SECURITY & COMPLIANCE IN THE CLOUD AGE

QUALYS®

Table of Contents

Introduction 2

Security and Compliance in the Cloud Age 3

Challenges of Security and Compliance in the Cloud Age 5

The Cloud Security Platform 7

Providing Security and Compliance in the Cloud Age 9

The QualysGuard Cloud Platform 11

Why Qualys 13

Introduction

We have entered the age of pervasive technology. At home, in the office, or on the road, a vast portion of us are connected wherever we are, not only with people but with an array of information and technologies. It has become hard to distinguish between work time and leisure time, with the same devices used for both contexts interchangeably. This inescapable trend provides both tremendous opportunities and significant risks to organizations that embrace the "always on" culture for their customers, trading partners and employees.

Technology services are consumed whenever and wherever needed, and the associated data can be stored anywhere. We believe at Qualys that organizations, at the risk of being left behind, must enter the "Cloud Age," marking a major departure from the constraints of client/server and even the first generation Web applications, enabling a new connectivity-based world to foster better communications, tighter collaboration and accelerating productivity.

Security and Compliance in the Cloud Age

The Cloud Age can be described by a few attributes:

Browser-Centricity

The web browser is the common interface to the Internet, corporate systems and data stores. This opens up pervasive access to all constituencies on a variety of devices, including PCs and smartphones owned by both the organization and employees (BYOD). Yet browsers contain vulnerabilities that can lead to malware infection – despite efforts from developers to patch and address these issues – and have become the path of least resistance for attackers to capture information, steal access credentials or gain control of users' devices.

Web Applications: The New Perimeter

Easier to build and deploy, web applications now represent the main access point to enterprise networks and data, thus replacing the traditional perimeter. Organizations now must spend as much time and effort detecting, tracking and managing web applications as they do their traditional perimeter networks. The importance of these applications and the quantity and sensitivity of their underlying data have attracted attackers intent on exploiting web application weaknesses and configuration flaws to steal sensitive data or to reduce application availability.

Data Location Independence

Cloud computing enables applications to be composed of data from anywhere and everywhere, stored in a variety of internal and cloud-based data stores, requiring secure communications between these various locations. Although many cloud application providers have made significant security investments, cloud services (by definition) provide organizations with limited visibility and access to the underlying architecture, inhibiting organizations from identifying potential gaps and validating the effectiveness of their security strategies.

Globalization Is the Norm, Not the Exception

The cloud disintegrates regional and territorial boundaries. Data moves from place to place, users move transparently between locations, and systems can be administered by a variety of authorized parties, not necessarily employees of your organization. This creates jurisdictional complexities, authentication and trust requirements, and complicates compliance reporting and attestation.

Hybrid Infrastructure

No organization of scale can shut down their internal systems overnight, but they have been making significant efforts to make those resources more efficient through consolidation and virtualization. Given IT infrastructure will remain a hybrid of traditional physical data center and cloud-based technologies for the foreseeable future, security controls must be enforced and compliance documentation produced consistently regardless of whether the technology asset is in your organization's data center or a cloud-provider anywhere in the world.

The productivity, agility and economic advantages of cloud computing mean there is no stopping the drive to the Cloud, regardless of the risks and complexities. So let's dig a little deeper into the challenges the Cloud Age introduces for every IT organization.

Challenges of Security and Compliance in the Cloud Age

Security is a battle that your organization can't win, and success is usually measured by keeping organizations out of the news and your senior executives out of jail. The drive to a web-based reality and increasing adoption of new cloud-based and hybrid infrastructures further complicate the job of the typical security professional.

Securing at Cloud Scale

As described by the Cloud Security Alliance, one of the essential characteristics of the cloud is "rapid elasticity," meaning the cloud can grow as quickly as your organization needs it to. In the old days, devices needed to be procured, provisioned, and installed, giving the organization time to protect the new devices. Provisioning a new cloud instance takes minutes, creating issues in both visibility (knowing what devices are actually out there at any point in time) and control (ensuring proper configurations and controls are implemented on new resources).

Increasing Attack Surface

With web applications emerging as the "New Perimeter," organizations must embrace the reality that they have as many perimeters as they have web applications. This combined with increased outsourcing and business partnering result in a dramatic expansion of the attack surface. This exponential increase of targets, including databases, desktops, mobile devices, routers, servers and switches, mushrooms the number of security vulnerabilities potentially providing hackers with unauthorized access to IT systems. It's no longer sufficient to build a strong network security perimeter and neglect the security of internal networks and devices.

Leveraging Existing Security Controls

Organizations have historically deployed niche security products to address specific security issues. However, this approach often does not provide a current, accurate and global picture of an organization's security and compliance. As IT infrastructures evolve to include a mixture of on-premise, cloud and hybrid, these task-specific security products running on premise create challenges providing a complete and accurate inventory of IT assets and configurations, thus preventing organizations from effectively protecting their infrastructures from the threats of the Cloud Age.

Securing Thin Devices

The evolution of smartphone technology has brought more sophisticated and secure mobile operating systems, locked down by default, yet offering limited visibility and control to the operating system core. Yesterday's kernel-level anti-malware techniques are no longer relevant. As data leakage and malware continue to plague these devices, organizations will need to consider different methods to provide sufficient security for these devices.

Prioritizing Security Activities

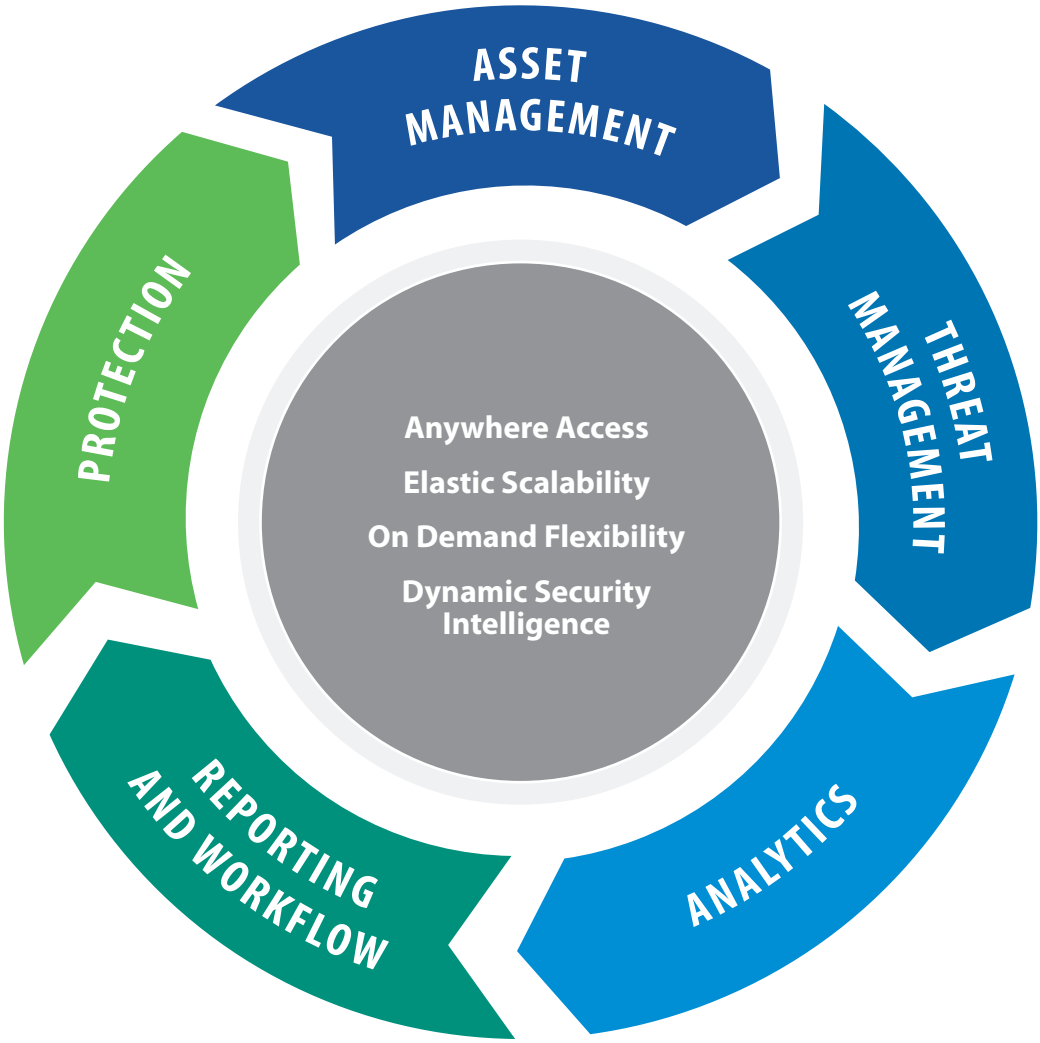
Ongoing funding, resource and expertise constraints make it difficult for many organizations to remain protected in the Cloud Age, thus security success depends on carefully selecting which activities get done. The Cloud Age complicates these decisions forcing organizations to prioritize security activities across a number of internal/external service providers and staff that may not be under your control. Compounding the issue is the dynamic nature of the attackers, who could launch a new attack requiring immediate activity, rendering the best-laid plans irrelevant.

Reporting for Compliance

One of the unfortunate effects of security breaches is an increasingly restrictive regulatory and compliance environment. Given the global nature of most Cloud Age business, your organization likely must adhere to regulations and policies from multiple national and local authorities, which frequently overlap and change. Compliance with these various regulatory regimes requires costly and time-consuming measures and carries significant financial and reputational consequences for non-compliance. Examples of such external regulations include the Revised International Capital Framework, or Basel II, the Health Insurance Portability and Accountability Act, or HIPAA, North American Electric Reliability Corporation Standards, or NERC, Payment Card Industry Data Security Standards, or PCI DSS, and the Sarbanes-Oxley Act of 2002, or SOX. A 2011 Gartner survey estimates that it costs organizations an average of $1.7 million to become compliant with PCI DSS, and that is only one regulation.

The Cloud Security Platform:

Laying the Foundation of Security and Compliance in the Cloud Age



Today's customer premise-based solutions cannot meet the needs of security and compliance in the Cloud Age, so a new solution is required.

Cloud platform essential characteristics:

Anywhere Access

Your employees, service providers, and customers can be anywhere, thus your cloud security platform must be accessible from anywhere, at any time.

Elastic Scalability

The security and compliance function for the Cloud Age needs to be as elastic and scalable as the cloud itself. As your organization's IT infrastructure grows, the platform you use to secure it needs to grow in lock step.

On Demand Flexibility

The platform to secure the Cloud Age needs to have flexibility to offer your organization only what's needed, when it's needed, and charge only for the amount used.

Dynamic Security Intelligence

Battling constantly changing, finely tuned attacks, the cloud security platform needs to be updated dynamically with the most current vulnerability, configuration, and malware information to allow your organization to respond faster to emerging threats.

The cloud security and compliance platform must deliver the following features to meet the needs of today's organizations:

Asset Management

Your organization cannot protect unknown assets. Furthermore, in order to prioritize, the value of the asset to your organization must be considered. Thus, the platform needs to have a robust asset management capability.

Threat Management

The platform must have the ability to scan for vulnerabilities, assess and monitor configurations, and determine the risk an attack presents to the organization. In hybrid IT environments, the platform must provide a single view across the traditional data center and in private/public cloud environments, across a multitude of devices and across the application layer.

Analytics

The key to helping prioritize activities and combat advanced attacks is generating actionable information from a variety of data sources. The platform needs to be able to analyze the data and provide clear visualization of the information to security administrators needing to make instant decisions.

Reporting and Workflow

Given the increasing number of regulatory mandates across regions and jurisdictions, the platform needs to provide a common set of reports across the enterprise, while supporting any regulatory reporting regime, and offering the ability to support inter-enterprise workflows, as outsourcing security functions becomes more prevalent.

Protection

If it's possible to block an attack while minimizing false positives, the platform should provide a capability to either provide direct protection or integrate with other active defenses, including web application firewalls, intrusion prevention, and next generation firewalls.

Building a Cloud Security Platform doesn't happen overnight. In fact, it takes over a decade to gain the critical mass, global presence, security intelligence and world-class expertise required. It takes a unique company to meet the security and compliance needs of organizations in the Cloud Age: that company is Qualys.

Providing Security and Compliance in the Cloud Age

Qualys was founded in 1999 at the height of the technology bubble, when Internet security was just beginning to appear on executive agendas. In December 2000, the company became one of the first entrants in the vulnerability management market. Driven by a powerful combination of highly accurate and easy-to-use scanning technology delivered via the web, Qualys pioneered the use of "Software-as-a-Service," or SaaS, to address security and compliance problems for organizations of all sizes.

The heart of Qualys is the QualysGuard Cloud Platform, which provides an integrated suite of solutions to automate the lifecycle of asset discovery, security assessment and compliance management for an organization's IT infrastructure and assets, whether they reside inside the organization, on their network perimeter or in the cloud. QualysGuard's cloud delivery model can be easily and rapidly deployed on a global scale, enabling faster implementation, broader adoption and lower total cost of ownership than traditional on-premise enterprise software products. By deploying QualysGuard, organizations can gain actionable security intelligence into potential vulnerabilities and malware in their IT infrastructure and expedite their compliance with internal polices and external regulations.

The results speak for themselves. Over the past 12 years, Qualys has built a global customer base of over 5,700 organizations located in 100+ countries, including a majority of both the Forbes Global 100 and Fortune 100. These customers perform over 500 million IP audits annually.

The Cloud Age will force organizations of all shapes and sizes to become more nimble in how they protect critical corporate information assets. QualysGuard delivers actionable security intelligence, and is positioned to be the organization's strategic IT security and compliance platform for years to come.

QUALYSGUARD® Cloud Platform

The QualysGuard Cloud Platform consists of a suite of IT security and compliance solutions that leverage shared and extensible core services and a highly scalable multi-tenant cloud infrastructure.

QualysGuard Cloud Infrastructure

QualysGuard's infrastructure includes the data, analytical capabilities, software and hardware infrastructure and infrastructure management capabilities providing the foundation for the cloud platform. Here are some key aspects:

Scalable Capacity

QualysGuard's modular and scalable infrastructure leverages virtualization and cloud technologies allowing our operations team to dynamically allocate additional capacity on demand across our entire QualysGuard Cloud Platform to provide for the growth and scalability of our solutions.

Big Data Indexing and Storage

Built on top of our secure data storage model, QualysGuard's analytics engine indexes petabytes of data and uses this information in real time to execute tags or rules to dynamically update IT asset properties, for use in various workflows for scanning, reporting and remediation.

KnowledgeBase

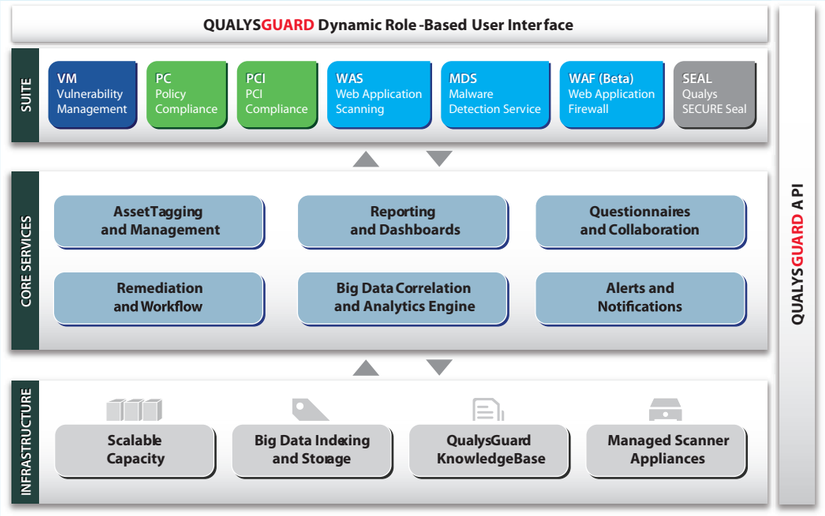
QualysGuard relies on our comprehensive repository, the QualysGuard KnowledgeBase, of known vulnerabilities and compliance controls for a wide range of devices, technologies and applications to power our security and compliance technology. The KnowledgeBase is dynamically updated with information on new vulnerabilities, control checks, validated fixes and content refinements on an ongoing basis.

Managed Appliances

Qualys hosts and operates thousands of globally distributed physical appliances used to assess customers' externally facing systems and web applications. To assess internal IT assets, organizations deploy either physical appliances or downloadable virtual images within their internal networks. QualysGuard appliances update themselves in a transparent manner using our automated and proprietary management technology.

QualysGuard Core Services

QualysGuard's Core Services enable integrated workflows, management and real-time analysis and reporting across all of our IT security and compliance solutions. Our Core Services include:



Asset Tagging and Management

Enables your organization to easily identify, categorize and manage large numbers of assets in highly dynamic IT environments and automates the process of inventory management and hierarchical organization of IT assets.

Reporting and Dashboards

A highly configurable reporting engine that provides your organization with reports and dashboards based on user roles and access privileges.

Questionnaires and Collaboration

A configurable questionnaire engine enables your organization to easily capture existing business processes and workflows to evaluate controls and gather evidence to validate and document compliance.

Remediation and Workflow

An integrated workflow engine allows your organization to automatically generate helpdesk tickets for remediation and to manage compliance exceptions based on organizational policies, enabling subsequent review, commentary, tracking and escalation. This engine automatically distributes remediation tasks to IT administrators upon scan completion, tracks remediation progress and closes open tickets once patches are applied and remediation is verified in subsequent scans.

Big Data Correlation and Analytics Engine

An analytics engine indexes, searches and correlates petabytes of security and compliance data with other security incidents and third-party security intelligence data. Embedded workflows enable your organization to quickly assess risk and access information for remediation, incident analysis and forensic investigations.

Alerts and Notifications

An alert engine creates email notifications to alert team members of new vulnerabilities, malware infections, scan completion, open trouble tickets and system updates.

QualysGuard Cloud Suite

QualysGuard enables your organization to use the solutions you need, when you need them and pay for only what you use. Your organization can subscribe to one or more of our security and compliance solutions, and over time expand your use.

Vulnerability Management

QualysGuard VM is an industry leading and award-winning solution that automates network auditing and vulnerability management across an organization, including network discovery and mapping, asset management, vulnerability reporting and remediation tracking. Driven by our comprehensive KnowledgeBase of known vulnerabilities, QualysGuard VM enables cost-effective protection against vulnerabilities without substantial resource deployment.

Policy Compliance

QualysGuard PC enables organizations to analyze and collect configuration and access control information from their networked devices and web applications and automatically maps this information to internal policies and external regulations in order to document compliance. QualysGuard PC is fully automated and helps reduce the cost of compliance without requiring the use of software agents.

PCI Compliance

QualysGuard PCI can provide organizations storing cardholder data a cost-effective and highly automated solution to verify and document compliance with PCI DSS. QualysGuard PCI allows merchants to complete the annual PCI Self-Assessment Questionnaire, as well as performing vulnerability scanning for quarterly PCI audits and web application security.

Web Application Scanning

QualysGuard WAS uses the scalability of our cloud platform to allow organizations to discover, catalog and scan any and all of an organizations web applications. QualysGuard WAS scans and analyzes custom web applications and identifies vulnerabilities that threaten underlying databases or bypass application access controls.

Malware Detection Service

QualysGuard MDS enables organizations to scan, identify and remove malware infections from their websites. QualysGuard MDS utilizes behavioral and static analysis to detect malware and monitor web sites on an ongoing basis.

Web Application Firewall

QualysGuard WAF, currently in beta testing, delivers enterprise-grade web application security without the costs, footprint, and complexity associated with appliance-based web application firewall solutions. It protects web applications from attack vectors by enhancing default web application configurations and virtual patching. QualysGuard WAF also improves web site performance by reducing page load times and optimizing bandwidth, leveraging our global network of web caches.

Qualys SECURE Seal

QualysGuard SECURE Seal enables organizations to demonstrate to online customers that they maintain a proactive security program. SECURE Seal includes scanning for the presence of malware, network and web application vulnerabilities and validates the integrity of SSL certificates. Organizations showing no critical security issues can display a QualysGuard SECURE Seal on their web sites.

Why Qualys?

Qualys' vision is to transform the way organizations secure and protect their IT infrastructures and applications. Qualys is the best choice for your security and compliance needs.

Trusted brand in cloud security

Qualys pioneered cloud security, having introduced the first vulnerability management solution as a service in 2000, and maintains a reputation as a trusted and objective provider of reliable and accurate vulnerability and compliance assessments.

Scalable and extensible cloud security platform

Our highly-scalable cloud architecture and modular security and compliance solutions allow customers of all sizes, across many industries to access the functionality to help ensure the security of their IT infrastructures. Our cloud platform serves organizations ranging from small businesses to globally distributed enterprises with millions of networked devices and applications.

History of cloud security and compliance innovation

For over 12 years, Qualys has introduced innovative cloud security and compliance solutions allowing our customers to protect their IT environments more effectively and at a lower cost. We have invested significantly in the QualysGuard Cloud Platform and are well positioned to address the challenges of the evolving IT security and compliance landscape.

Pay for What You Use, When You Use It

QualysGuard allows customers to easily try one or more of our solutions without risk from any web browser. This model allows our customers to subscribe to only the solutions they need and provides the ability to easily expand the breadth and depth of their deployment as their needs evolve.

To get a free trial of the QualysGuard Cloud Suite, visit http://www.qualys.com/trial

QUALYS

Qualys, Inc. - Headquarters
1600 Bridge Parkway
Redwood City, CA 94065 USA
T: 1 (800) 745 4355, info@qualys.com

Qualys is a global company with offices around the world. To find an office near you, visit **http://www.qualys.com**