Risk Management and Threat Visualization with QualysGuard and RedSeal

> *"We are pleased to see these two providers of proactive security come together in what is a natural technology partnership. The merging of Qualys' results with RedSeal's appliance makes high priority risk information quick and easy to identify, significantly reducing our time to remediation. It allows our security team to focus on keeping our systems as secure as they can be."*
>
> Brad Robinson, Security Manager
> **Postini Inc.**

Integration of Redseal SRM with QualysGuard gives enterprises the ability to model their network topology, determine what vulnerabilities are present on their network and understand which vulnerable systems can actually be accessed based upon the network traffic filtering policies. All of this information is used to ultimately measure risk for asset groups and prioritize remediation.

Assess Exposure of Business Assets

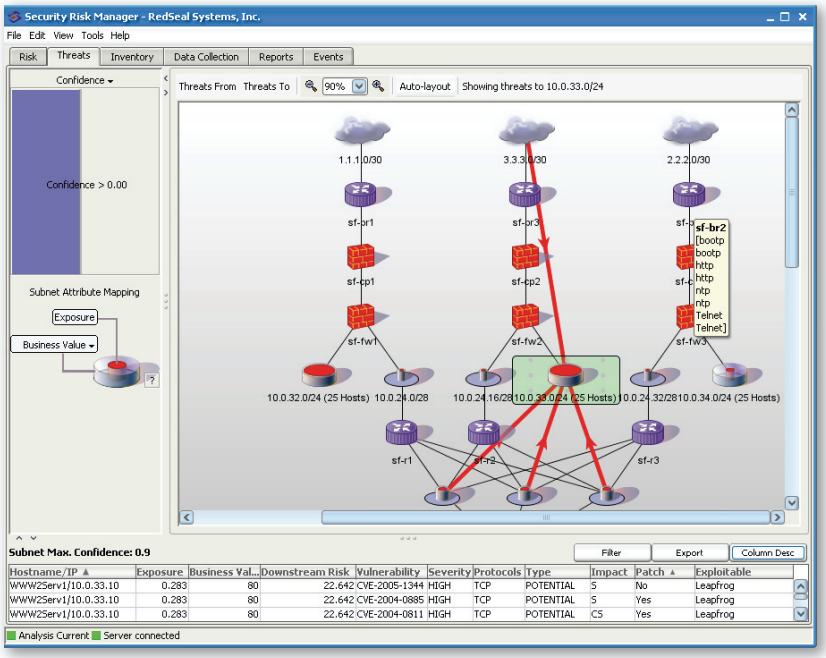
QualysGuard excels at detecting vulnerabilities on any device connected to the network. When these vulnerabilities are overlaid on the network topology and traffic flow model generated by Redseal SRM, the exposure of business assets to threats can be determined. This allows an enterprise to assess its security posture.

Mitigate Threats

The integration allows an enterprise to identify systems and networks that pose the highest threat to business assets. These threats can then be mitigated through traffic filtering and patching of vulnerable systems.

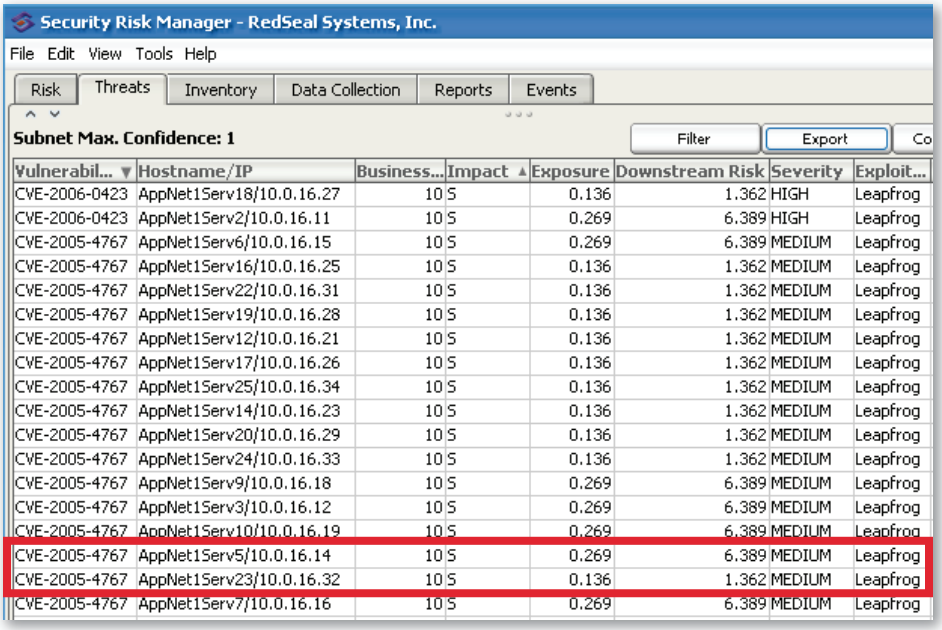
Prioritize remediation of vulnerabilities

A mature security process requires remediation of all vulnerabilities within an enterprise. However, several factors such as lack of resources, pre-production staging procedures and compatibility issues can delay the remediation process. A risk analysis performed using QualysGuard and Redseal SRM determines the actual risk posed by vulnerabilities to an enterprise. This enables the enterprise to focus its resources on mitigating vulnerabilities that provide the greatest reduction in risk.



How it Works

Integration of Redseal SRM with QualysGuard allows customers to import QualysGuard scan reports of their network into Redseal SRM using QualysGuard API or XML reports. Redseal SRM collects configuration files from networking devices such as routers, firewalls and switches. This configuration information in conjunction with the host and application information from QualysGuard is used to model a network map of the enterprise. Networks which the enterprise has little or no control over, such as guest networks or even the Internet can be categorized as untrusted. The threat that untrusted sources pose to business assets can then be analyzed based on the vulnerabilities (reported by QualysGuard) on intermediate systems and the traffic filtering policies (ACLs) between the systems. Interactive threat and risk maps can be used to visualize the threat of untrusted sources and vulnerable systems to other assets.



Vulnerabil...	Hostname/IP	Business...	Impact	Exposure	Downstream Risk	Severity	Exploit...
CVE-2006-0423	AppNet1Serv18/10.0.16.27	10	S	0.136	1.362	HIGH	Leapfrog
CVE-2006-0423	AppNet1Serv2/10.0.16.11	10	S	0.269	6.389	HIGH	Leapfrog
CVE-2005-4767	AppNet1Serv6/10.0.16.15	10	S	0.269	6.389	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv16/10.0.16.25	10	S	0.136	1.362	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv22/10.0.16.31	10	S	0.136	1.362	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv19/10.0.16.28	10	S	0.136	1.362	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv12/10.0.16.21	10	S	0.136	1.362	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv17/10.0.16.26	10	S	0.136	1.362	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv25/10.0.16.34	10	S	0.136	1.362	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv14/10.0.16.23	10	S	0.136	1.362	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv20/10.0.16.29	10	S	0.136	1.362	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv24/10.0.16.33	10	S	0.136	1.362	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv9/10.0.16.18	10	S	0.269	6.389	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv3/10.0.16.12	10	S	0.269	6.389	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv10/10.0.16.19	10	S	0.269	6.389	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv5/10.0.16.14	10	S	0.269	6.389	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv23/10.0.16.32	10	S	0.136	1.362	MEDIUM	Leapfrog
CVE-2005-4767	AppNet1Serv7/10.0.16.16	10	S	0.269	6.389	MEDIUM	Leapfrog

Figure 1: Prioritizing Risk Remediation

Each enterprise has its own policy to evaluate and prioritize remediation of vulnerabilities. For example, an enterprise might mandate remediation of those vulnerabilities which pose the most downstream risk because they can be leveraged by worms to attack other systems in the network. Figure 1 above shows a vulnerability which exists on two systems and is rated as Medium severity by QualysGuard. However, running a risk analysis against the network reveals that the vulnerability poses a higher downstream risk on AppNet1Serv5 than AppNet1Serv23 because the ACLs on the routers and firewalls in the network allow the vulnerability on AppNet1Serv5 to be exploited from more networks. This helps the system administrator determine that AppNet1Serv5 should be patched before AppNet1Serv23.

For more information about deploying this solution, visit www.qualys.com/integrations.

About Redseal

RedSeal Systems develops innovative security risk management (SRM) software designed to streamline and automate the security management lifecycle. RedSeal's solutions enable companies to quantify overall security, assess critical areas of risk and validate that their security infrastructure successfully stops attacks. With RedSeal, enterprises can measure and reduce security risks, increase responsiveness to business demands, and reduce operational costs. More information can be found at www.redseal.net.

About Qualys

Qualys, Inc., the leader in on demand vulnerability management and policy compliance serves thousands subscribers around the world including 200 of the Forbes Global 2000. QualysGuard Software as a Service (SaaS) solutions help security managers effectively strengthen the security of their networks, conduct automated security audits and ensure compliance with internal policies and external regulations. Qualys' cost effective on demand technology requires no capital outlay, infrastructure or maintenance and can be deployed in a matter of hours anywhere in the world. Qualys global customers include AXA, DuPont, eBay, ICI Ltd, Kaiser Permanente, Novartis, Oracle and many others.

QUALYS®
www.qualys.com

USA – Qualys, Inc.
1600 Bridge Parkway
Redwood Shores
CA 94065
T: 1 (650) 801 6100
sales@qualys.com

UK – Qualys, Ltd.
224 Berwick Avenue
Slough, Berkshire
SL1 4QT
T: +44 (0) 1753 872101

Germany – Qualys GmbH
München Airport
Terminalstrasse Mitte 18
85356 München
T: +49 (0) 89 97007 146

France – Qualys Technologies
Maison de la Défense
7 Place de la Défense
92400 Courbevoie
T: +33 (0) 1 41 97 35 70

ON DEMAND SECURITY