INFORMATION SECURITY®

BUYER'S GUIDE TO Vulnerability Management

Understanding your weak spots will help you pick the right vulnerability management solution. We'll offer suggestions on how to weave technologies with policy and process.

INSIDE

TechTarget
The Technology Media ROI Experts

INFOSECURITYMAG.COM

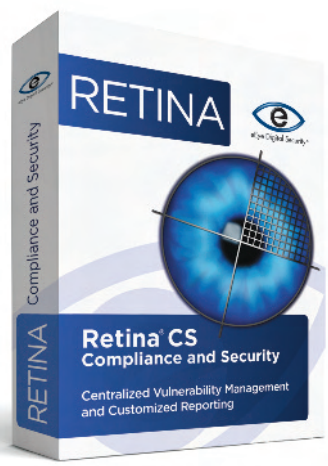
Power Meets Simplicity

All the Power of Retina with a New & Easy to use Interface!

Retina's renowned power has been harnessed in an easy to use Vulnerability Management Solution, now complete with simplified navigation, a rich Internet interface and superior workflow. From vulnerability assessment to endpoint protection, Retina CS provides you with a highly sophisticated, yet intuitive security solution complete with improved workflows and standardized reporting capabilities.

Identify, protect and fix vulnerabilities with power and simplicity.

Take a demo today!



About eEye Digital Security

eEye Digital Security is the global leader in the next generation of security solutions: comprehensive vulnerability management and zero-day endpoint security protection. To learn more, please visit **www.eeye.com** or call 866.282.8276.

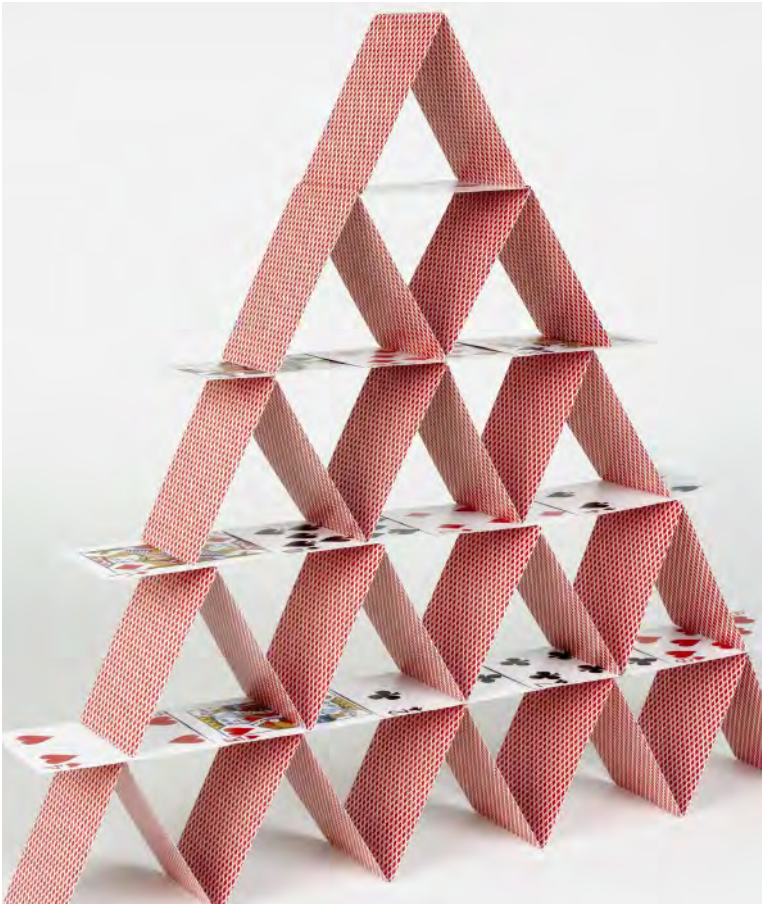
The endpoint to vulnerability starts here.

eEye Digital Security®

CHOOSING THE RIGHT Vulnerability Management Technologies

Understanding your weak spots will help you pick the right vulnerability management solution. We'll offer suggestions on how to do this and weave technologies with policies and process.

BY ED MOYLE



HAVE YOU EVER SEEN one person alone on a seesaw? Of course not, right? That's because the seesaw works on the principle of balance—two people in balance allows the whole system to move, whereas just one alone is completely static.

There are some things in life that are better when balanced: a balanced diet is healthiest, a seesaw is only fun with two people, a balanced checkbook is worry-free. In information security, it's vulnerability management. Vulnerability management (VM) isn't just one single, monolithic concept but rather a number of sub-concepts that all work together to make up a VM strategy.

Some think that VM is just about deploying assessment tools while others think VM is about applying operating system patches. In reality a VM strategy is about something bigger. It's about balance: balancing your detection capability with your capacity to remediate, and balancing your policy and planning with monitoring and follow-up. When all these factors are in sync, you wind up with something greater than the sum of the parts. But build up one at the expense of the others and—just like the person alone on the teeter-totter—you'll be left scratching your head wondering why nothing is happening.

Getting Started

How does a company make progress? After all, the marketplace is pretty confusing: dozens of vendors sell products that claim to do VM—but they all seem to approach the problem from different directions. How does a firm know where to invest, especially since most firms probably have aspects of VM in place already. And since no two organizations will have identical requirements, one firm's VM strategy might look completely different from someone else's.

The challenge for firms looking to get the most out of vulnerability management is to take a hard, honest introspective look at their organization, understand what processes and technology they have in place already that will form the skeleton for their VM strategy, and craft a vision for what technologies and processes they'll deploy in the future to get them where they want to go.

It's not a process that's for the faint of heart—but for mature security programs looking to expand their technical capabilities, there's tremendous value to be had.

At a high-level, VM is a process that involves setting a desired end state for an environment via policy, checking for areas where the environment deviates from the desired, prioritizing and vetting the issues, and then remediating them.

What is Vulnerability Management?

First of all, companies seeking to craft a VM strategy should first spend some time assessing what they have in place already. A complete vulnerability management strategy incorporates detection and remediation as well as policy and process.

At a high-level, VM is a process that involves setting a desired end state for an environment via policy, checking for areas where the environment deviates from the desired, prioritizing and vetting the issues, and then remediating them. The process is iterative—repeated on a continuous basis to make sure that components stay secure. Folks who are familiar with formal QA models like the Shewhart cycle (i.e., "Plan, Do, Check, Act") might find some of these concepts familiar. It's basically QA for vulnerabilities: you're defining what your environment should look like (Plan), implementing processes to bring the environment into alignment with that standard (Do), building a detection capability to find deviations from that baseline (Check),

and bringing the environment back in line with the standard (Act).

On the detection side you need to locate and identify potential exposures in your environment. These exposures can be related to hosts, applications, or systems within your environment that would allow attackers to gain access. They could take the form of missing security patches, insecure configuration, Trojans and rootkits, or any other potential security vulnerability. The key concern in the detection phase is coming up with an accurate list of potential issues. Since the list needs to be accurate—and many of the technical tools we have to assist sometimes aren't—the detection side also includes vetting of potential issues for errors. And lastly, detection includes a reporting capability as well—since you'll want to somehow communicate potential issues to staff.

Remediation needs to include a triage component–some way to prioritize which changes are most critical and what changes are less critical.

Remediation, on the other hand, is the ability to fix the problems that you find during detection. Now, being able to detect an issue is important, but it's not that useful if you can't fix what you find. Once you start looking for problems, you're likely to find so many issues that you can't act on them all at once. As a result, remediation needs to include a triage component—some way to prioritize which changes are most critical and what changes are less critical. That way your staff can make sure biggest issues are resolved sooner while leaving smaller issues unresolved until there's more time to remediate them.

More Process than Technology

Now, if your organization is like most, you're probably doing many of these things already. In fact, nowadays you almost have to. You might have deployed a scanning tool to locate and report on vulnerabilities, you might have contracted with an external testing firm to perform quarterly scanning as part of PCI, or you might have deployed technology like WSUS to help keep devices current. All of these tools are arguably part of a VM strategy—they just need the processes molded around them to integrate into a larger holistic VM strategy.

A useful first step for firms looking to get serious about VM is to take stock internally. Look at what tools and processes are already in place and can support the broader goal. If your operations or compliance teams are already using a scanning tool (or a scanning service) as part of their processes, why duplicate efforts? Does your organization already have a software delivery tool? Why add an extra layer of complexity? So, like most activities, VM should start with introspection. What technologies do you have, how are they're being used and how can you integrate them into your larger VM strategy?

Next, you'll need to decide what your processes are going to be with respect to testing/scanning. Are you going to scan every day or once per quarter? Are you going to scan the entire environment or just the production environment? Are you going to scan off-hours when production impacts are less noticeable or during

business hours when staff can respond more quickly to problems? Each environment's requirements are going to be different, so it pays to plan ahead of time what specific requirements you have and how the tools you'll bring in will fit in with your requirements and the processes you already have in place.

It also pays to outline potential hiccups—unexpected scenarios that could cause highly visible production impact. For example, do you have specialized infrastructure like a SCADA network or biomedical devices that could compromise safety if scanned aggressively? Do you support specialized devices like HL7 interface engines that are easily brought down by routine scanning? Ideally, you should map out any potential problem areas ahead of time so that you know where you can open the throttle and where you need to wear kid gloves.

Lastly, plan out what your remediation cycle will be. Do you have a defined mechanism for prioritizing vulnerabilities when you find them? If so, don't standardize on a prioritization strategy that's different from what you're using in other areas. For example, does an external firm provide quarterly vulnerability reports as part of your PCI compliance? If so, don't buy a tool for internal scanning that can't report using that same standard. The whole point of VM is to add situational awareness to your security program—having two different reporting standards detracts from that situational awareness.

Approach Vendors with Requirements in Hand

Once you have a good idea of what your requirements are with respect to detection and remediation, now's the time to bring vendors in to help round out plan. The VM space includes a large swath of vendors—and not all of them define VM the same way—so it's up to you to dictate your requirements to them, not vice-versa.

For example, some organizations might have scanning tools deployed but might not have technology in place to remediate. On the other hand, other firms might have automated software delivery tools already deployed along with robust configuration, but they might not have any way to locate potential issues.

Let's take a brief look at some of the types of tools and services you may wish to consider once you've laid out your requirements:

Vulnerability Information Management: As anybody in operations will tell you, there's a tremendous amount of noise and chatter about new vulnerabilities—and getting good data about new threats is challenging. Information management tools centralize information about vulnerabilities and streamline the flow of information about new vulnerabilities into your organization. These tools consolidate the dozens (potentially even hundreds) of external locations where information about new issues is published, standardize that information, and deliver it rapidly to you.

Automated Vulnerability Scanners: These highly-prevalent tools iterate through the hosts in your environment, examine those hosts looking for known areas of weakness such as poor configuration choices or missing patches, and report on those areas of weakness. These tools are very mature, are ubiquitously deployed throughout many segments of industry, and come in both appliance and software-only form factors. Since these tools compare against a list of known

issues, they're less useful against previously unknown issues (so called "zero-day" vulnerabilities) and they need to be kept updated to stay current.

Asset Inventory Tracking: Inventory tracking and prioritization tools help you keep track of what devices you have fielded and those you discover during scanning. Since many issues are specific to particular software packages, knowing what you have out there helps weed out noise—and reliable intelligence about the role of devices will be key to your prioritization efforts.

Risk Management and Prioritization: The more devices you scan, the more issues you'll find—both real issues and false positives. In fact, you'll find so many that you won't be able to fix everything at once. Often used in combination with an asset inventory, risk management and prioritization tools help you to put discovered issues in context in order to perform triage—by providing information about which issues are likely to be exploited and which aren't. They help you decide what needs to get fixed today and what can wait for tomorrow.

Software Delivery and Patch Management: These tools help you apply software changes—including security changes—once you've located an issue, prioritized it, and planned a fix. Manually installing software to every machine is probably not feasible, so these tools help you send the right fix to the right machines.

Governance, Remediation Management, and Reporting: Vulnerability management is a complicated endeavor. As you move forward with your strategy, you'll likely want to keep track of the work you've done, the work you can't do yet (for example, due to technical limitations), as well as manage the overall workflow of the VM process. These tools provide a framework for doing just that. They track workflow, keep track of exceptions such as patches that can't be installed or known problematic configurations, and provide a framework to report those metrics to management.

Vulnerability management isn't hard, but it requires knowledge of your organization, knowledge of investments you've made already and where your weak spots currently are. It's not just about buying tools—it's about weaving technology together with processes and policy in a way that's balanced.

And most importantly, remember your VM solution might look totally different from another firm's depending on your unique needs and your unique requirements.›

Ed Moyle is Founding Partner of Security Curve where he provides consulting and solutions to clients worldwide. Prior to joining Security Curve, Moyle was Vice President and Information Security Officer for Merrill Lynch Investment Managers (MLIM,) where he was responsible for coordinating all aspects of information security within the 2,500 employee, $500 billion, business unit. During his tenure at Merrill, Ed also developed firm-wide cryptographic solutions for secure data transfer, secure key management, authentication and data integrity. Before joining Merrill, Moyle worked within the federal sector for Computer Science Corporation (CSC,) where he consulted to the Department of Defense's Joint Service Computer Aided Acquisition and Logistics System. Moyle was responsible for security engineering activities, including platform security, security evaluation activities and vendor evaluation/deployment activities.

BUYER'S GUIDE

Vulnerability Management

HERE IS A PRODUCT LISTING OF VULNERABILITY MANAGEMENT, VULNERABILITY ASSESSMENT SCANNERS AND AUTOMATED PATCH MANAGEMENT SOLUTIONS.

Beyond Security
www.beyondsecurity.com

BigFix
www.bigfix.com

Computer Associates
www.ca.com

EMC (Configuresoft)
www.emc.com

Ecora
www.ecora.com

eEye Digital Security
www.eeye.com

Everdream (owned by Dell)
www.everdream.com

GFI
www.gfi.com

IBM (Internet Security Systems)
www.iss.net

LANDesk
www.landesk.com

McAfee
www.mcafee.com

Microsoft
www.microsoft.com

nCircle
www.ncircle.com

NetIQ
www.netiq.com

NetVision
www.netvision.com

Novell
www.novell.com

PatchLink (now Lumension)
www.lumension.com

Qualys
www.qualys.com

Red Seal Systems
www.redseal.net

Safety-Lab
www.safety-lab.com

Saint
www.saintcorporation.com

Scriptlogic
www.scriptlogic.com

Secureworks/ LURHQ
www.secureworks.com

Shavlik
www.shavlik.com

StillSecure
www.stillsecure.com

Symantec
www.symantec.com

Tenable Network Security
www.tenablesecurity.com

Tripwire
www.tripwire.com

Information Security magazine offers comprehensive Buyer's Guides on the following topics:

Antimalware

Application Security

Authentication

DLP

Email Security

Identity and Access Management

Intrusion Detection/Prevention

Mobile Data Security

Network Access Control

Network Firewalls

Policy and Risk Management

Remote Access

SIEM

UTM

Vulnerability Management

Web Security Gateways

Wireless Security

For more information, contact:
jgarland@techtarget.com

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY®

EDITORIAL DIRECTOR Kelley Damore

EDITOR Michael S. Mimoso

SENIOR TECHNOLOGY EDITOR Neil Roiter

FEATURES EDITOR Marcia Savage

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Jay G. Heiser, Marcus Ranum, Bruce Schneier

CONTRIBUTING EDITORS
Michael Cobb, Eric Cole, James C. Foster, Shon Harris, Richard Mackey Jr., Lisa Phifer, Ed Skoudis, Joel Snyder

TECHNICAL EDITORS
Greg Balaze, Brad Causey, Mike Chapple, Peter Giannacopoulos, Brent Huston, Phoram Mehta, Sandra Kay Miller, Gary Moser, David Strom, Steve Weil, Harris Weisman

USER ADVISORY BOARD
Edward Amoroso, AT&T
Anish Bhimani, JPMorgan Chase
Larry L. Brock, DuPont
Dave Dittrich
Ernie Hayden, Seattle City Light
Patrick Heim, Kaiser Permanente
Dan Houser, Cardinal Health
Patricia Myers, Williams-Sonoma
Ron Woerner, TD Ameritrade

SEARCHSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS EDITOR Robert Westervelt

ASSOCIATE EDITOR William Hurley

ASSISTANT EDITOR Maggie Wright

ASSISTANT EDITOR Carolyn Gibney

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS Amy Cleary

EDITORIAL EVENTS MANAGER Karen Bagley

VICE PRESIDENT AND GROUP PUBLISHER
Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Kristin Hadley

SALES MANAGER, EAST Zemira DelVecchio

SALES MANAGER, WEST Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
Suzanne Jackson

PRODUCT MANAGEMENT & MARKETING
Corey Strader, Jennifer Labelle, Andrew McHugh

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Neil Dhanowa ndhanowa@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Meghan Kampa mkampa@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Eric Sockol

EUROPEAN DISTRIBUTION
Parkway Gordon Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES
Kelly Weinhold
Phone 781-657-1691 Fax 781-657-1100

REPRINTS
FosteReprints Rhonda Brown
Phone 866-879-9144 x194
rbrown@fostereprints.com

TechTarget
The Technology Media ROI Experts

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 117 Kendrick St., Suite 800, Needham, MA 02494 U.S.A.; Phone 781-657-1000; Fax 781-657-1100.

eEye Digital Security

See ad page **2**

- eEye Solutions
- Retina CS Hosted Service Demo
- Retina Security Scanner Free Trial

About eEye Digital Security

eEye Digital Security is the global leader in the next generation of security solutions: comprehensive vulnerability management and zero-day endpoint security protection. eEye enables secure computing through world-renowned research and innovative technology, supplying the world's largest businesses with integrated and research-driven vulnerability assessment, intrusion prevention, asset security and compliance solutions. eEye's research team is consistently the first to identify new threats in the wild and our products leverage that research to deliver the tools necessary to protect our customers' environments. The endpoint to vulnerability starts here.