

## Networks

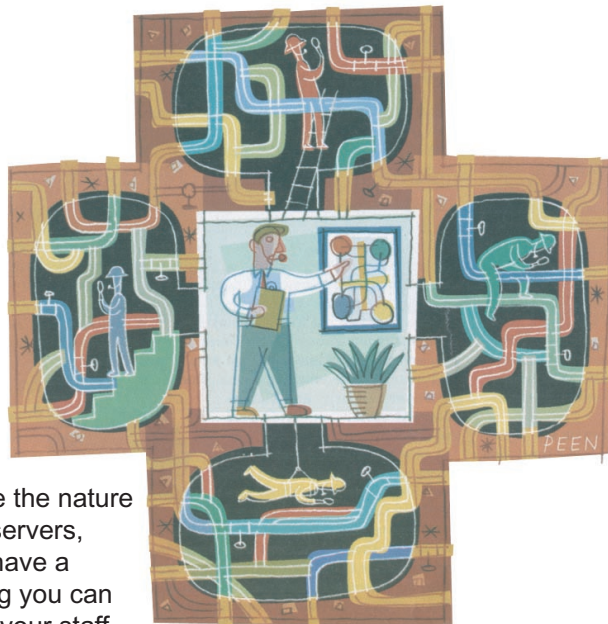
STRATEGIC NEWS AND ANALYSIS 02.24.03

### Eyes on the network

Retina Enterprise Suite brings manageability to strong vulnerability assessment

By **Wayne Rash, P.J. Connolly** ..... February 21, 2003

To say that keeping on top of your OS updates is a pain is to vastly understate the nature of the problem. If you're responsible for an enterprise with even a few dozen servers, plus a few appliances, some routers and switches, and a firewall or two, you have a huge management problem. Applying all of the necessary patches -- assuming you can figure out which patches you need and which are actually available -- can tax your staff to the breaking point. Worse, with larger enterprises, the problems mushroom.



Meanwhile, of course, you're being taken to task by everyone from the board to random magazine pundits for not having every patch installed within milliseconds of when it's announced. Then, when a worm shows up and wreaks havoc on your network, everybody's pointing fingers -- at you.



eEye Digital Security's popular Retina Network Security Scanner is quite capable of keeping an administrator apprised of vulnerabilities on a single network. But there was never a way to extend Retina's capabilities to the enterprise — until now.

eEye's Retina Enterprise Suite ties individual Retina scanners together, allowing all of them to be managed from a single station. In fact, Retina Enterprise Suite will allow you to handle up to 65,000 individual IP addresses in your enterprise.

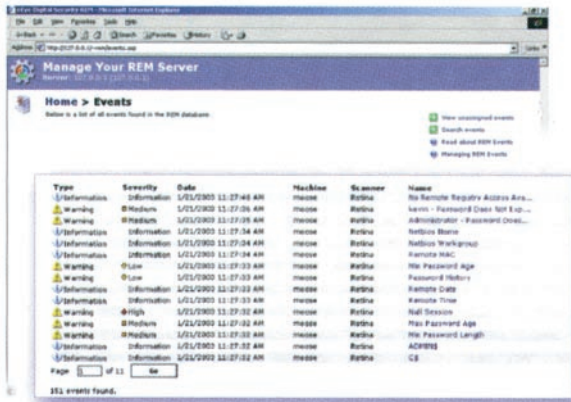
Retina Enterprise Suite draws its vulnerability scanning smarts from the Retina scanner. Retina Remote Manager makes each scanner capable of communicating with the enterprise manager. Tying everything together is the REM Security Management Platform. This product consolidates the information from the Retina scanners, manages security certificate distribution and event logging. The server is designed to communicate with the REM Events Manager.

The REM Events Manager, the fourth component of Retina Enterprise Suite, provides the REM user interface. It also handles the reporting for the consolidated enterprise data, or from any individual scanner. Further, the Events Manager handles the process of delegating tasks to other administrators. It can reduce workload by automating the process of distributing reports to the affected organizations or locations according to predetermined scopes, rules or levels of authority. Conveniently, the Events Manager is a Web-based application, so you can reach your management console from nearly anywhere.

Finally, there's also a REM Event Client, which is a middleware bridge between the Events Manager and the Retina Remote Manager.

Assuming you already have a database server running on your network, deploying Retina Enterprise Suite is fairly simple. Everything comes on one CD, and you install the various parts in order, following the directions on the screen. The biggest inconvenience is typing in long lists of characters in groups of four to activate the license. This boring process seems to be the current way of making sure the product isn't pirated.

# NETWORKS



REM Event Manager provides warnings of deficiencies and how-to-fix details for each deficiency event.

Once REM Events Server and Events Manager are installed and the database access is working (which took us only a few seconds to complete on the test network), you're ready to install the Retina Scanner and Remote Manager software. You'll need one scanner and remote manager for each separate network, both of which are available on the same CD as the other Retina Enterprise Suite components.

Once the software is installed, all you need to do is set up the scanning and reporting within the REM Event Manager. The REM Event Manager uses a stand-alone application to designate the database and Web servers, the Web server's virtual directory, and authentication credentials for the database and Web server. Other reporting and scanning functions are set up from a Web browser; this can be local or on a separate host.

Once Retina Enterprise Suite is up and running, you can order a scan via the console of all of the networks you control. When we tried this, we were told that it might take a while, so we went to lunch. It wasn't a long lunch, but the scanning was complete before we returned.

testing at the same time had freaked out. Apparently it decided that all of the queries from Retina Enterprise Suite were attacks. We probably should have told the IDS about Retina.

The scan resulted in several discoveries. First, we found that just about every computer on our test network was in need of some kind of vulnerability fix. This wasn't a surprise, since we deliberately have different levels of software on our many machines. Second, an IDS (intrusion-detection system) we were

Third, we found that Retina's attempts to probe one of our Solaris boxes resulted in the box generating streams of report messages. But the Sun box didn't prevent Retina from getting the information it needed.

What defeated Retina, and thus Retina Enterprise Suite, was Zone Alarm. Retina simply could not find a Zone-Alarm-equipped computer, much less report on its vulnerabilities. This isn't exactly a significant failure, however, since Zone Alarm and other similar firewalls eliminate (or make irrelevant) many vulnerabilities anyway.

Still, if you really want to keep on top of your network, you probably should find a way to get past the personal firewalls in your enterprise. Even with an excellent product such as Zone Alarm (or its enterprise cousins) vulnerabilities remain, even if they're more difficult to exploit.

Using Retina Enterprise Suite after the scan is remarkably intuitive, considering you're managing the vulnerability tracking and remediation of myriad computers and other network devices. Each device with an IP address is listed separately and each vulnerability is listed within, ranked in order of severity. As you click on each vulnerability listing, you're told what the problem is, how serious it is, and what can be done to fix it. If Retina Enterprise Suite can fix the problem, such as one that required a change to a registry setting, it will do so. Otherwise, it will provide a link that will let you implement the fix, or it will tell you what the problem is and where to find the fix.

Via the Console, you can assign staff members to fix vulnerabilities, then track the overall level of completion, down to the individual fix. You can even generate charts that show the reduction in threat to the entire enterprise due to your efforts to fix problems.

It is, in fact, the reports Retina Enterprise Suite produces that make it unusually useful. Yes, you can focus on a single endpoint, but you can also produce meaningful reports that reflect the entire enterprise, reports that you can use to drill down as needed. As a result, Retina Enterprise Suite becomes more than just useful for the enterprise; it becomes an asset. The fact that it will assess virtually any device on the network (unless it's a Mac, and eEye will have Mac support soon, the company says) makes it a valued asset. This is a product worth having.

Wayne Rash is a senior analyst at the InfoWorld Test Center. Contact him at wayne\_rash@infoworld.com. P.J. Connolly is a senior analyst at the InfoWorld Test Center.

## THE BOTTOM LINE

### Retina Enterprise Suite

**BUSINESS CASE:** This solid solution identifies, manages, and fixes vulnerabilities while keeping staff resources in check.  
**TECHNOLOGY CASE:** consolidates vulnerability assessment from multiple networks into a single management point.

#### PROS

- Makes eEye's Retina software easily managed across the enterprise
- Handles nearly every operating platform
- CON
- Management console is Windows only

**COST:** Retina: \$6,520 for 250 IP addresses; Retina Remote Manager: \$1,995 per Retina scanner; REM Events Server: \$4,995; REM Events Manager: \$9,995 (includes five manager accounts)  
**PLATFORMS:** Management server Windows NT/2000. Requires a separate server with an ODBC compliant database  
**COMPANY:** eEye Digital Security; www.eeye.com

EASE OF USE:	8
IMPLEMENTATION:	8
INNOVATION:	8
INTEROPERABILITY:	9
SCALABILITY:	9
SECURITY:	8
SUITABILITY:	7
SUPPORT:	8
TRAINING:	8
VALUE:	8
<b>DEPLOY</b>	
1 2 3 4 5 6 7 <b>8.1</b> 9 10	