WHITE PAPER

beyondtrust®

Beyond Traditional Security

Avoiding the Top 5 Vulnerability Management Mistakes

The New Rules of Vulnerability Management

Table of Contents

Introduction

WE'VE ENTERED AN UNPRECEDENTED ERA

Technological advances have transformed today's organizations into practically borderless entities, making it harder than ever to protect the network. Employee-owned devices, mobile computing, desktop applications, unmanaged administrator rights, and social networks have broadened the security field into new territories.

The cost and consequences of maintaining security and compliance are steeper than ever. Zero-day vulnerabilities aren't slowing down and attackers have gotten smarter about how to penetrate your network. You need safeguards to protect everything from laptops, printers, and web apps to servers, databases, and networking devices. Essentially, any device connected to your network could be leveraged if vulnerabilities are present. Plus, with new technical standards and government regulations, the urgency to secure and manage every aspect of the IT infrastructure increases even further.

This guide outlines the top five mistakes around vulnerability management and how to avoid them to protect critical IT assets and improve your security posture, while reducing costs.

Mistake 1: Disjointed Vulnerability Management

The job of protecting corporate assets would be challenging enough, even without new attack vectors being exploited through desktop applications, employee-owned devices, mobile computing, and social networks. Everyday you face new network devices, operating systems, applications, databases, web applications, plus numerous IP-enabled devices (laptops, servers, printers, etc.). These lists seem to never stop growing.

Clearly, as things get more complicated, they get more difficult to manage. Many organizations take the approach of using disparate, stand-alone solutions to accomplish the key aspects of vulnerability management—assessment, mitigation, and protection. However, this leaves them with a disjointed picture of security, which is not only more difficult to manage, but also more expensive.

TAKE A UNIFIED APPROACH

With security budgets and resources under pressure, you need to take the most efficient approach possible, one that brings the key pieces of vulnerability management together in a single solution. The answer is Unified Vulnerability Management, which delivers a consolidated solution for assessing, mitigating, and protecting your environment, while reducing the overall cost of security and compliance.

ASSESSMENT

Vulnerability assessment must deliver unified configuration and vulnerability scanning across network devices, operating systems, applications, databases, and web applications using a scalable, non-intrusive approach. It's critical that vulnerability management includes configuration assessment, not just patches. Poorly set internal configurations can be as harmful as security violations from an outside source. Ideally, assessment should include unified reporting over all of these assets as well.

MITIGATION

You need prescriptive guidance and recommendations to effectively remediate critical vulnerabilities and strategically prioritize the rest. Make sure your solution adheres to broadly accepted standards which include integration with both SCAP and ASV (PCI) for assessment, risk scoring and reporting. In addition, look for alert and notification capabilities so you can take immediate action on critical issues.

PROTECTION

You need zero-day protection in cases when a vendor has not yet created patches against vulnerabilities in their operating system or application. Your solution should also reduce risk with intrusion prevention, application control, and USB and firewire controls.

Bringing assessment, mitigation, and protection together under one roof, in the form of a single solution, will ultimately save you countless hours and dollars.

Mistake 2: Relying on Remote Assessment Alone

Running remote vulnerability assessments works for many systems, but what about those blocked by firewalls or segregated from the network? What about mobile and offline devices? These are potential gaps that could be exploited.

In most environments, not every system can be reached. Thus, they can't be updated immediately without impacting stability, introducing operating incompatibilities, disrupting business processes, or negating internal or regulatory compliance. Relying solely on remote vulnerability assessments is not enough—and may, in fact, cause your organization to be exposed to threats.

CLOSE THE GAPS WITH REMOTE AND LOCAL VULNERABILITY ASSESSMENT

For truly complete security, you need remote vulnerability assessment as well as local assessment for assets that are disconnected, unmanaged, or "exception" systems. Using a lightweight agent is the best way to get at these types of systems. It serves to augment your remote scans and makes it easier to meet stringent regulatory compliance requirements, where local credentials and more frequent scans are required.

With combined local and remote vulnerability assessment, you'll:

- Strengthen security posture and ease the burden of regulatory compliance with local and remote vulnerability assessment
- Close the security gap on assets that are disconnected, unmanaged, or "exception" systems
- Get full visibility into both remote and local vulnerabilities

Lastly, you need full visibility via a single console to view the combined results of all scans to ensure complete security.

Mistake 3: Unprotected Zero-day Vulnerabilities

Zero-day vulnerabilities continue to increase as attackers find new ways to penetrate your network. Clearly, you need safeguards to protect against these exploits and other complex attacks. Of course, like nearly all companies, you have anti-virus and anti-spyware in place. These signature-based technologies work well, but must be augmented with zero-day vulnerability management to protect systems when vendor-supplied patches do not yet exist for an operating system or application. Continuous zero-day vulnerability monitoring and protection is a must have in today's threat landscape.

ADD A LAYER OF PROTECTION

Augment foundational security components like anti-virus and anti-spyware with an additional layer that stops zero-day vulnerabilities. The ideal solution leverages a host-based intrusion prevention engine to dynamically collect and incorporate new threat data in real-time. With this, you can enforce policy and secure your organization from targeted email or internet attacks that could compromise your systems and data.

Zero-day protection helps you:

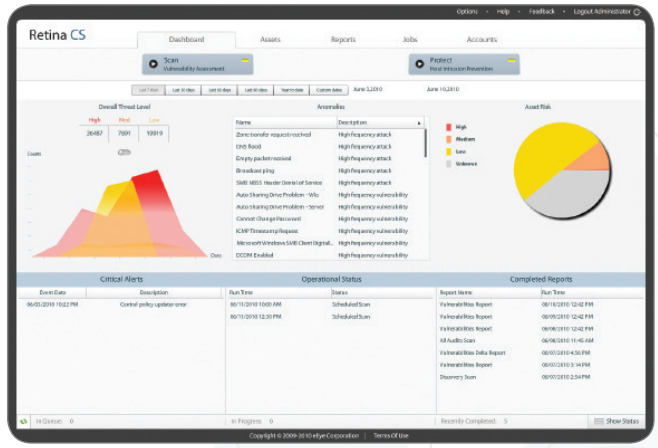
- Reduce risk with intrusion prevention and zero-day protection where a vendor has not yet created patches to protect against vulnerabilities in their OS or application
- Improve system protection by setting policy over which applications are allowed to function and preventing modification of specific registry settings
- End data theft and leakage by regulating USB and firewire access, preventing transfer of sensitive or confidential data to personal storage devices

Mistake 4: Decentralized Visibility

Decentralized security visibility is one pitfall that trips up many organizations. Many organizations perform assessment, mitigation, and protection activities at individual locations but lack centralized management across the enterprise. Quickly identifying which assets are most at risk is imperative for the overall health of an organization. But, the challenge is finding a solution with a strong distributed architecture and the ability to provide a single point of management and visibility across the enterprise.

CENTRALIZE VISIBILITY

To achieve centralized visibility, look for a fully integrated, completely web-based security console product. An easy add-on to some vulnerability management solutions, this will dramatically simplify the management of distributed, complex infrastructures while providing true end-to-end protection. The key is becoming more efficient at finding, fixing, and protecting against the most urgent vulnerabilities and strategically prioritizing the rest.



Look for a workflow-oriented console to make it easier to meet regulatory and security compliance requirements. Also, one that offers an asset-driven architecture will enable you to make logical groupings of assets regardless of their IP address and business function. But, you should also be able to view and prioritize risks grouped by business function or event, as well as by asset.

Mistake 5: Compliance at the Expense of Security

Yes, you need to meet regulatory compliance. Many organizations place heavy focus on meeting requirements, which is certainly a wise approach. Especially for regulations such as HIPAA and PCI, audit failures (in the form of fines) are not only expensive, but potentially devastating to customer confidence. Some high-profile, highly publicized breaches serve to highlight what can happen if an organization takes their eye off the ball. However, a truly comprehensive security initiative requires focus not just on compliance, but also on the broader management of security and vulnerabilities.

CREATE A SECURITY BASELINE AND MEASURE AGAINST THOSE STANDARDS

Institute comprehensive, strategic security initiatives that include compliance. This can be facilitated by finding a solution that let's you easily create a security baseline and then measure against those standards. From there, you should be able to measure against internal security policy and regulatory compliance. In other words, implement a solution that gives you the tools to meet compliance regulations and then go beyond those requirements to actually improve security posture and reduce risk.

Why You Need Local Vulnerability Assessment, Too

DISCONNECTED SYSTEMS

With your mobile workforce, you likely have systems that are offline or disconnected from the network, which makes it almost impossible to perform an assessment or to apply a patch or update.

UNMANAGED SYSTEMS

Some peoples' roles require them to be excluded from the direct control of the IT security staff—such as executives, engineers, and technical staff. Their systems connect to the network, but may be excused from updates.

CAN'T CHANGE THE SYSTEM

In some cases, the systems are always on and always connected. For example, systems that perform critical business operations or highly specialized functions.

OLD SYSTEMS

You'd update these, but they may be running older versions of the operating system or business applications that can't be changed due to licensing restrictions, support requirements, or as a result of known or potential compatibility issues with the update.

"EXCEPTION" SYSTEMS

Some systems can't be changed due to external regulation. For example, those certified by the FDA to be HIPAA compliant can't be changed if they are to retain their certification status.

SYSTEMS RUNNING ON SYSTEMS

Virtualization technologies introduce on-demand system provisioning. With this, the number of new systems running within an organization increases dramatically. And, chances are, a large number of these remain undiscovered, unmanaged, and un-patched.

About BeyondTrust

With more than 25 years of global success, BeyondTrust is the pioneer of Privileged Identity Management (PIM) and vulnerability management solutions for dynamic IT environments. More than half of the companies listed on the Dow Jones Industrial Average rely on BeyondTrust to secure their enterprises. Customers include eight of the world's 10 largest banks, seven of the world's 10 largest aerospace and defense firms, and six of the 10 largest U.S. pharmaceutical companies, as well as renowned universities. The company is privately held, and headquartered in Carlsbad, California. For more information, visit **beyondtrust.com**.

CONTACT INFO

NORTH AMERICAN SALES
1.800.234.9072
sales@beyondtrust.com

EMEA HEADQUARTERS
Suite 345 Warren Street
London W1T 6AF
United Kingdom
Tel: + 44 (0) 8704 586224
Fax: + 44 (0) 8704 586225
emeainfo@beyondtrust.com

CONNECT WITH US
Twitter: @beyondtrust
Facebook.com/beyondtrust
Linkedin.com/company/beyondtrust
www.beyondtrust.com

