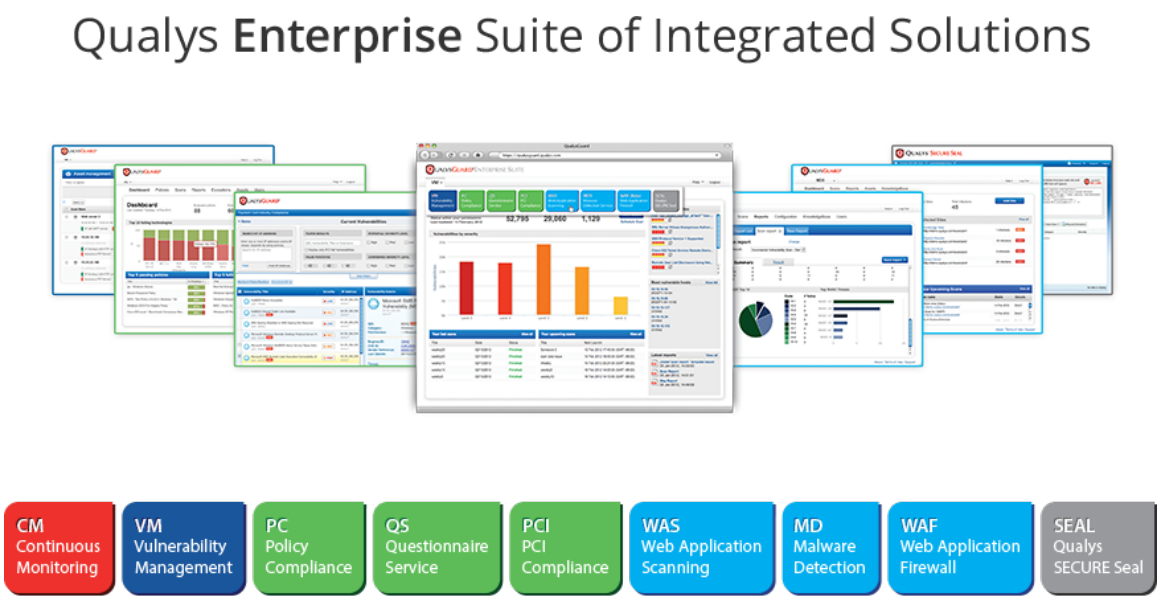
Executive Summary

Qualys permette alla Vostra organizzazione di utilizzare le soluzioni di cui necessita, quando ne ha necessità e solo per quanto effettivamente serve. E' possibile sottoscrivere una o più delle soluzioni ed eventualmente estenderne l'utilizzo nel tempo. La Piattaforma Qualys fornisce le seguenti soluzioni:



Vulnerability Management (VM). Il Vulnerability Management di Qualys è una soluzione leader di mercato che automatizza le funzioni di network auditing e di gestione delle vulnerabilità, includendo funzionalità di network discovery & mapping, asset management, reporting e remediation tracking. Grazie alla più completa knowledgebase di vulnerabilità note Qualys abilita una protezione contro le vulnerabilità note senza richiedere un significativo uso di risorse.
Continuos Monitoring (CM). Costruita sopra la soluzione di Vulnerability Management il Continuos Monitoring è un servizio cloud innovativo che controlla la rete alla ricerca di minacce e cambiamenti inattesi, prima che si traducano in violazioni. Ogni volta che viene riconosciuta un'anomalia viene avvisato il personale incaricato esattamente di quel sistema.
Policy Compliance (PC). La soluzione di Policy Compliance consente di raccogliere e analizzare le informazioni relative alle configurazioni dei sistemi correlandoli con le politiche ed i regolamenti in essere, in modo da documentare effettivamente la conformità rispetto alle regole. Si tratta di un sistema totalmente automatizzato che

aiuta a ridurre i costi della gestione della compliance senza richiedere necessariamente l'utilizzo di agenti.
Questionnaire (QS). Il Questionnaire è un servizio di immediato utilizzo ma particolarmente potente per automatizzare il workflow. Include la capacità di centralizzare ed automatizzare il risk assessment, raccogliendo ed archiviando le evidenze da impiegati o partner, controllando il progresso del processo di assessment.
PCI Compliance (PCI). Qualys PCI offre alle organizzazioni che registrano i dati dei proprietari di carte una soluzione efficace ed economica, oltre che altamente automatizzata, per verificare e documentare la conformità rispetto alla normativa PCI DSS.
Web Application Scanning (WAS). La nota ed apprezzata scalabilità dei servizi Qualys permette di scoprire, catalogare e scansionare tutte le applicazioni web presenti in un'organizzazione, identificando quelle vulnerabilità che minacciano i database piuttosto che il controlo degli accessi.
Web Application Firewall (WAF). Il Web Application Firewall di Qualys è una soluzione di livello enterprise che protegge le applicazioni web interagendo dinamicamene con il sistema WAS.
Qualys ThreatProtect (TP). Nuove vulnerabilità sono scoperte di continuo, diverse migliaia ogni anno. Non tutte le vulnerabilità però sono identiche: la correlazioni delle informazioni di intelligence arricchisce le informazioni utilizzabili per prioritizzare le azioni nei confronti delle vulnerabilità.

Vantaggi operativi e tecnici della piattaforma Qualys

Il modello SaaS (Software as a Service) fornisce diverse vantaggi che sono illustrati nei prossimi paragrafi. Combinati con il vantaggio derivante da una sicurezza End-to-End, alla superiore tecnologia di scansione, al robusto sistema di reporting e data modeling, alla semplicità di gestione ed alla disponibilità di una completa e ben documentata API questo costituisce la soluzione più completa ed economicamente efficace disponibile oggi sul mercato.

La piattaforma Qualys, Software as a Service

Qualys ha iniziato ad erogare la propria piattaforma in forma di software as a service oltre 18 anni fa, e da allora è leader per facilità di deployment e scalabilità.

Facilità di utilizzo

La piattaforma Qualys può essere attivata in minuti e utilizzando gli scanner on premise consente di estendere il controllo alle reti interne. Questi scanner possono

essere forniti in forma di scanner hardware, virtuali o agenti; sono distribuiti da remoto, gestiti centralmente e si auto aggiornano.

Qualys Scanner

Gli Scanner Qualys sono in effetti l'unica parte dell'archiettura che richiede un minimo di configurazione (almeno l'inserimento di un codice seriale od eventualmente la configurazione di rete quando non sia erogata via DHCP).

Qualys Cloud Agent

Il Cloud Agent permette di estendere la sicurezza attraverso ogni componente dell'azienda. Questi agenti leggeri (2MB) sono distribuiti da remoto, gestiti centralmente e si aggiornano autonomamente consumando poche risorse (massimo 5% al picco, meno del 2% normalmente e 0,01% quando inattivi). Gli Agenti possono essere distribuiti in numero illimitato senza costi di licenza al fine di mantenere le migliori e più aggiornate informazioni per il sistema di Asset Management.

Basso costo di possesso (TCO)

Il modello SaaS consente di ottenere un TCO inferiore e predicibile. Ci sono infatti molti costi che devono essere considerati valutando soluzioni altrimenti distribuite: costi legati al deployment, alla gestione, alla manutenzione e poi quelli accessivi relativi ai sistemi operativi, al loro hardening, alle licenze aggiuntive etc. La piattaforma Qualys fornisce invece:

- appliance che non richiedono manutenzione
- nessun software da installare e mantenere
- nessun database da installare, gestire e per il quale effettuare capacity planning
- nessun backup da gestire
- nessun costo di personale per manutenere l'infrastruttura di scansione
- aggiornamenti totalmente automatizzati
- training gratuito (fisico o online) con certificazione erogato da personale Qualys
- Supporto globale 24x7x365
- Nessun costo nascosto

La sottoscrizione del servizio include la copertura di tutto quanto necessario per effettuare il deployment e la gestione della soluzione. Questo include tutti i csti di gestione/manutenzione delle applicazioni, della piattaforma, della parte hardware, dei database e di tutto quanto elencato qui sopra. Gli analisti di mercato, a partire da Gartner, riconoscono a Qualys il fatto di erogare una soluzione caratterizzata dalla

miglior qualità disponibile, con un TCO basso ed una struttura di costi totalmente predicibile.

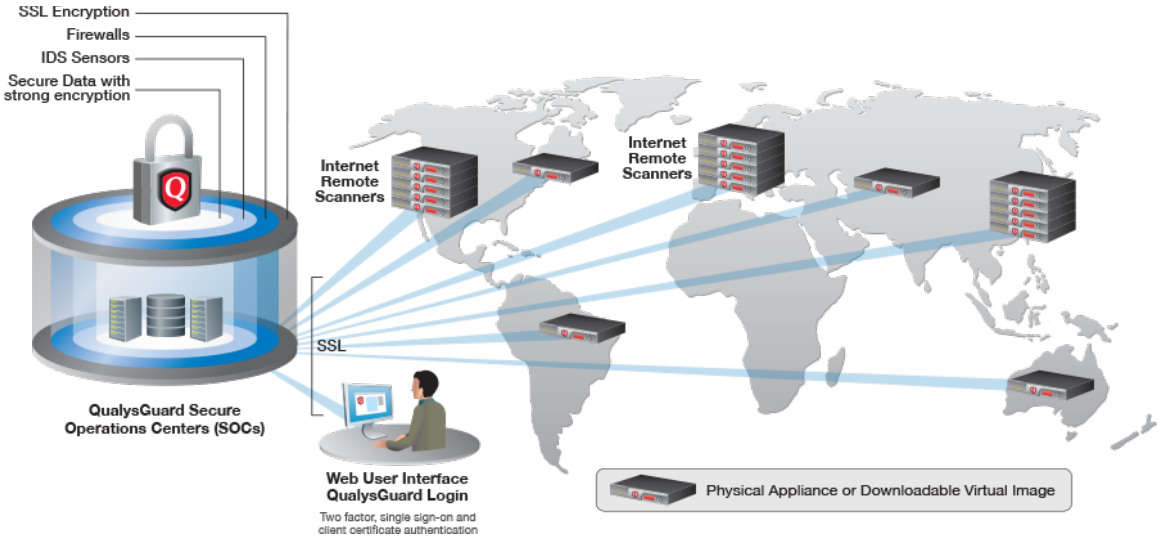
Mappa dei centri di supporto Qualys:

Parallel/Load balanced scanning.
Al fine di offrire la miglior scalabilità la piattaforma Qualys permette di sfruttare funzionalità di scansione parallelizzata (cioè distribuendo una scansione tra diversi device). Inoltre è possibile eseguire contemporaneamente diverse scansioni su diversi device.

End to end security.

La piattaforma Qualys cifra i dati end-to-end, in transit ed in storage. Tutte le interazioni con la piattaforma (interattive o via API) avvengono in HTTPS (TLS v1.2), utilizzando solo le combinazioni di cifratura più robuste. La piattaforma Qualys non supporta alcuna forma di comunicazione in chiaro per alcuna operazione.
Tutte le comunicazioni tra gli Scanner e la piattaforma sono cifrate in TLS o in SSH incapsulato in TLS. Questo meccanismo consente di fornire la forza di un tunnel ssh con una chiave a 2048 bit e la flessibilità di una connessione https in uscita. In questo modo non sono necessarie modifiche significative all'infrastruttura di

sicurezza perimetrale ed è possibile supportare i web proxy con o senza autenticazione.
Tutti i dati relativi alle vulnerabilità sono cifrate per cliente e registrati utilizzando un algoritmo AES con una chiave generate casualmente per ogni account. Questo garantisce che solo il personale autorizzato possa accedere ai dati delle scansioni. La chiave utilizzata per decifrare le informazioni vulnerabilità è sbloccata durante il processo di login dell'utente (one-way hash). La piattaforma non scrive mai la chiave su disco in chiaro e non la memorizza altrove che in RAM, pertanto le informazioni sono cifrate prima di essere registrate nel database. Per questo nessun impiegato Qualys e nessuna applicazioni hanno accesso logico ai dati delle vulnerabilità del cliente.



Self improving.

Come Qualys misura e risolve i difetti (cioè i falsi positivi) è un elemento di differenziazione particolarmente rilevante. I falsi positivi hanno il più alto livello di priorità a livello di supporto ed engineering. Tipicamente vengono immediatamente sottoposti a validazione ed al processo di rimedio attraverso un processo formalizzato di Q&A. Il risultato, ovvero la "signatura" migliorata viene implementato in produzione nell'arco di pochi giorni. La centralizzazione della Knowledgebase consente di portare il miglioramento istantaneamente a tutti i clienti. Questo spiega la natura "self improving" del sistema ed il costante aumento di clienti della piattaforma.

Tecnologia di scansione

La piattaforma Qualys utilizza un motore di scanning basato su inferenze che è significativamente diverso dalle tecnologie convenzionali (tree-based). Il sistema

procede iniziando con un accurato inventario di sistema operativio protocolli, porte e servizi sulla macchina oggetto di scansione. Questo inventario viene utilizzato per alimentare un sistema esporto che sceglie l'insieme appropriato delle vulnerabilità da controllare tra centinaia di moduli disponibili. Il risultato è un test su misura per ogni singolo oggetto di analisi. Questo significa che l'utente non ha bisogno di conoscere nel dettaglio i sistemi da analizzare. Inoltre questo significa che, ad esempio, se il web server è basato su IIS verranno testate le vulnerabilità di IIS e non quelle di Apache, con evidenti benefici.

Accuratezza nell'analisi dei servizi

Durante una scansione Qualys effettua la scansione delle porte TCP, UDP e RPC seguita da una serie di attività denominate di Service Discovery. Questa identifica ogni porta come aperta o filtrata e determina in modo intelligente il tipo di applicazione, il vendor e la versione (quando possibile) combinando diverse tecniche attive senza affidarsi ai soli banner. Questa è una delle ragioni della maggior accuratezza fornita dalla soluzione Qualys.

Efficienza.

L'efficienza della scansione viene misurata da Qualys sulla base di diversi elementi: bilanciamento delle risorse e delle performance, impatto sulla rete e sugli host, accuratezza e completezza dei risultati. Non certo e non solo la velocità di esecuzione piuttosto che il numero di controlli dichiarati apoditticamente.
Il motore ad inferenze logiche è stato progettato per effettuare scansioni che possano coniugare accuratezza, precisione e performance. La piattaforma Qualys in particolare controlla le performance della rete durante la scansione e nel momento in cui, per un qualsiasi motivo, i tempi di risposta degradano allora la velocità di scansione viene diminuita aumentando l'intervallo tra i pacchetti generati relativamente ai test che stanno subendo il ritardo.
L'altro elemento di particolare rilevanza utile a valutare l'efficienza è la completezza del database delle vulnerabilità. La knowledgebase di Qualys copre non solo tutti i principali sistemi ma anche il maggior numero di di sistemi operativi, embedded device e applicazioni.

Reporting & data model

Molti sistemi di vulnerability scanning richiedono che le opzioni per il reporting siano configurate prima di lanciare la scansione. Se il report richiede modifiche allora e' necessario ripetere una nuova scansione. Con la piattaforma Qualys il reporting e' indipendente dalla scansione. Il sistema basato su modelli (template) permette di fare data-mining analogamente a quanto si farebbe con un database SQL.

Risultati per scansione e per host.

Qualys registra tutti i dati della scansione per scansione e per asset (tracciabile per ip, nome NetBIOS o nome DNS). Anche se altre soluzioni consentono di modificare il formato del report queste normalmente registrano i dati solo per scansione il che ne limita notevolmente le capacità. Combinare i risultati di diverse scansioni in un singolo report può essere fatto facilmente ma combinare i risultati della scansione 1 sul host A, della scansione 2 sugli host B e C, della scansione 3 sugli host D, E, F e G diventa pressochè impossibile. La piattaforma Qualys invece permette di combinare diverse scansioni in un singolo report ovvero diverse scansioni di uno stesso host in un report che ne mostra l'andamento storico.

Consolidamente automatico

La piattaforma Qualys è stata volutamente progettata per effettuare attività distribuite di scansione mantenendo una gestione centralizzata con un reporting consolidato delle vulnerabilità (e della compliance). Tutti i dati della scansione, indipendentemente dalla sorgente, vengono mandati alla piattaforma in modo sicuro e automaticamente consolidati in un singolo database sicuro e gestito. Per altri vendor questo e' un problema legato al fatto che le soluzioni nascono basate sul singolo scanner ed il consolidamente avviene artificiosamente posteriori, come dimostrato da motori di reportistica particolarmente complessi ed onerosi in termini di gestione.

Report personalizzati e collaborazione

La piattaforma offre un sistema di reporting basato su modelli che può produrre report tecnici altamente dettagliati, ovvero scorecard ideali sintetiche ideali per il management, molto velocemente e semplicemente. La piattaforma include un gran numero di modelli standard e gli utenti possono modificarli a piacere. Le funzionalità di trending del sistema di reporting a livello dell'organizzazione consentono di tracciare i progressi per processo di gestione delle vulnerabilita' nel tempo ed accuratamente. Tutti gli elementi grafici o testuali possono essere inclusi od esclusi singolarmente. Ci sono diverse opzioni di ordinamento e di selezione dei dati (es. solo le vulnerabilità critiche). Altre soluzioni richiedono esperienza e padronanza del linguaggio SQL per estrarre le informazioni direttamente dai database!

La piattaforma include anche un Report Center, una piattaforma collaborativa che consente di archiviare i report ed automatizzarne la distribuzione. Via API e' possibile pianificare la generazione dei report ed automatizzare il reperimento del report desiderato. I report possono essere generati e scaricati in diversi formati, inclusi PDF, HTML, MHT, CSV e XML.

Tracciamento dello stato delle vulnerabilità

La piattaforma Qualys normalizza automaticamente i dati provenienti dalle scansioni per tracciare il ciclo di vita delle vulnerabilità dal momento della loro scoperta fino alla loro risoluzione sul singolo host. Gli stati delle vulnerabilità sono: New, Active, Re-Opened e Fixed. Questa e' una funzionalità chiave che consente di non perdere di vista quelle vulnerabilità che potrebbero non essere state cercate con l'ultima scansione, e non per questo possono considerarsi risolte o svanite.

Patch Supercedence

Qualys pone molta attenzione nell'analizzare le informazioni provenienti dai diversi vendor, in particolare per verificare se una nuova "patch" renda obsolete quelle precedenti. Questo consente al cliente di non sprecare tempo nel cercare di identificare quale "patch" tra quelle disponibili possa risolvere il problema. Questo elemento e' reso evidente nel "Patch Report" che consente di identificare velocemente quali "patch" risolvano il maggior numero di problemi.

Amministrazione

La piattaforma Qualys include funzionalità chiave che riducono notevolmente il tempo necessario per la sua amministrazione e configurazione. Oltre al sistema di reporting basato sui modelli descritto in precedenza le "Search List" sono un'ulteriore feature che fornisce efficienza rispetto ad altre soluzioni. Queste possono essere infatti applicate agli "option profile" che guidano la scansione, ai modelli dei report ed alle regole di remediation che servono ad aprire automaticamente i ticket. Si tratta di metodi per la selezione delle vulnerabilità che una volta configurati si aggiornano dinamicamente applicando i medesimi criteri alle nuove vulnerabilità.

Configurazione modulare.

La piattaforma Qualys include diverse funzionalità che riducono la quantità di lavoro necessaria per effettuare compiti ripetitivi. Per esempio quando si configurano diverse scansioni "option profile" e "search list" posssono essere riutilizzati, questo significa che quando fosse necessaria una modifica questa si riflettera' su tutte le scansioni senza bisogno di ripeterla meccanicamente "n" volte ed il cambio si propagherà a tutte le scansioni programmate o future.

Gestione gerarchica degli utenti

L'organizzazione può fornire accesso ai dati sfruttando il sistema gerarchico di role-based administration:

- *Manager*, Security Manager
- *Unit Manager*, laddove si utilizzi un modello con Business Unit
- *Scanner*, Security Manager, operatori
- *auditor*, Auditor che hanno necessità di accedere ai report
- *Reader*, chi abbia bisogno di accesso in sola lettura quali auditor, executive, system owners, business owners..
- *Contact*, tipicamente network operations

Questo organizzazione consente al team di security di delegare compiti e fornire strumenti che consentono di migliorare i processi di gestione delle vulnerabilita' e della compliance.

Asset Groups

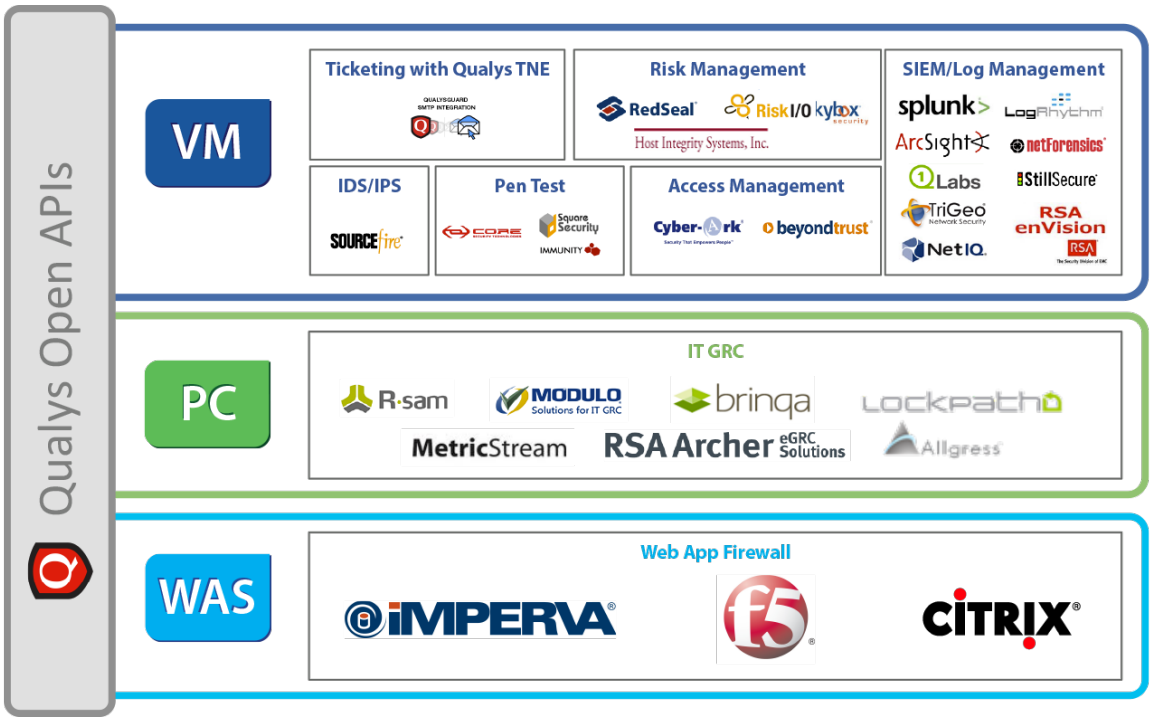
Gli Asset Group consentono una grande flessibilità nella gestione della propria organizzazione: si possono configurare diversi Asset Group su di un singolo device in modo che questi dati siano utilizzabili in fase di scansione, reporting o ticketing.

Risk based vulnerability severity

Qualys consente ai propri clienti di ignorare globalmente o su singoli host determinate vulnerabilità, cosí come di cambiarne il rating. Questa funzionalità è offerta nel sistema e non richiede servizi professionali o di personalizzazione.

Qualys API - Integrazione con terze parti

l"API di Qualys e' ampiamente e pubblicamente documentata. Basata sullo standard XML consente a clienti e terze parti di creare modi unici per lavorare i dati ed integrarli in altre aree operative. In particolare la nostra soluzione aperta e' cosi' apprezzata e pratica che un almeno un competitor ha scelto di copiarla verbatim.



Molti leader di mercato hanno scelto di integrare i loro prodotti con la piattaforma Qualys per offrire valore aggiunto a soluzioni ben apprezzate. Una lista completa delle partnership tecnologiche e' disponibile su
http://www.qualys.com/partners/solution-technology/