QUALYSGUARD® VULNERABILITY MANAGEMENT

VERZE ENTERPRISE

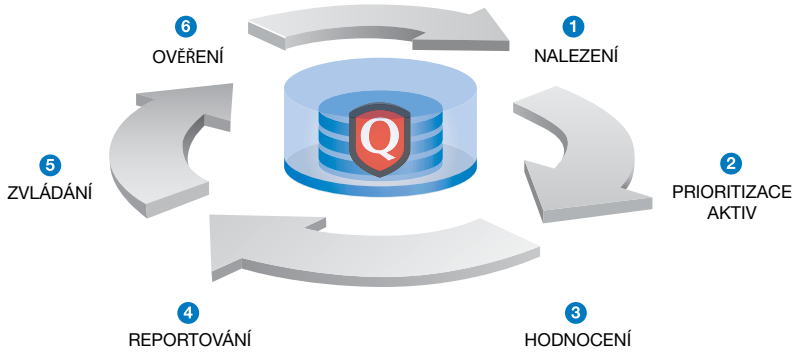
ZPROVOZNĚTE ŘÍZENÍ ZRANITELNOSTÍ A RIZIK IS — SLUŽBA NA VYŽÁDÁNÍ

QualysGuard® Vulnerability Management (VM) automatizuje auditování počítačových sítí a řízení technických zranitelností ICT infrastruktury v rámci celé organizace, a to včetně mapování sítě, prioritizace aktiv, reportování míry zranitelností a řízení nápravy dle skutečných rizik. Díky QualysGuard Vulnerability Management mohou bezpečnostní manažeři auditovat, prosazovat a dokumentovat bezpečnost sítí podle interních směrnic a externích regulatorních požadavků. Navíc není zapotřebí pořizovat a spravovat žádnou speciální infrastrukturu díky formě software-jako-služba (SaaS - Software-as-a-Service).

QualysGuard Vulnerability Management pro velké a rozsáhlé organizace

QualysGuard VM umožňuje organizacím efektivní správu zranitelností a kontrolu nad bezpečností jejich IS pomocí centralizovaného reportování, návrhu nápravných opatření a plného řízeného procesu nápravy zranitelností za pomoci tzv. trouble tiketů. QualysGuard poskytuje komplexní reportování zjištěných zranitelností včetně ohodnocení jejich závažnosti, možného negativního dopadu a stanovení lhůty pro nápravu. K tomu je možné sledovat analýzy trendů v bezpečnostních oblastech.

Životní cyklus QualysGuard Vulnerability Management



Výhody QualysGuard Vulnerability Management:

- Snížení rizik díky automatické identifikaci zranitelností a prioritizaci nápravných opatření založené na aktuální úrovni rizik.
- Auditování a testování ICT bez instalace agentů, vysoké zabezpečení auditních záznamů proti změnám a jistota, že budou v souladu s požadavky třetích stran.
- SaaS technologie nabízí významné ekonomické výhody, bez dalších nákladů na lidské zdroje a na pořízení a údržbu infrastruktury pro testování zranitelností.
- Velká škálovatelnost, snadnost a pružnost nasazení je ideální pro velké a rozsáhlé společnosti.
- Rychlá identifikace, vizualizace a organizace aktiv IS do skupin a jednotlivých oddělení usnadňuje jejich správu.

Qualys má tisíce zákazníků po celém světě, pokrývá více než 35 firem z žebříčku Fortune Global 100 největších firem světa a má světově největší podíl ve FORTUNE 50. S více než 223 testovacími zařízeními instalovanými v 53 zemích světa a skenujícími přes 700 000 systémů má Qualys největší celosvětové řešení pro řízení zranitelností ICT.

"QualysGuard učinil auditování naší sítě mnohem jednodušší. Dříve jsme se museli dlouze probírat výsledky a dělat mnoho manuálních analýz k vytvoření smysluplných zpráv, které pak ani nebyly konzistentní."

Chris Lalonde, Senior Manager of Information Security
eBay

"QualysGuard nám umožňuje spouštět bezpečnostní audity kdykoliv je třeba, rozpoznat zranitelnosti ihned, jak jsou přidány do databáze, a aktivně pracovat na jejich odstranění. To nám pomáhá zabezpečit všechna přístupová místa do sítě, prosadit bezpečnostní politiku společnosti ICI a dosáhnout shody s federálními požadavky."

Paul Simmonds, Director of Global Information Security
ICI

SC MAGAZINE AWARDS 2008 WINNER

– QualysGuard byl dva roky po sobě vyhodnocen jako Nejlepší řešení pro auditování a řízení zranitelností.

Vlastnosti QualysGuard Vulnerability Management:

Centralizované řízení technických zranitelností ICT

- Automatické a centralizované reportování distribuovaných skenů.
- Společná správa interního a externího (z internetu) skenování sítí.
- Přehledný ovládací panel (dashboard) pro vedoucí pracovníky.
- Portálové řešení založené na interaktivním vyhledávání aktiv.
- Autorizovaný přístup z jakéhokoliv místa.
- Export reportů do formátů HTML, MHT, PDF, CSV a XML.

Automatizace

- Plánování skenů a mapování sítě.
- Každodenní automatické aktualizace databáze zranitelností.
- Automatické generování trouble tiketů a jejich kontrola.

Interní skenovací zařízení QualysGuard Scanner Appliance je snadno použitelným řešením pro skenování rozsáhlých sítí, přičemž nasazení je otázkou minut.

Přesnost

- Vyčerpávající databáze zranitelností disponuje tisíci unikátními testy.
- Důvěryhodné auditování a certifikace bezpečnosti díky auditním zprávám zabezpečenými vůči modifikaci nebo podvržení.
- Nedestruktivní technika skenování se schopností odvodit netestované nebezpečné zranitelnosti bezpečným způsobem.
- Skenování s autentizací i bez.
- Interní a externí testování poskytuje komplexní pohled na zranitelnosti celého systému.
- Konfigurovatelné možnosti skenování pro speciální audity a testy.
- Podpora více než 2 000 operačních systémů, aplikací a protokolů.

Reportování

- Nastavitelné možnosti reportů pro manažery a vedoucí pracovníky.
- Reporty sledující stavy, vývoj v čase, změny a trendy.
- Reporty o nápravě zranitelností: sledování stavu tiketů podle skupin aktiv, uživatelů a zranitelností.
- Srovnávací stavové reporty pro všechny zainteresované strany.
- Automatické generování a rozesílání reportů.
- Různé možnosti distribuce reportů včetně šifrovaných PDF.

Škálovatelnost / Využitelnost

- Technologie typu SaaS umožňuje rozsáhlé globální skenování bez použití dodatečné infrastruktury.
- Rychlé skenování díky řízení zátěže skenovacích zařízení.
- Definovatelná struktura uživatelů a skupin aktiv, dle požadavků na správu a provoz ICT.
- End-to-end šifrování zjištěných informací o zranitelnostech.
- Hierarchické rozdělení uživatelských rolí umožňující delegování odpovědností podle organizační struktury společnosti.
- Proces nápravy zranitelností založený na definovaných pravidlech s automatickým generováním a přiřazováním trouble tiketů.

Propojitelnost

- Rozšiřitelná XML API knihovna a rozhraní.
- Existující integrace typu out-of-the-box s předními řešeními v oblasti SIM (Security Information Management).
- Integrace se systémy HelpDesk a ServiceDesk.
- Integrace se systémy Patch Management schopná automatizovat nápravu.
- Podpora hodnocení zranitelností dle standardu Common Vulnerability Scoring System (CVSS).
- Podpora tvorby vlastních definic zranitelností dle standardu Open Vulnerability Assessment Language (OVAL).

Podpora / správa

- Zákaznická nonstop podpora 24/7/365.
- Každodenní automatická aktualizace nových zranitelností a aktualizace nových funkcí probíhá vzdáleně a transparentně směrem k zákazníkovi.
- Probíhající zákaznická školení po webu.
- Technická školení a certifikační workshopy.

Ceny

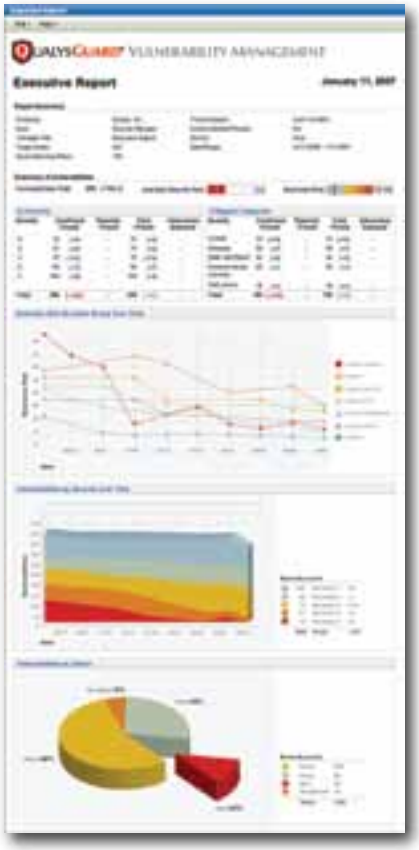
- **Roční licence:** pro neomezené množství testů předem definovaného počtu IP adres je ideální volbou pro pravidelné hodnocení bezpečnosti aktiv IS a zavedení procesu Řízení zranitelností (Vulnerability Mng.).
- **Licence Per Scan:** pro flexibilní, nárazové použití QualysGuard ve společnostech s požadavky na čtvrtletní nebo nepravidelné skenování.

QualysGuard Vulnerability Management je dostupný také jako součást QualysGuard Security & Compliance Suite, který zahrnuje:

- **QualysGuard Vulnerability Management**
- **QualysGuard Policy Compliance**
- **QualysGuard PCI Compliance**
- **QualysGuard Web Application Scanning**

Pro více informací navštivte www.qualys.cz

Nastavitelný ovládací panel (dashboard) dle potřeb každého uživatele.



Report vývoje provozních rizik IS v čase.

Risk Analysis Consultants, s. r.o.
Španělská 2
120 00 Praha 2
Česká republika
telefon: +420 221 628 400
fax: +420 221 628 401
email: qualys@rac.cz
www.rac.cz

Risk Analysis Consultants je nezávislá poradenská společnost poskytující služby a řešení ve všech oblastech bezpečnosti informací v souladu s mezinárodními normami, související národní legislativou a respektováním individuálních podmínek klientů. Od roku 1995 pomáhá zajišťovat bezpečnost informací v informačních systémech organizací státní správy, bank, finančních institucí, telekomunikačních společností a průmyslových podniků v České republice i v zahraničí.

QUALYS®
www.qualys.com