

REM Security Management Console

CENTRALIZED VULNERABILITY MANAGEMENT

The REM Security Management Console provides IT professionals with a single point of visibility into an organization's security posture.

Today's IT professionals are faced with an overwhelming number of network vulnerabilities and intrusion attempts. This, combined with the growing complexity of networks, creates the increasingly difficult task of centrally managing and protecting assets within an organization. Quickly identifying which assets are most at risk is imperative for the overall health of an organization.

The REM Security Management Console provides IT professionals with a single point of visibility into an organization's security posture. REM enables an organization to quickly identify and prioritize vulnerabilities by balancing the asset value with the severity of the threat. Users can then efficiently allocate resources based upon threat level and business function to focus on the most critical vulnerabilities and attacks first.

REM is a multi-tier, scalable component to eEye's expanded Integrated Security and Threat Management Solutions. Available as software or an appliance, REM is capable of centrally administering Retina, the industry's leading network vulnerability scanner and Blink, the most powerful and comprehensive endpoint security software product. This solution provides a complete end-to-end vulnerability management and endpoint product solution for organizations that need to simplify the management of distributed, complex infrastructures while protecting its mission critical assets from evolving threats.

CENTRALIZED THREAT AND VULNERABILITY MANAGEMENT

The REM security Management Console was designed from the ground up to be a focal point for information regarding security risks within an environment. Using advanced metrics and graphical representations, assets are rated by both their vulnerabilities and attack vectors currently being exploited. REM can immediately determine and illustrate where potential risks lie within an organization regardless of where the asset resides, such that security information is always aggregated to one single centralized view.

FAST FACTS

USES STANDARD BROWSER based technology for logon, management, and reporting

THE ASSET DRIVEN architecture enables users to manage by logical grouping or assets regardless of the IP address

ADVANCED CHARTING permits rapid determination of the highest risks within an environment by business function or asset

REM IS AVAILABLE AS software or an appliance

COMPLETE MANAGEMENT and reporting of eEye's award winning Retina and Blink solutions



eEye Digital Security®

INFORMATION MANAGEMENT

The asset driven architecture of REM empowers users to manage data in logical groupings called attributes. Based on business functions and asset traits, such as geography, facilities, business unit, machine type, or any other custom container, users can automatically place assets into groups for reporting, filtering, and even role based security. This allows team members to view and manage security information by an asset classification at the granularity level desired. The management of information makes REM excel by reducing data overload and simplified third party integration.

SOLUTION FLEXIBILITY

REM has the flexibility to be deployed the way you want, and managed the way your organization has set its business requirements. As a software based solution, REM can be installed on existing servers within an environment using standard Microsoft Windows operating systems and databases. As an appliance, eEye delivers REM as an embedded solution on a hardened operating system with all appropriate licenses and exceptional performance.

INTEGRATED TASK SYSTEM

REM improves the overall efficiency of an organization by incorporating a task based ticketing system directly into the solution. Vulnerabilities and attacks can be automatically assigned to users and groups for investigation, mitigation, or remediation. With the ability for email alerts, users can be notified for any type of security event by asset, risk, threat, vulnerability, or even discovery of a new TCP service.

DETAILED REPORTING

Detailed and flexible reporting allows REM to provide the information in almost any consumable format. Execute a wide variety of reports from vulnerability details, to assets and hardware inventory, delta reports, patch reports, trending graphs, and even export data in HTML, CSV, Excel, PDF, and active reports formats.

SYSTEM REQUIREMENTS

WINDOWS 2000 SERVER SP4 OR HIGHER

WINDOWS SERVER 2003 SP2 OR HIGHER (32-BIT)

WINDOWS SERVER 2008 (32-BIT AND 64-BIT)

MICROSOFT SQL SERVER 2000 SP4 OR HIGHER

MICROSOFT SQL SERVER 2005 SP1 OR HIGHER

MICROSOFT SQL SERVER 2008

INTEL PENTIUM IV 2.0GHZ (OR COMPATIBLE)

1GB MEMORY

HARD DRIVE: 300MB (SOFTWARE INSTALL) / 20GB (DATABASE)

NETWORK INTERFACE CARD (NIC) WITH TCP/IP ENABLED

MICROSOFT .NET FRAMEWORK 2.0 (INCLUDED WITH INSTALLER)

MICROSOFT INTERNET INFO SERVICES (IIS) 6.0 OR HIGHER ASP.NET

About eEye Digital Security

Since 1998, eEye Digital Security has made vulnerability management simpler, less expensive, and more effective by providing the only unified vulnerability and compliance management solution that integrates assessment, mitigation, and protection into a complete offering. Consistently the first to uncover critical vulnerabilities and prevent their exploit, eEye leverages its world-renowned research and development to strategically secure customer assets. Thousands of mid-to-large size organizations, including some of the most complex IT environments in the world, rely on eEye solutions to protect against the latest known, unknown, and zero-day vulnerabilities.

[See more at www.eeye.com](http://www.eeye.com)

CONTACT INFORMATION

UNITED STATES
1.866.282.8276

NORTH AMERICA SALES
sales@eeye.com

GERMANY
+49 (0) 8031 2227 432

INTERNATIONAL SALES
sales.eu@eeye.com

UNITED KINGDOM
+44 (0) 20 8432 3490

www.eEye.com

111 THEORY, SUITE 250 | IRVINE, CALIFORNIA 92617