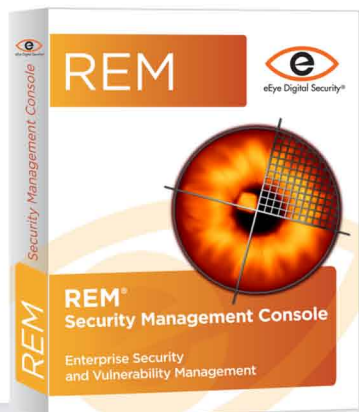




REM[®] Security Management Console

Centralized Vulnerability Management.



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, an appliance, or a managed service
- Complete management and reporting of eEye's award winning Retina and Blink solutions

**Secure
Your Business.**
www.eEye.com
866-282-8276

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, an appliance, or a managed service, 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. Considering that an asset can move around an organization, traveling beyond the perimeter firewalls and then back again, makes identification by device, rather than just IP address, of utter importance. 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.

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. Additionally, the underlying, searchable database structure ensures the speed, accuracy, and scalability of information to deliver real time views of all assets, and integrate with call centers, network management solutions, and security information managers using scalable standards such as SNMP and Windows Event Logs. The management of information makes REM excel by reducing data overload and simplified third party integration.

Solution Flexibility

The REM security Management Console represents the state of the art in security solution management. 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. In addition, REM can be utilized as a managed service hosted by eEye. REM has the flexibility to be deployed the way you want, and managed the way your organization has set its business requirements.

REM[®]

Additional Features and Benefits

Integrated Task System

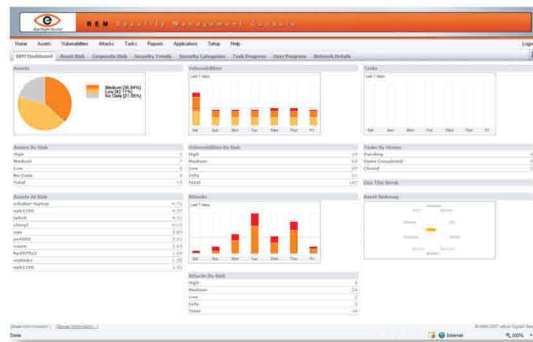
REM improves the overall efficiency of an organization by incorporating a task based ticketing system directly into the solution. Vulnerabilities and attacks can be automatically assigned to users and groups for investigation, mitigation, or remediation. With the ability for email alerts, users can be notified for any type of security event by asset, risk, threat, vulnerability, or even discovery of a new TCP service. The implementation of the task system allows detailed tracking of all security anomalies, with user notes and comments, to satisfy the most stringent compliancy requirements for tracking and resolution.

Detailed Reporting

Reports are critical to every team member reviewing security information in an organization. Whether it is the chief information officer signing off on corporate compliancy or the security engineer reviewing a potential virus; good reports complete a solution. Within REM, team members can 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. All of the reports can be executed ad-hoc, scheduled, emailed, or attached to a vulnerability assessment job such that they are committed at the completion of a scan job. Detailed and flexible reporting allows REM to provide the information in almost any consumable format the end user desires.

“A good product for organizations of most sizes, especially those with widely distributed networks and limited security management resources.”

- SC Magazine



About eEye Digital Security

eEye[®] Digital Security is pioneering a new class of security products: integrated threat management. This next-generation of security detects vulnerabilities and threats, prevents intrusions, protects all of an enterprise's key computing resources, from endpoints to network assets to web sites and web applications, all while providing a centralized point of security management and network visibility. eEye's research team is consistently the first to identify new threats in the wild, and our products leverage that research to deliver on the goal of making network security as easy to use and reliable as networking itself. Founded in 1998 and headquartered in Orange County, California, eEye Digital Security protects more than 9,000 corporate and government organizations worldwide, including half of the Fortune 100. **For more information, please visit www.eEye.com.**

U.S. Tel: 1.866.282.8276

N. America: 1.949.333.1900

Germany: +49 (0) 8031 2227 432

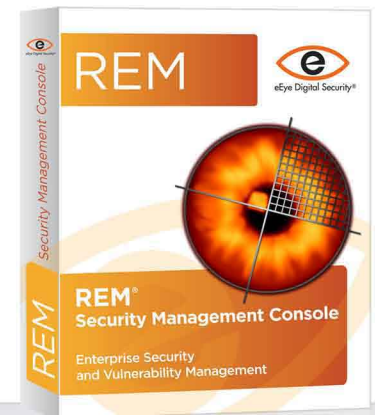
U.K.: +44 (0) 20 8144 1102

Asia Pacific: +603 79581575

N. America Sales: sales@eEye.com

International Sales: sales.eu@eEye.com

Asia Pacific Sales: apacsales@eEye.com



System Requirements

- Microsoft Windows 2000 SP4 or 2003 SP2
- Microsoft IIS 6.0 (Internet Information Services or higher)
- Microsoft .NET Framework 2.0 (and ASP.NET on 2003)
- Intel Pentium IV 1.4 GHz CPU
- 1GB of RAM or Higher
- 300 MB HDD for the software installation and 20 GB HDD for event storage, NTFS Required
- Microsoft SQL 2000 Server SP4 or SQL 2005 SP1 or higher