

# 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.



# Strategies for the Efficient CISO

## The Shift into the Cloud

### TABLE OF CONTENTS

OVERVIEW .....	2
THE CHALLENGE OF TRADITIONAL SOFTWARE .....	2
A CATALYST OF CHANGE .....	2
EMERGING ROLE OF CISO .....	3
BALANCING SECURITY AND INNOVATION .....	3
SHIFTING INVESTMENTS TO THE CLOUD .....	5
THREE MAJOR ADVANTAGES OF SAAS APPLICATIONS.....	6
RELYING ON SECURITY SERVICES IN THE CLOUD TO MANAGE VULNERABILITIES AND IT SECURITY COMPLIANCE.....	6
EFFICIENT SECURITY AND COMPLIANCE.....	8
INTEGRATED VIEW OF IT SECURITY COMPLIANCE.....	9
QUALYSGUARD MEETS THE DEMANDS OF TODAY'S CISO.....	9

### APPENDIX

CASE STUDY: EBAY

CASE STUDY: ORACLE

CASE STUDY: MCDONALD'S FRANCE

## OVERVIEW

Who would have believed, barely a few years ago, that so much highly coveted data – financial, customer, medical, marketing, and more – would have moved so quickly to the cloud. Today, it seems, there’s hardly an application that hasn’t been made available as an online service. Even among the proponents of cloud computing, few thought corporate software and data wanted to be liberated so quickly – and be readily available anywhere, anytime, on any device. Today, it seems more unusual not to have a Software-as-a-Service (SaaS) or cloud offering that adds to, or completely replaces, a software maker’s traditional applications.

We believe that the SaaS and cloud computing revolution holds the potential to benefit everyone in the software industry, and all who rely on it for their business. For instance, we in the industry are well experienced with the fact that software is evolving too rapidly to keep up. And managing on-premise applications is a never ending process of software enhancements, upgrades, security fixes, and new installations. Few would disagree that there are too many security vulnerabilities affecting too many applications – and creating too much risk for enterprises everywhere. And within this disorder, most of the burden has fallen on the shoulders of corporations that have had to dedicate extraordinary resources to patch and mitigate the security holes.

## THE CHALLENGE OF TRADITIONAL SOFTWARE

According to the Laws of Vulnerabilities 2.0 research, the average time it takes companies to patch their vulnerabilities is 59 days. Five years ago, that number was 60 days. That’s a reduction of one day in the past five years. When one considers all of the effort and automation that has gone into patch management in the past five years, that’s not much improvement. This shows not only how steep the challenge is, but just how broken the current ecosystem of traditional software is.

Nothing is without tradeoffs. And we’re sure that along with all of the benefits of SaaS, new risks and challenges lay ahead. This is especially true as even more mobile devices access critical corporate data. Consider the fact that 1 out of 10 laptops in use today will be lost or stolen – and we are well aware that most will not be encrypted. Also, there’s a challenge today and going forward with securing new cloud computing architectures, and all of their various shapes and sizes.

## A CATALYST OF CHANGE

Fortunately, and overwhelmingly, the SaaS and cloud computing models are positive disruptions on the infrastructure of both private networks and the Internet. Unlike patching done by individual organizations patch (work that must be duplicated for every system and at every business installation), when SaaS vendors update their software applications, all of their customers are patched instantaneously as well. Thanks to this simple fact, many of the security problems that plague today’s business-technology systems – such as patches and software misconfiguration issues – are solved. And in this and many other ways, the burden of maintaining a secure application largely is transferred from the software user to the software service provider. The effect of proper patching is amplified throughout all of the IT systems the SaaS and cloud providers touch.

Some still are fighting the shift to SaaS and cloud computing, but that resistance to the transformation of on-premise business IT to cloud computing-based IT cannot continue for long. The business benefits, cost savings, and reduction in complexity are just too compelling for businesses to overlook.

Surprisingly, the strongest resistance today emanates from IT departments and IT security staff – mainly out of fear of what will happen if one loses control of his/her data to an outsourced provider. This is a false choice, and the market will not reward cloud or SaaS providers that attempt customer data lock-in. Ultimately, the customer is always in control.

We believe one of the most important challenges for the CISO today – and in the years ahead – will be to help their organizations make the shift into the cloud, as securely and effectively as possible.

## **EMERGING ROLE OF CISO**

Despite reservations from IT departments, businesses will move forward with SaaS and cloud computing adoption. To remain competitive, businesses will have no option but to choose the path that simplifies today's IT complexities the most. And in this switch, the primary – and strategic – role of IT security will be to manage successfully and securely the privacy and security risks posed to the business that are associated with data living in the cloud.

It's crucial that businesses be able to define accurately how their enterprise can integrate and secure their current infrastructure as more of it is moved to cloud services. All businesses, security professionals, CIOs, and vendors need to work together to make this transformation successful for all. Some of the organizations working hard to ensure that we build this new cloud infrastructure right from the beginning include the Cloud Secure Alliance and the Jericho Forum, both of which are promoting cloud computing best practices.

While the visible shift to cloud computing to date has been the movement of applications and data to the cloud, it's not going to stop there. Soon, the day will come when companies not only outsource their software, but their network infrastructure as well. One day, most everything we do on private networks – manage information, applications, infrastructure, and services – will be accessible instantly and secured from any Web browser anywhere. It's time to prepare. And it is the CISO who will be charged with leading the strategy and guiding security parallel with the business, so that IT security and regulatory compliance mandates are met.

The key, moving ahead, will be balance.

## **BALANCING SECURITY AND INNOVATION**

To succeed, the CISO will need many skills. Sure, the technical excellence required to deploy tactical security problems always will be a core responsibility, as will the ability to communicate well among technologists, business managers, and members of the board. However, enterprises also will have to demonstrate ability to achieve results within budgetary constraints and the strategic insight necessary to help grow the business. In all, we believe the CISO will have to excel in innovation, technology, stewardship, and operational efficiencies:

- **Enable new business innovation**

Organizations are advancing plans for new revenue-generating services, strategic investments in business partnerships, and acquisition opportunities. Whether the business innovation leverages technologies such as virtualization, cloud computing services, mobile devices for users, or easily accessible web-based applications, security issues will require innovative strategies to scale as the business grows.

- **Upgrade the technical infrastructure**

Many organizations have postponed investing in their technical infrastructure. Now, organizations need to address infrastructure challenges such as upgrading end-point operating systems, increasing bandwidth for enhanced application performance, and consolidating server resources in virtual data centers. Still, security priorities, including protecting against malicious code and the strategic requirement to audit the infrastructure for regulatory compliance, need to be applied effectively with infrastructure upgrades. The CISO's challenge is to evolve security performance to protect legacy applications against modern threats.

- **Lead in socially rewarding initiatives**

Modern businesses are improving the quality of life with initiatives such as green IT to conserve energy with fewer servers and facilities, leading edge cloud-based mobility, and social networking. The CISO is contributing to changes in social norms by addressing the security issues involved with a combination of products, services, and end user training. Effective CISOs know they cannot block progress on the grounds of security, but are finding ways to help the organization participate in socially rewarding initiatives.

- **Improve the bottom line of security**

IT and security teams are expected to find ways to reduce operating expenses. And the corporate goal of realizing continuous improvements in operational efficiency leads the CISO to seek automated solutions that require less administrative overhead, less invasive products that reduce support costs, and strategies that apply equally to enable new business innovation, upgrade the technical infrastructure, and lead in socially rewarding initiatives. This balance between strategic initiatives, tactical solutions, and the dynamics of the business is represented in Exhibit 1.



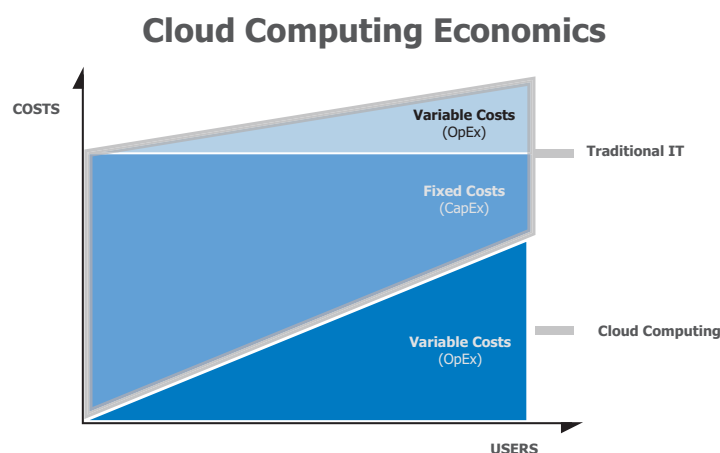
**Exhibit 1.** Achieving balance between strategic initiatives, tactical solutions, and the dynamics of the business.

This is why the efficient CISO seeks a security strategy that orchestrates the launching of new business initiatives, technical infrastructure, and leading the organization toward socially rewarding activities. It's certainly a challenge to achieve a balance between these three business objectives. For instance, the CISO can improve the bottom line of security by purchasing fewer products, which will leave security gaps in the business. Or he/she can decline to offer a security strategy for intelligent handheld devices at the risk of alienating end users. Also, the CISO can invest in only one business driver at the expense of the others, so to be successful there is the need to find a security strategy that achieves a balance among the business drivers, strategic initiatives, and tactical solutions.

Fortunately, the SaaS delivery model helps the CISO succeed in each of these efforts. That's why leading CISOs are increasingly adopting SaaS as a means to efficiently secure the business while keeping innovation, security, and cost control in balance. And, for these reasons, SaaS is becoming an increasingly important strategic element in IT and security arsenals. IDC estimates total IT cloud services revenue will grow from \$17.4 billion in 2009 to \$44.2 billion by 2013. Qualys is leading this strategic shift into the cloud with compliance and vulnerability management solutions that are delivered as a security service.

## SHIFTING INVESTMENTS TO THE CLOUD

This trend toward cloud and SaaS-based applications is driven by the needs for enterprises and SMBs alike to innovate, simplify, and cut costs. Qualys' on demand approach to IT security and compliance enables organizations of all sizes to achieve both vulnerability management, policy compliance and web application security initiatives cohesively, while reducing costs and streamlining operations. One of the key distinguishing features of cloud-based security is the lack of equipment or software that security teams must deploy throughout the organization – the SaaS provider hosts those resources within secure data centers. That means there is less equipment to deploy and software to install in order to achieve the benefits. Furthermore, without capital equipment requirements, the economics of cloud computing are dominated by variable costs – costs that are controlled by the customer according to the organization's use of the service, as shown in Exhibit 2.



**Exhibit 2.** The economics of cloud computing provide CISOs with total control

Influencing the behavior of others has always been a fundamental security skill, but the scale of the emerging requirement is substantially greater, requiring an understanding of psychology and marketing, as well as social networking skills. The targets of this influence are diverse, demanding the political skills to present a complex business case in person to an investment appraisal board, as well the marketing skills to direct a sophisticated program of security awareness and behavior change across a large, remote customer base.

A further essential skill is the ability to direct the strategic response to a major incident involving multiple business partners and suppliers. The growing complexity of information systems combined with the increasing impact of breaches on intellectual assets, such as corporate reputation, demands a sophisticated, business-focused response, not just an operational fix. Responding strategically requires exceptional crisis coordination skills and an ability to think objectively, improvise creatively, and draw on intelligence sources, investigative services and digital forensics. Such a combination of skills is hard to find, teach and apply.

## THREE MAJOR ADVANTAGES OF SAAS APPLICATIONS

- **Deploys with minimal infrastructure or labor overhead**

Since there is little or no equipment required on-premise, security teams can deploy the cloud-based service across the organization with relative ease. The SaaS offering provides a strategic solution that covers new business initiatives as well as technical infrastructure upgrades and support for new socially rewarding ways of conducting business.

- **Performs its job only when needed**

Cloud computing can be in use within a matter of minutes or hours, and its use of the web as a transport mechanism to provider data centers actually increases the availability of the service to the organization. Additionally, the organization automatically receives the latest functional upgrades and service improvements from the provider whenever the service is requested.

- **Places total control of costs in the hands of the CISO**

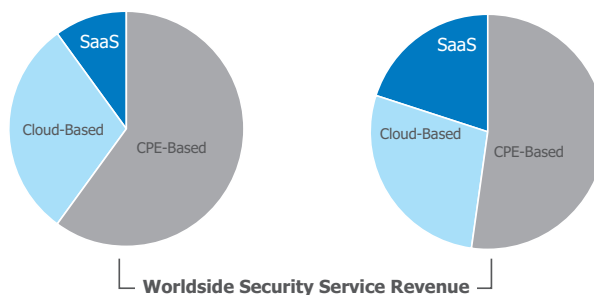
The cloud application executes only when requested – putting the security group in total control of operating expenses. CISOs being measured by reducing the bottom line impact of security are shifting resources to the cloud due to the lack of up-front capital investment in equipment, software, and labor, and the “pay as you use” control of variable expenses.

## RELYING ON SECURITY SERVICES IN THE CLOUD TO MANAGE VULNERABILITIES AND IT SECURITY COMPLIANCE

The shift to mature cloud-based SaaS solutions for security is proving too compelling for many to let pass. Consider the findings of Infonetics Research: SaaS revenue is forecast to grow from 10% of total security service revenue in

2009 to 22% in 2014, with cloud-based and CPE-based security services making up the balance. In addition, also from Infonetics Research, worldwide revenue derived from security services delivered through SaaS grew 70% last year. The primary driver for this growth is the great efficiency cloud-based security services provide the CISO to help the business succeed.

### SaaS Security Service Revenue Share Grows Dramatically from 2010 to 2014



© Infonetics Research, Managed Security Services and SaaS Biannual Market Size and Forecasts, Mar. 2010.

In addition to the ease of deployment, continuous availability, and variable cost control afforded by SaaS, security in the cloud also has benefits that are directly related to providing advanced security services based on inspection of content or systems for advanced threats. There are good reasons why efficient CISOs are allocating more of their budgets to cloud-based services:

- **Operating with the most up-to-date threat information possible.**

Recognizing the latest vulnerability, malicious code, or rogue web site requires a dedicated team of researchers to characterize the threat and update the security inspection process. A security SaaS offering, such as that delivered by Qualys, relieves the CISO organization of the onerous task of distributing updates to customer premise equipment. The cloud ensures that the most recent information possible is utilized every time the organization invokes the service.

- **Automating compliance verification.**

Cloud-based security solutions can correlate information from system inspections to generate reports of security performance automatically and vet those results against compliance baselines. This way, automating compliance verification saves the CISO precious time and energy, and allows security teams to monitor critical systems continuously for security incidents.

- **Reaching every corner of the organization.**

With a security SaaS solution that is delivered through the cloud, the CISO does not have to spend incremental time and resources distributing the solution to remote data centers, campuses, and facilities. The dispersed business receives enhancements from the security vendor without the need to schedule and push upgrades throughout the organization.

## QUALYS' ON DEMAND IT SECURITY RISK AND COMPLIANCE SOLUTIONS

Recognized as the leading provider of on demand IT security risk and compliance solutions, Qualys enables organizations of all sizes to easily and cost-effectively ensure that their business technology systems remain highly secure and within regulatory compliance. Through its IT security and compliance solutions, Qualys makes it possible for organizations to strengthen the security of their networks and web applications, and conduct automated security audits that ensure regulatory compliance and adherence to internal security policies.

Qualys is the only security company that delivers these solutions through a single Software-as-a-Service platform: QualysGuard®. All of Qualys' on-demand solutions can be deployed within hours anywhere around the globe, providing an immediate view of security and compliance posture. As a result, QualysGuard is the most widely deployed security-on-demand solution in the world, performing more than 500 million audits per year.

## EFFICIENT SECURITY AND COMPLIANCE

Qualys' security and compliance services enable CISOs to achieve both network security and policy compliance initiatives cohesively, while reducing costs and streamlining operations. The QualysGuard Security and Compliance Suite incorporates Qualys' industry-leading vulnerability management service with a robust IT compliance solution, comprehensive web application scanning, and malware detection services.

### **Together in one security management platform, organizations can:**

- ✓ Define policies to establish a secure IT infrastructure in accordance with proper governance and best practices frameworks.
- ✓ Automate ongoing security assessments and manage vulnerability risk on systems and applications effectively.
- ✓ Mitigate risk and eliminate threats, utilizing the most trusted vulnerability management application in the industry.
- ✓ Monitor and measure IT compliance from one unified console – saving time and reducing costs.
- ✓ Distribute security and compliance reports customized to meet the unique needs of CISOs, business executives, auditors and other security professionals.

## INTEGRATED VIEW OF IT SECURITY AND COMPLIANCE

For CISOs with limited staff and financial resources, the QualysGuard Security and Compliance Suite eliminates network auditing and compliance inefficiencies by leveraging the organization's core IT security information. In one consolidated suite, groups with different responsibilities can utilize similar information for their specific needs.

The QualysGuard Security and Compliance Suite automates the process of vulnerability management and policy compliance across the enterprise, providing network discovery and mapping, asset prioritization, vulnerability assessment reporting, and remediation tracking according to business risk. Policy compliance features allow security managers to audit, enforce, and document compliance with internal security policies and external regulations.

**The core components of the QualysGuard Security and Compliance Suite include:**

### 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

### Qualys SECURE Seal

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



The QualysGuard  
IT Security & Compliance Suite

## QUALYSGUARD MEETS THE DEMANDS OF TODAY'S CISO

Qualys has built its service on the ability to detect and report vulnerabilities effectively across an entire organization's infrastructure. Since there are relatively few known vulnerabilities, compared to known attack exploits, it makes sense to prioritize the discovery and patching of vulnerabilities, rather than fight every potential exploit or newly written malware. QualysGuard is an ideal match for today's challenges because it readily ensures a secure and compliant environment.

**Here's how QualysGuard supports today's CISO:**

- **Provide global visibility of organization's IT security and compliance posture**  
QualysGuard highly scalable global deployment capabilities with a centralized database of results provides the CISO increased transparency into its IT systems risk and the ability to remedy noncompliant systems rapidly.
- **Enable new business innovation**  
The CISO easily can add new applications and lines of business to the Qualys vulnerability and compliance management program with no constraints placed on business infrastructure.
- **Upgrade technical infrastructure**  
The CISO can ensure compliance and detection of malware for new operating environments and applications. The Qualys security service provides value as the infrastructure changes, and allows the CISO to plan an evolutionary change to the technology supporting the business.
- **Improve the bottom line of security**  
Qualys requires no upfront investment in people or equipment. Service fees are based on the number of requested scans and the scope of the vulnerability analysis. The CISO controls how often the Qualys service is utilized.
- **Lead in socially rewarding initiatives**  
Security in the cloud is one of the leading contributors to green IT programs, as solutions such as Qualys' relieve IT of having to spend on power and cooling resources for dedicated servers. Also, security risk and compliance management for new cloud-based computing models is leveraged efficiently.
- **Embrace tactical solutions**  
No matter how much planning is done within the business, there will be situations such as discovery of a new application or a merger with another business in which Security needs to quickly assess a technical environment against compliance guidelines. The Qualys service enables the CISO to perform the assessment and get an operational report in hours – anywhere in the world.
- **Advance strategic initiatives**  
The use of the Qualys service provides a strategic tool for building an IT security risk and compliance program. Once in use, it can perform automated validation that the business infrastructure is resilient to the latest advanced threats.

It's clear that SaaS and cloud computing are positive disruptions on the IT infrastructure. And, when CISOs select the best SaaS providers possible, not only are many of today's native enterprise security problems solved, but SaaS security services help CISOs to keep their data secure and systems operating more cost effectively and efficiently within regulatory compliance.

*The case studies referenced at the end of this document provide further examples of how leading organizations are taking advantage of this shift into the cloud to achieve their security and compliance goals.*

**To learn more about Qualys and try the QualysGuard IT Security & Compliance Suite, visit: [www.qualys.com](http://www.qualys.com).**

# Appendix

---

CASE STUDY: EBAY

CASE STUDY: ORACLE

CASE STUDY: MCDONALD'S FRANCE