuard® SaaS Applications



QUALYS®

ON DEMAND SECURITY

Parting Thoughts…

- Don't get hung up on definitions. Don't focus on the jargon of whether something is cloud computing, or software as a service, or the latest buzzword. Instead, focus on the changing IT equation. The world of computing is moving away from the on premises IT model, where you keep buying servers, PCs and software licenses as your business grows
- Is Cloud Computing Reliable and Secure? To put it in perspective, ask yourself this: Is there any reason to be less comfortable having your data in a "cloud" than your own data center? When managing a data center, you should compare your ability against that of a third-party provider in supporting high availability, continuity, security, disaster recovery, power consumption and the ongoing management of technical and physical infrastructure.
- As the entire enterprise computing industry continues its consolidation and move to the cloud at an accelerated pace, corporations will be faced with infrastructure and applications becoming obsolete and becoming very difficult to secure.

QUALYS®

ON DEMAND SECURITY

QUALYS®

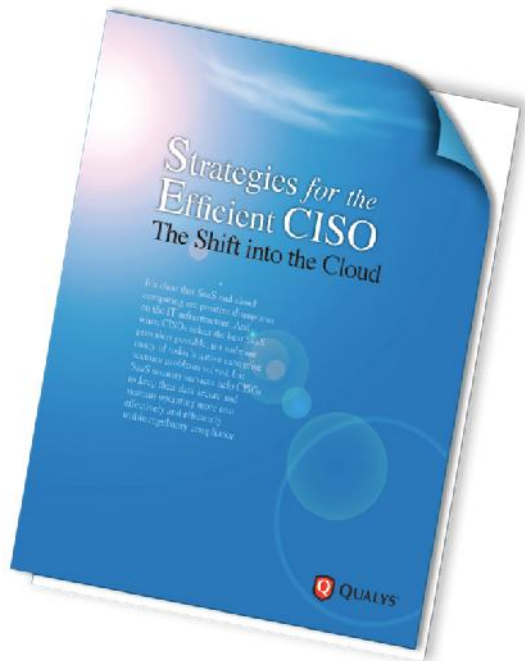
Thank You

Cloud Computing
Major Shift in IT and IT Security

Strategies for the Efficient CISO

The Shift into the Cloud

Cloud computing and SaaS are clearly here to stay and are presenting a major disruption to the IT industry. This paper discusses how this new model will ultimately make security easier and more embedded into the architecture of cloud services, while allowing CISOs to select the best cloud providers and SaaS applications to keep their data secure and systems operating more cost effectively and efficiently within regulatory compliance.



DOWNLOAD A FREE COPY AT:
http://www.qualys.com/efficient_ciso

QUALYS®

ON DEMAND SECURITY