SICHERHEIT & COMPLIANCE IM CLOUD-ZEITALTER

QUALYS®

Inhalt

Einführung

Wir leben heute im Zeitalter der allgegenwärtigen Technologie. Viele von uns sind ständig vernetzt – zu Hause, im Büro und unterwegs, und nicht nur mit anderen Menschen, sondern auch mit einer Vielzahl von Informationsquellen und Technologien. Die Grenzen zwischen Arbeit und Freizeit verschwimmen, da wir hier wie dort dieselben Geräte verwenden. Für Unternehmen, die die „Always on"-Kultur für ihre Kunden, Geschäftspartner und Mitarbeiter pflegen, birgt dieser unumkehrbare Trend sowohl immense Chancen als auch erhebliche Risiken.

Technische Dienste werden in Anspruch genommen, wann und wo immer man sie braucht, und die damit verbundenen Daten können überall gespeichert sein. Wir bei Qualys glauben, dass Unternehmen ins „Cloud-Zeitalter" einsteigen müssen, um nicht hinter ihren Mitbewerbern zurückzufallen. Dieser Schritt bedeutet eine erhebliche Abweichung von den Beschränkungen des Client/Server-Modells und selbst von den Webanwendungen der ersten Generation. Er eröffnet eine neue vernetzte Welt, die bessere Kommunikation, engere Kooperation und höhere Produktivität fördert.

Sicherheit und Compliance im Cloud-Zeitalter

Das Cloud-Zeitalter lässt sich anhand einer Reihe von typischen Merkmalen beschreiben:

Der Browser im Zentrum

Der Webbrowser dient als gemeinsame Schnittstelle zum Internet, den unternehmenseigenen Systemen und Datenspeichern. Alle Nutzergruppen haben durchgehenden Zugriff auf eine Vielzahl von Geräten, darunter PCs und Smartphones, die dem Unternehmen oder auch den Mitarbeitern selbst gehören (BYOD). Browser enthalten jedoch Schwachstellen, die zu Malware-Infektionen führen können. Wenngleich die Entwickler bemüht sind, diese Probleme zu lösen, sind die Browser zum meistgenutzten Einfallstor für Angreifer geworden, die sich Informationen verschaffen, Zugangsdaten entwenden, oder Geräte unter ihre Kontrolle bringen wollen.

Webanwendungen: Der neue Perimeter

Webanwendungen sind vergleichsweise einfach zu entwickeln und bereitzustellen und bilden mittlerweile die Hauptzugangspunkte zu Unternehmensnetzen und -daten. Damit ersetzen sie den traditionellen Perimeter. Unternehmen müssen heute für die Inventarisierung, Überwachung und Verwaltung ihrer Webanwendungen genauso viel Zeit und Mühe aufwenden wie für ihre traditionellen Perimeternetze. Die Bedeutung dieser Anwendungen und die Menge und Sensibilität der zugrundeliegenden Daten locken Angreifer an, die die Schwachstellen und Konfigurationsfehler in Webanwendungen ausnutzen, um vertrauliche Daten zu stehlen, oder die Verfügbarkeit der Anwendungen zu behindern.

Unabhängigkeit vom Datenspeicherort

In der Cloud können Anwendungen aus Daten bestehen, die aus den unterschiedlichsten Quellen stammen und in den verschiedensten internen und cloudbasierten Datenspeichern abgelegt sind. Dabei ist eine sichere Kommunikation zwischen den verschiedenen Speichern erforderlich. Viele Anbieter von Cloud-Anwendungen haben zwar erheblich in Sicherheitsmaßnahmen investiert, doch bieten Cloud-Dienste den Unternehmenskunden (per Definition) nur beschränkten Einblick in die zugrundeliegende Architektur. Dies macht es für die Kunden schwierig, potenzielle Sicherheitslücken zu ermitteln und zu überprüfen, wie effektiv die Sicherheitsstrategien des Anbieters sind.

Globalisierung ist nicht die Ausnahme, sondern die Regel

Die Cloud lässt regionale und territoriale Grenzen verschwimmen. Daten werden von einem Ort zum anderen übertragen, Nutzer bewegen sich transparent zwischen verschiedenen Ressourcen hin und her und Systeme können von einer Vielzahl autorisierter Parteien verwaltet werden, die nicht unbedingt Mitarbeiter Ihres Unternehmens sind. Das wirft komplexe Fragen der rechtlichen Zuständigkeit auf, macht Authentifizierungen und Nachweise der Vertrauenswürdigkeit erforderlich und erschwert es, die Einhaltung von Vorschriften nachzuweisen.

Hybride Infrastruktur

Kein größeres Unternehmen kann seine internen Systeme über Nacht abschalten, doch bemühen sich die meisten Unternehmen, ihre Ressourcen durch Konsolidierung und Virtualisierung effizienter zu machen. In absehbarer Zukunft werden IT-Infrastrukturen eine Mischung aus traditionellen physischen Rechenzentren und cloudbasierten Technologien bleiben. Und ganz gleich, ob sich Ihre IT-Assets im Rechenzentrum Ihres Unternehmens, oder bei einem Cloud-Anbieter in irgendeinem Teil der Welt befinden – Sie müssen in jedem Fall konsequent Sicherheitsmaßnahmen durchsetzen und Compliance-Dokumentationen erstellen.

Angesichts der Produktivität, Flexibilität und wirtschaftlichen Vorteile von Cloud Computing ist die Reise in die Wolke nicht aufzuhalten – allen Risiken und Komplexitäten zum Trotz. Sehen wir uns deshalb die Herausforderungen näher an, die das Cloud-Zeitalter für jede IT-Organisation mit sich bringt.

Herausforderungen für Sicherheit und Compliance im Cloud-Zeitalter

Sicherheit ist ein Kampf, den Ihr Unternehmen nicht gewinnen kann und der Erfolg bemisst sich in der Regel danach, dass Unternehmen nicht in die Schlagzeilen kommen und die leitenden Mitarbeiter nicht ins Gefängnis. Die verstärkte Nutzung webbasierter Technologien und die zunehmende Einführung neuer Cloud- und Hybrid-Infrastrukturen machen die Arbeit des typischen Sicherheitsmanagers noch komplizierter.

Sicherheit im Cloud-Maßstab

Gemäß Definition der Cloud Security Alliance ist „Rapid Elasticity" (schnelle Anpassbarkeit) eines der wichtigsten Eigenschaften der Cloud. Das bedeutet, dass die Cloud so schnell wachsen kann, wie es für Ihr Unternehmen erforderlich ist. Früher mussten Geräte erst angeschafft, verteilt und installiert werden, was den Unternehmen Zeit gab, für den Schutz der neuen Geräte zu sorgen. Die Bereitstellung einer neuen Cloud-Instanz dauert dagegen nur Minuten. Das erschwert sowohl die Sichtbarkeit (d.h. den Überblick darüber, welche Geräte aktuell vorhanden sind) als auch die Kontrolle (d.h. sicherzustellen, dass die richtigen Konfigurationen und Kontrollen für die neuen Ressourcen implementiert werden).

Wachsende Angriffsfläche

Da sich Webanwendungen immer mehr zum „neuen Perimeter" entwickeln, müssen Unternehmen der Tatsache ins Auge sehen, dass sie heute so viele Perimeter wie Webanwendungen haben. In Kombination mit vermehrtem Outsourcing und geschäftlichen Partnerschaften führt dies zu einer immensen Vergrößerung der Angriffsfläche. Mit der exponentiellen Zunahme der potenziellen Angriffsziele, wie etwa Datenbanken, Desktops, Mobilgeräte, Routern, Servern und Switches, schießt auch die Zahl der Sicherheitslücken in die Höhe, die Hackern den unbefugten Zugriff auf IT-Systeme ermöglichen können. Der Aufbau eines starken Netzwerk-Sicherheitsperimeters reicht nicht mehr aus – auch die Sicherheit der internen Netzwerke und Geräte darf nicht vernachlässigt werden.

Nutzung bestehender Sicherheitskontrollen

Seit jeher setzen viele Unternehmen Nischenprodukte zur Lösung spezifischer Sicherheitsprobleme ein. Dies hat allerdings oft zur Folge, dass ein Unternehmen kein aktuelles, genaues und umfassendes Bild von seinem Sicherheits- und Compliance-Status erhält. Je mehr sich IT-Infrastrukturen hin zu einer Mischung aus On-Premise-, Cloud- und Hybrid-Komponenten entwickeln, desto schwieriger wird es, mit solchen aufgabenspezifischen, hausinternen Sicherheitsprodukten ein komplettes und genaues Inventar der IT-Bestände und Konfigurationen zu erstellen. Ohne ein solches Inventar können Unternehmen ihre Infrastrukturen jedoch nicht wirksam vor den Bedrohungen des Cloud-Zeitalters schützen.

Schutz von „Thin Devices"

Die Entwicklung der Smartphone-Technologie hat komplexere und sicherere mobile Betriebssysteme hervorgebracht, die standardmäßig abgeriegelt sind. Dadurch bieten sie aber auch nur begrenzte Einblicke in und Zugriffsmöglichkeiten auf den Systemkern. Die Malwareschutz-Technologien von gestern, die auf der Kernel-Ebene ansetzen, sind damit nicht mehr relevant. Da die Geräte jedoch weiterhin von Datenlecks und Malware betroffen sind, müssen Unternehmen andere Methoden in Erwägung ziehen, um sie zu schützen.

Priorisierung von Sicherheitsmaßnahmen

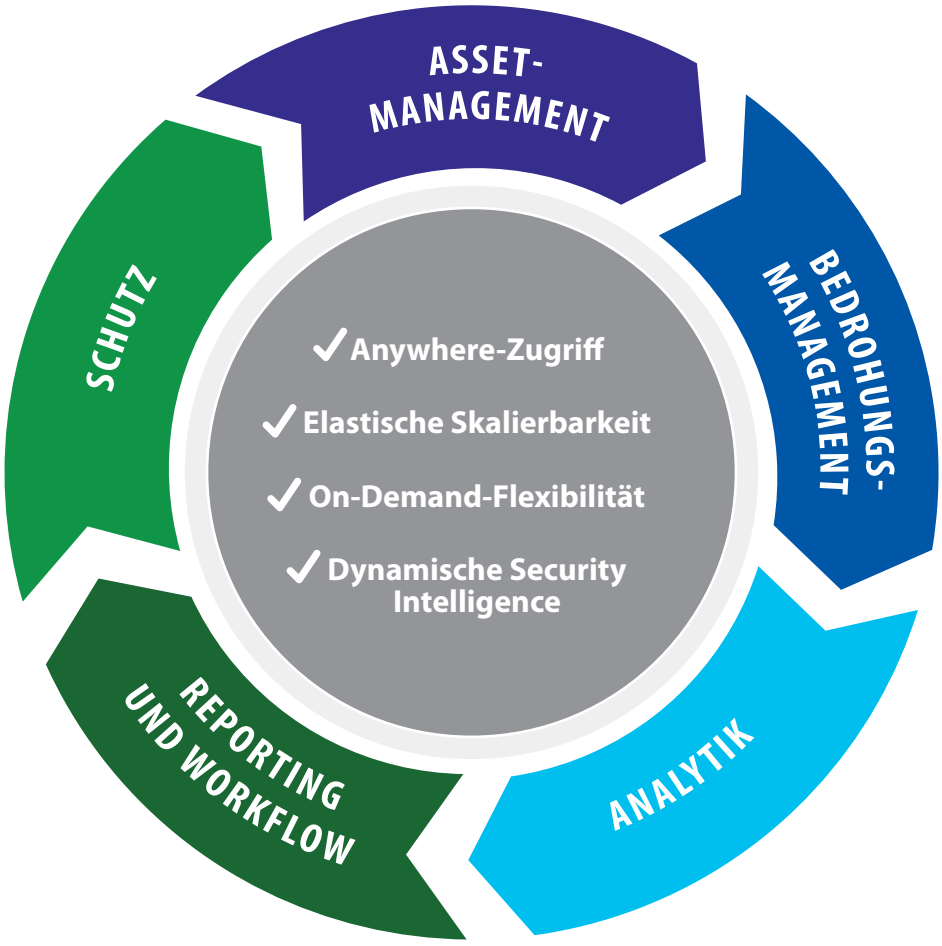
Beschränkte Budgets, Ressourcen und Fachkenntnisse machen es vielen Unternehmen schwer, sich im Cloud-Zeitalter zuverlässig zu schützen. Eine erfolgreiche Sicherheitsstrategie setzt deshalb voraus, dass Unternehmen sorgfältig auswählen, welche Maßnahmen durchgeführt werden sollen. Diese Auswahl wird im Cloud-Zeitalter allerdings noch komplizierter: Heute müssen Sicherheitsmaßnahmen priorisiert werden, die eine Vielzahl interner/externer Dienstleisterund Mitarbeiter einbeziehen, über die die Sicherheitsadministratoren möglicherweise gar keine Kontrolle ausüben können. Erschwerend kommt die Wendigkeit der Angreifer hinzu: Sie können jederzeit eine neue Attacke starten, die sofortiges Eingreifen erfordert und damit alle sorgfältig erstellten Pläne über den Haufen wirft.

Compliance-Berichterstattung

Die Vielzahl der Sicherheitsverstöße hat unter anderem zur Folge, dass das Regelungs- und Compliance-Umfeld immer restriktiver wird. Da Geschäfte im Cloud-Zeitalter überwiegend globaler Natur sind, muss Ihr Unternehmen vermutlich Vorschriften und Richtlinien mehrerer nationaler und lokaler Behörden einhalten, die sich häufig überschneiden und verändern. Die Einhaltung dieser verschiedenen Regelwerke macht kosten- und zeitaufwändige Maßnahmen erforderlich, und wenn sie nicht beachtet werden, drohen erhebliche finanzielle Konsequenzen und Imageverluste. Beispiele für solche externen Regelwerke sind: das Revised International Capital Framework (Basel II), der Health Insurance Portability and Accountability Act (HIPAA), die North American Electric Reliability Corporation Standards (NER), der Payment Card Industry Data Security Standard (PCI DSS), oder der Sarbanes-Oxley Act von 2002 (SOX). Laut einer Gartner-Studie aus dem Jahr 2011 verursacht die Einhaltung von PCI DSS in einem Unternehmen geschätzte Durchschnittskosten von 1,7 Mio. US-Dollar. Und PCI DSS ist nur ein Regelwerk.

Die Cloud-Sicherheitsplattform:

Grundlage für Sicherheit und Compliance im Cloud-Zeitalter



Die heutigen standortgebundenen, vom Kunden selbst betriebenen Lösungen können die Sicherheits- und Compliance-Anforderungen des Cloud-Zeitalters nicht mehr erfüllen. Daher ist eine neue Lösung erforderlich.

Wesentliche Eigenschaften einer Cloud-Sicherheitsplattform:

Anywhere-Zugriff	Elastische Skalierbarkeit	On-Demand-Flexibilität	Dynamische Security Intelligence
Ihre Mitarbeiter, Serviceanbieter und Kunden können sich überall befinden. Daher muss Ihre Cloud-Sicherheitsplattform an jedem Ort und zu jeder Zeit zugänglich sein.	Eine Sicherheits- und Compliance-Lösung für das Cloud-Zeitalter muss so elastisch und skalierbar sein wie die Cloud selbst. Wenn die IT-Infrastruktur Ihres Unternehmens wächst, muss die Plattform, die sie schützen soll, stetig mitwachsen.	Die Sicherheitsplattform für das Cloud-Zeitalter muss flexibel genug sein, um Ihnen nur die Lösungen bereitzustellen, die Sie brauchen; sie nur dann bereitzustellen, wenn Sie sie brauchen; und nur das in Rechnung zu stellen, was Sie tatsächlich nutzen.	Die Cloud-Sicherheitsplattform muss hoch veränderliche, zielgenaue Angriffe abwehren. Daher muss sie laufend mit den aktuellsten Daten zu Schwachstellen, Konfigurationen und Malware aktualisiert werden, damit Ihr Unternehmen schneller auf neue Bedrohungen reagieren kann.

Um den heutigen Unternehmensanforderungen gerecht zu werden, muss die Cloud-Sicherheits- und Compliance-Plattform folgende Leistungsmerkmale bieten:

Asset-Management	Bedrohungs-management	Analytik	Reporting und Workflow	Protection
Unbekannte Assets kann Ihr Unternehmen nicht schützen. Um Prioritäten setzen zu können, muss zudem der Wert berücksichtigt werden, den ein Asset für Ihr Unternehmen hat. Die Plattform muss daher eine robuste Asset-Management-Funktionalität bieten.	Die Plattform muss Schwachstellen ermitteln, Konfigurationen überprüfen und überwachen sowie das Risiko einschätzen können, das ein Angriff für Ihr Unternehmen darstellt. In hybriden IT-Umgebungen muss die Plattform eine einheitliche Sicht bieten, die sowohl das traditionelle Rechenzentrum als auch die Private/Public Cloud-Umgebungen umfasst und zahlreiche Geräte sowie die gesamte Anwendungsschicht einschließt.	Der Schlüssel zur Priorisierung von Aktivitäten und der Bekämpfung hochentwickelter Angriffe sind umsetzbare Informationen aus einer Reihe von Datenquellen. Die Plattform muss diese Daten analysieren und übersichtlich visualisieren, damit die Sicherheits-administratoren schnelle Entscheidungen treffen können.	Angesichts der wachsenden Zahl von Vorschriften in unterschiedlichen Regionen und Rechtssystemen muss die Plattform einheitliche Berichte für das ganze Unternehmen bieten und zugleich alle Berichtspflichten für die verschiedenen Vorschriften unterstützen. Zudem müssen auch unternehmensü-bergreifende Workflows unterstützt werden, da Sicherheitsaufgaben immer häufiger ausgelagert werden.	Wenn es möglich ist, einen Angriff zu blocken und gleichzeitig die False Positives zu minimieren, sollte die Plattform die betroffenen Ressourcen entweder direkt schützen oder sich mit anderen aktiven Abwehrvorrichtungen integrieren können, z.B. Web Application Firewalls, Intrusion-Prevention-Systemen und Firewalls der nächsten Generation.

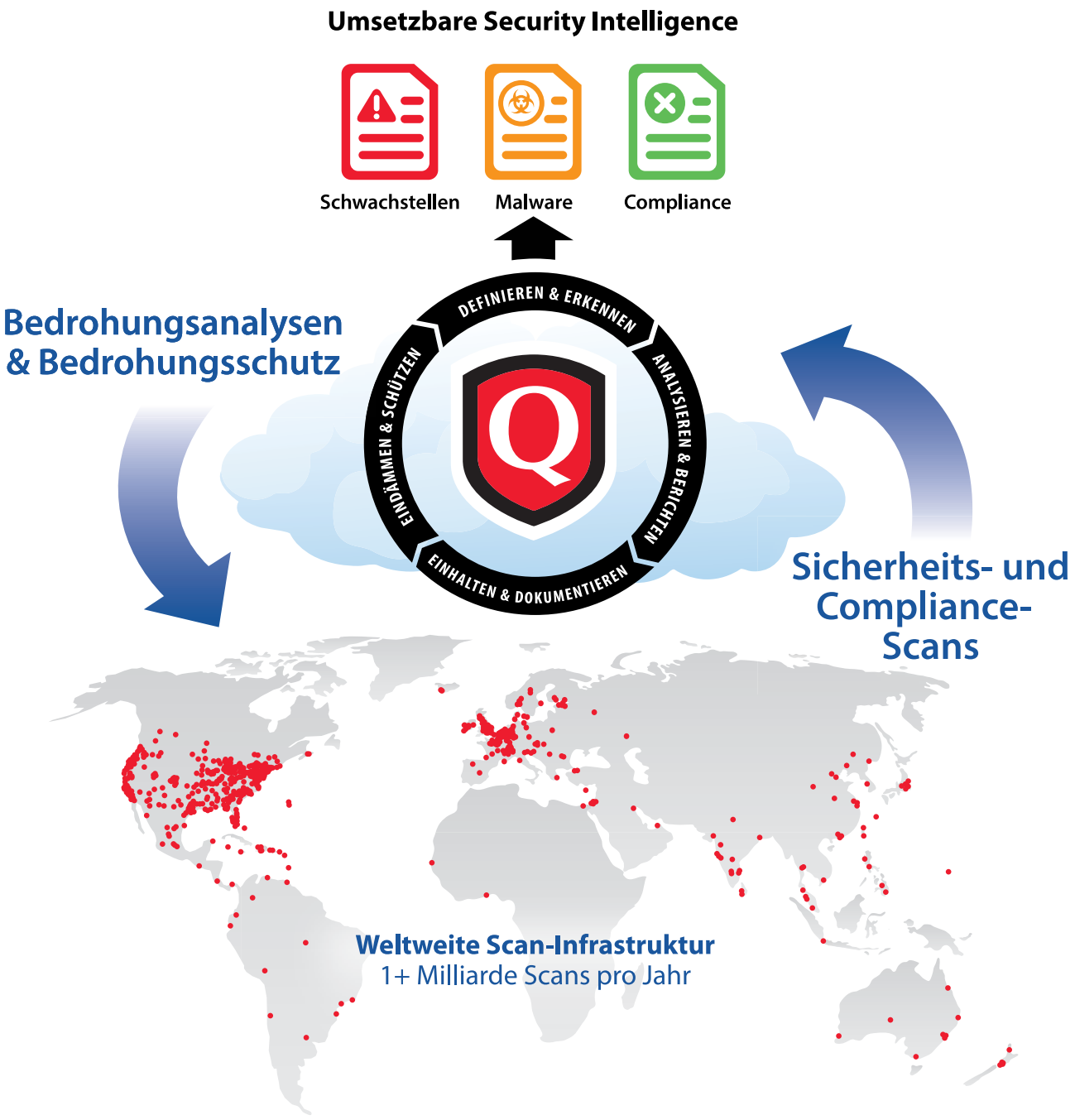
Eine Cloud-Sicherheitsplattform kann nicht über Nacht aufgebaut werden. Es dauert mehr als ein Jahrzehnt, die kritische Masse, globale Präsenz, das herausragende Know-how und die umfassenden Sicherheitserkenntnisse zu erwerben, die eine solche Plattform erfordert. Daher kann nur ein einzigartig qualifizierter Anbieter die Sicherheits- und Compliance-Anforderungen von Unternehmen im Cloud-Zeitalter erfüllen. Dieser Anbieter ist Qualys.

Gewährleistung von Sicherheit und Compliance im Cloud-Zeitalter

Qualys wurde 1999 auf dem Höhepunkt der Technologieblase gegründet, als die Internetsicherheit in den Chefetagen gerade erst zum Thema wurde. Im Dezember 2000 stieg das Unternehmen als einer der ersten Akteure in den Markt für Schwachstellenmanagement ein. Qualys hatte eine außerordentlich präzise und benutzerfreundliche Scantechnologie entwickelt, die über das Web bereitgestellt wird. Als erster Anbieter setzte Qualys das „Software-as-a-Service" (SaaS)-Modell ein, um Unternehmen aller Größen bei der Lösung von Sicherheits- und Compliance-Problemen zu unterstützen.

Das Kernstück der Lösung von Qualys ist die Cloud-Plattform QualysGuard, auf der eine integrierte Lösungssuite aufsetzt. QualysGuard automatisiert den gesamten Lebenszyklus der Asset-Erkennung, Sicherheitsbewertung und Compliance-Verwaltung für die IT-Infrastrukturen und Assets eines Unternehmens – unabhängig davon, ob sich diese innerhalb des Unternehmens, am Netzwerk-Perimeter, oder in der Wolke befinden. Das cloudbasierte Bereitstellungsmodell von QualysGuard ist leicht und schnell im gesamten Unternehmen umsetzbar. Dies gewährleistet eine schnellere Implementierung, umfassendere Einsatzmöglichkeiten und niedrigere Gesamtbetriebskosten als bei herkömmlichen On-Premise-Softwareprodukten für Unternehmen. Durch die Implementierung von QualysGuard erhalten Unternehmen umsetzbare Informationen über potenzielle Schwachstellen und Malware in ihrer IT-Infrastruktur. So können sie internen Richtlinien und externen Vorschriften schneller gerecht werden.

Die Ergebnisse sprechen für sich: In den letzten 12 Jahren hat Qualys einen weltweiten Kundenstamm von mehr als 6.700 Unternehmen in mehr als 100 Ländern aufgebaut. Dazu zählen auch die Mehrzahl der Unternehmen in der Forbes Global 100- und Fortune 100-Liste. Diese Kunden führen mehr als 1 Milliarde IP-Scans / IP-Audits pro Jahr durch.



Das Cloud-Zeitalter wird Unternehmen aller Art und Größe zu mehr Beweglichkeit beim Schutz kritischer IT-Bestände zwingen. QualysGuard liefert praktisch umsetzbare Sicherheitserkenntnisse und ist ideal als langfristige, strategische IT-Sicherheits- und Compliance-Plattform für Unternehmen geeignet.

QUALYSGUARD® Cloud Platform

Die Cloud-Plattform QualysGuard umfasst Lösungen für IT-Sicherheit und Compliance, die auf gemeinsamen, erweiterbaren Kerndiensten und einer hoch skalierbaren Multi-Tenant Cloud-Infrastruktur basieren.

Die QualysGuard Cloud-Infrastruktur

Zur Infrastruktur von QualysGuard gehören die Daten, die analytischen Funktionalitäten, die Software- und Hardware-Infrastruktur sowie die Infrastrukturmanagement-Funktionen, die die Grundlage der Cloud-Plattform QualysGuard bilden. Sie umfasst. Hier einige wesentliche Aspekte:

Skalierbare Kapazität

Die modulare und skalierbare Infrastruktur von QualysGuard nutzt Virtualisierungs- und Cloud-Technologien, damit unser Operations Team innerhalb der gesamten QualysGuard Cloud-Plattform zusätzliche Kapazitäten on demand dynamisch zuteilen kann. Dadurch können unsere Lösungen flexibel wachsen und skalieren.

Indexierung und Speicherung riesiger Datenbestände

Basierend auf unserem sicheren Datenspeichermodell, indexiert die Analyse-Engine von QualysGuard Petabytes an Daten. Sie nutzt diese Informationen, um in Echtzeit Tags oder Regeln anzuwenden und die Eigenschaften von IT-Assets dynamisch zu aktualisieren. Die Tags können in verschiedenen Workflows für Scans, Berichterstattung und Schwachstellenbeseitigung eingesetzt werden.

KnowledgeBase

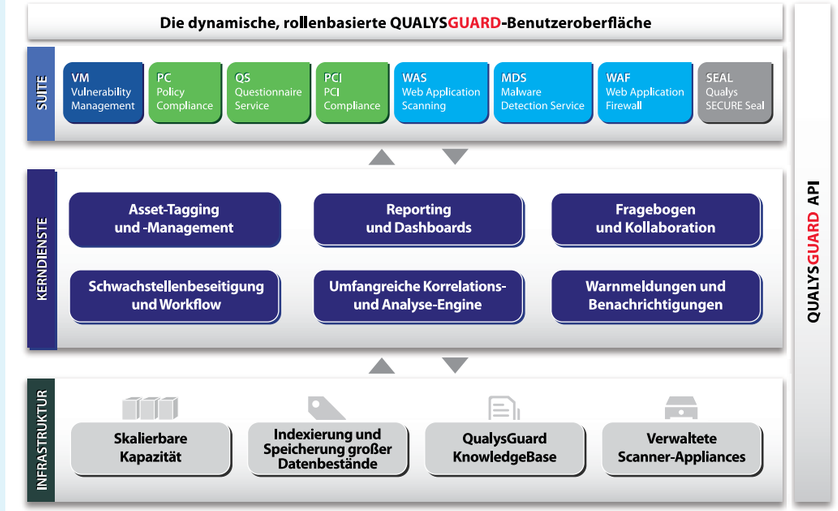
Die QualysGuard KnowledgeBase ist ein umfassendes Repository für bekannte Schwachstellen und Compliance-Kontrollen bei einem breiten Spektrum von Geräten, Technologien und Anwendungen, das als zentrale Informationsgrundlage für unsere Sicherheits- und Compliance-Technologien dient. Die KnowledgeBase wird laufend und dynamisch mit Informationen zu neuen Schwachstellen, Checks für Sicherheitskontrollen, geprüften Fixes und Content-Verbesserungen aktualisiert.

Verwaltete Appliances

Qualys hostet und betreibt weltweit Tausende von physischen Appliances, die die von außen erreichbaren Systeme und Webanwendungen der Kunden analysieren. Zur Überpüfung der internen IT-Assets setzen die Unternehmen in ihren internen Netzwerken entweder physische Appliances oder herunterladbare virtuelle Images ein. Die QualysGuard Appliances aktualisieren sich mithilfe unserer automatisierten, proprietären Management-Technologie transparent selbst.

QualysGuard Kerndienste

Die QualysGuard Kerndienste ermöglichen die integrierten Workflows, das Management sowie die Echtzeitanalysen und-berichterstattung für alle unsere IT-Sicherheits- und Compliance-Lösungen. Zu unseren Kerndiensten zählen:



Asset-Tagging und Asset-Management

Diese Dienste versetzen Ihr Unternehmen in die Lage, große IT-Bestände in hoch dynamischen IT-Umgebungen leicht zu identifizieren, zu kategorisieren und zu verwalten. Sie automatisieren das Inventarmanagement und die hierarchische Strukturierung von IT-Assets.

Reporting und Dashboards

Eine hochgradig konfigurierbare Reporting-Engine liefert Ihrem Unternehmen Berichte und Dashboards auf Basis von Benutzerrollen und Zugriffsrechten.

Fragebogen und Kollaboration

Mithilfe einer konfigurierbaren Fragebogen-Engine kann Ihr Unternehmen leicht bestehende Geschäftsprozesse und Workflows erfassen, um Kontrollen zu evaluieren und Nachweise zur Validierung und Dokumentation von Compliance-Maßnahmen zu sammeln.

Schwachstellenbeseitigung und Workflow

Mit der integrierten Workflow-Engine kann Ihr Unternehmen automatisch Helpdesk-Tickets zur Schwachstellenbeseitigung generieren und Compliance-Ausnahmen anhand unternehmensinterner Richtlinien verwalten. Die Workflow-Engine unterstützt spätere Überprüfungen, Kommentare, Nachverfolgung und Eskalierung. Sie verteilt nach einem abgeschlossenen Scan automatisch Aufgaben zur Beseitigung von Schwachstellen an IT-Administratoren, verfolgt die Fortschritte der Maßnahmen und schließt offene Tickets, sobald Patches installiert wurden und die Behebung der Schwachstellen bei erneuten Scans verifiziert wurde.

Umfangreiche Korrelations- und Analyse-Engine

Eine Analyse-Engine indexiert und durchsucht Petabytes an Sicherheits- und Compliance-Daten und korreliert sie mit anderen Sicherheitsvorfällen sowie Security-Intelligence-Daten aus externen Quellen. Eingebettete Workflows befähigen Ihr Unternehmen, Risiken schnell zu bewerten und auf die nötigen Informationen zuzugreifen, um Schwachstellen zu beseitigen, Ereignisse zu analysieren und forensische Untersuchungen durchzuführen.

Warnmeldungen und Benachrichtigungen

Eine Alert-Engine erzeugt E-Mail-Benachrichtigungen, um die Teammitglieder über neue Anfälligkeiten, Malware-Infektionen, abgeschlossene Scans, geöffnete Trouble-Tickets und System-Updates zu informieren.

QualysGuard Cloud Suite

Bei QualysGuard wählen Sie nur die Lösungen aus, die Sie wirklich benötigen; nehmen sie nur dann in Anspruch, wenn Sie sie wirklich brauchen; und zahlen nur für das, was Sie wirklich nutzen. Ihr Unternehmen kann eine oder mehrere unserer Sicherheits- und Compliance-Lösungen abonnieren und das Lösungsspektrum später erweitern.

Vulnerability Management

QualysGuard VM ist eine branchenführende, preisgekrönte Lösung, die die Netzwerk-Audits und das Schwachstellenmanagement im gesamten Unternehmen automatisiert. Dazu gehören Netzwerkerkennung und Netzwerk-Mapping, Asset-Management, Erstellung von Berichten zu den Schwachstellen und Nachverfolgung der Schwachstellenbeseitigung. Auf Basis unserer umfassenden KnowledgeBase für bekannte Schwachstellen bietet QualysGuard VM kosteneffektiven Schutz vor Sicherheitslücken, ohne nennenswerte Ressourcen in Anspruch zu nehmen.

Policy Compliance

QualysGuard Policy Compliance sammelt und analysiert Konfigurations- und Zugriffssteuerungsinformationen von den vernetzten Geräten und Webanwendungen im Unternehmen und bildet diese Daten auf interne Richtlinien und externe Vorschriften ab, um Compliance zu dokumentieren. QualysGuard PC ist vollständig automatisiert und hilft den Kunden, ihre Compliance-Kosten zu senken, ohne dass Software-Agenten eingesetzt werden müssen.

Questionnaire Service

QualysGuard QS ist eine cloudbasierte Lösung, die die Einleitung, Verfolgung, Prüfung und Genehmigung von Risiko- und Compliance-Bewertungen zentralisiert und automatisiert. Die Lösung senkt den Kosten- und Zeitaufwand beim Einholen von Informationen bei unterschiedlichen Akteuren. Damit hilft sie Unternehmen und Behörden, ihre Programme zur Bewertung von Anbieterrisiken, IT-Risiken und Compliance-Maßnahmen zu vereinfachen und zu erweitern.

PCI Compliance

QualysGuard PCI dient Unternehmen, die Kreditkartendaten speichern, als kosteneffektive und hoch automatisierte Lösung, um die Einhaltung des PCI DSS-Standards zu überprüfen und zu dokumentieren. Mit QualysGuard PCI können Händler den jährlichen PCI-Selbstbewertungsfragebogen ausfüllen und Schwachstellenscans für die vierteljährlichen PCI-Audits und die Prüfung der Webanwendungssicherheit durchführen.

Web Application Scanning

Dank der Skalierbarkeit unserer Cloud-Plattform versetzt QualysGuard WAS Unternehmen in die Lage, alle vorhandenen Webanwendungen zu inventarisieren und zu scannen. QualysGuard WAS scannt und analysiert auch kundenspezifisch angepasste Webanwendungen und ermittelt Anfälligkeiten in den zugrundeliegenden Datenbanken sowie Schwachstellen, die die Zugriffskontrollen für Anwendungen umgehen.

Malware Detection Service

Mit QualysGuard MDS können Unternehmen Malware-Infektionen auf ihren Websites finden und entfernen. QualysGuard MDS führt verhaltensbasierte und statische Analysen durch, um Malware zu entdecken, und überwacht die Websites laufend.

Web Application Firewall

QualysGuard WAF bietet Unternehmen Webanwendungsschutz ohne die Kosten, den Footprint und die Komplexität, die mit Web Application Firewalls auf Appliance-Basis verbunden sind. Die Lösung härtet Webanwendungen über die Standardkonfigurationen und virtuellen Patches hinaus und sichert sie so gegen Angriffe ab. Zudem verbessert QualysGuard WAF die Website-Performance: Mithilfe unseres globalen Netzwerks von Webcaches verkürzt sie die Seitenladezeiten und optimiert die Bandbreite.

Qualys SECURE Seal

Mit QualysGuard SECURE Seal können Unternehmen ihren Online-Kunden demonstrieren, dass sie proaktive Sicherheitsmaßnahmen einsetzen. SECURE Seal scannt auf Malware, ermittelt Schwachstellen in Netzwerken und Webanwendungen und validiert die Integrität von SSL-Zertifikaten. Unternehmen, bei denen keine kritischen Sicherheitsprobleme entdeckt werden, können das QualysGuard SECURE-Siegel auf ihren Websites zeigen.

Warum Qualys?

Qualys hat die Vision, die Art und Weise zu verändern, wie Unternehmen ihre IT-Infrastrukturen und Anwendungen schützen. Qualys ist die beste Wahl, wenn es um Ihre Anforderungen an Sicherheit und Compliance geht.

Bewährte Marke für Cloud-Sicherheit

Qualys ist der Pionier für Cloud-Sicherheit. Im Jahr 2000 führte Qualys die erste Schwachstellenmanagement-Lösung auf Servicebasis ein und hat sich seither als vertrauenswürdiger, objektiver Anbieter von zuverlässigen und präzisen Schwachstellen- und Compliance-Analysen bewährt.

Skalierbare und erweiterbare Cloud-Sicherheitsplattform

Qualys bietet eine hoch skalierbare Cloud-Architektur und modulare Sicherheits- und Compliance-Lösungen. Damit machen wir Unternehmen jeder Größe und Branche Funktionalitäten zugänglich, die ihnen helfen, die Sicherheit ihrer IT-Infrastrukturen zu gewährleisten. Zu den Nutzern unserer Cloud-Plattform zählen kleine Firmen ebenso wie internationale Großkonzerne mit Millionen von vernetzten Geräten und Anwendungen.

Tradition der Innovationen für Cloud-Sicherheit und Compliance

Vor mehr als 12 Jahren stellte Qualys die ersten innovativen cloudbasierten Sicherheits- und Compliance-Lösungen vor, mit denen die Kunden ihre IT-Umgebungen effektiver und kostengünstiger schützen können. Seither haben wir erheblich in die Cloud-Plattform QualysGuard investiert. Damit sind wir stabil aufgestellt, um die Herausforderungen der schnell veränderlichen IT-Sicherheits- und Compliance-Landschaft erfolgreich zu bewältigen.

Nur das bezahlen, was man wirklich nutzt

QualysGuard gibt den Kunden die Möglichkeit, jederzeit leicht und unverbindlich eine oder mehrere Lösungen über einen beliebigen Webbrowser zu testen. Dieses Modell ermöglicht es den Kunden, nur diejenigen Lösungen zu abonnieren, die sie tatsächlich benötigen. Kommen neue Anforderungen hinzu, können sie die Tiefe und Breite ihrer Installation problemlos erweitern.

Für ein Probe-Abonnement der QualysGuard Cloud Suite besuchen Sie bitte www.qualys.com/trials/de/

50+ der Forbes Global 100

nutzen die Security & Compliance Cloud-Plattform von Qualys

8 der Top 10 **Software**

8 der Top 10 **Biotech-Unternehmen**

8 der Top 10 **Technologie**

8 der Top 10 **Einzelhändler**

7 der Top 10 **Medizintechnikhersteller**

7 der Top 10 **Banken**

7 der Top 10 **Medienunternehmen**

7 der Top 10 **Hotels & Restaurants**

6 der Top 10 **Automobilhersteller**

6 der Top 10 **Chemieunternehmen**

6 der Top 10 **Telekomunternehmen**

6 der Top 10 **Mischkonzerne**

QUALYS®
CONTINUOUS SECURITY

Qualys GmbH
Airport Frankfurt – The Squaire
60549 Frankfurt
T: +49 (0) 89 97007 146, info-de@qualys.com

Qualys ist ein internationales Unternehmen mit Standorten auf der ganzen Welt. Um eine Niederlassung in Ihrer Nähe zu finden, besuchen Sie bitte **http://www.qualys.com**