
Balbix®
8
“Must Have” Features for Risk-Based Vulnerability Management and More

Introduction

Historically, vulnerability management (VM) has been defined as the practice of identifying security vulnerabilities in unpatched systems that can put your entire enterprise environment at risk. Though it is typically an integral part of every organization's cybersecurity strategy, the traditional VM approach has become increasingly ineffective as cyber-attacks continue to grow in volume and sophistication. It is no longer enough to just enumerate vulnerabilities due to unpatched systems, and this is where traditional VM unfortunately falls short. This e-book highlights 8 key distinguishing features that transform a traditional VM program into risk-based vulnerability management, which enables organizations to avoid breaches by continuously discovering and monitoring all points in their attack surface and take appropriate mitigation steps.

Traditional VM approaches:

- Do not provide accurate, up-to-date IT asset inventories
- Typically only scan certain types of assets, and usually only enterprise-owned ones
- Are episodic, with point-in-time scans
- Assess risk across only one attack vector, unpatched software, and do not cover the 200+ other attack vectors
- Use a static rules-based approach
- Spew out large numbers of vulnerabilities (often too much to implement)
- Do not prioritize actions granularly or by business risk

You need to take a more modern approach to properly understand your comprehensive risk posture. The answer is a *risk-based* approach to *vulnerability management* that not only *identifies* vulnerabilities but also *predicts breach risk, prioritizes action items based on business risk, and offers guidance on fixes to correct the issues*.

A truly risk-based vulnerability management solution will have the following key capabilities:

- **Automatic discovery** and **inventorying** of all IT assets, applications, and users
- Visibility on **all types of assets** including BYOD, IoT, cloud, and third party
- **Coverage** of attack vectors beyond just scanning for vulnerabilities in unpatched software
- **Continuous** and **real-time monitoring** of all assets across all attack vectors
- Understanding of **context** and **business risk** for each asset
- **AI and machine learning** to observe and analyze the volume of data collected from thousands of observations to create a complete picture
- **Prioritized list** of security actions based on comprehensive assessment of business risk
- **Prescriptive fixes** to address the security issues in a manner integrated with the enterprise workflow

Armed with a risk-based VM program encompassing these *powerful set of 8 must-have features*, organizations can identify, fix, and close vulnerabilities before they can be exploited.

#1: Automatic Discovery and Inventorying

Q: Do you know how many devices (managed, unmanaged, BYOD, IoT) are plugged into your environment at any point in time?

Traditional VM tools do not provide automatic discovery and inventory of the wide range and scope of IT assets that are typically at play in your organization. In order to control your environment, you need *an agile, real-time inventory of all assets* – devices, apps, and users.

RISK-BASED VULNERABILITY MANAGEMENT

Modern or risk-based VM should be easy to deploy and provide a comprehensive inventory of your existing asset ecosystem within hours of first deployment. After that, it needs to provide automatic and continuous discovery and inventorying of all applications, users, and IT assets including IoT, cloud, on-premises, and mobile. In addition to that, as soon as a new asset is plugged into your environment, the risk-based VM system should be able to identify it instantly and categorize it properly.

Balbix

#2: Visibility for *All Types of Assets*, including BYOD

Q: How helpful would it be if you had continuous visibility across all types of your assets?

Traditional VM tools typically scan enterprise-owned and managed IT assets such as corporate servers and laptops, and they leave out all the rest. But in today's modern enterprise, device demographics have shifted dramatically with the proliferation of different asset categories (unmanaged, BYOD, cloud-based, IoT, and mobile, to name just a few).

Business owners, security and IT teams need to understand and be cognizant of the security issues for all types of assets, and in order to do that they need comprehensive views across the entire IT ecosystem.

RISK-BASED VULNERABILITY MANAGEMENT

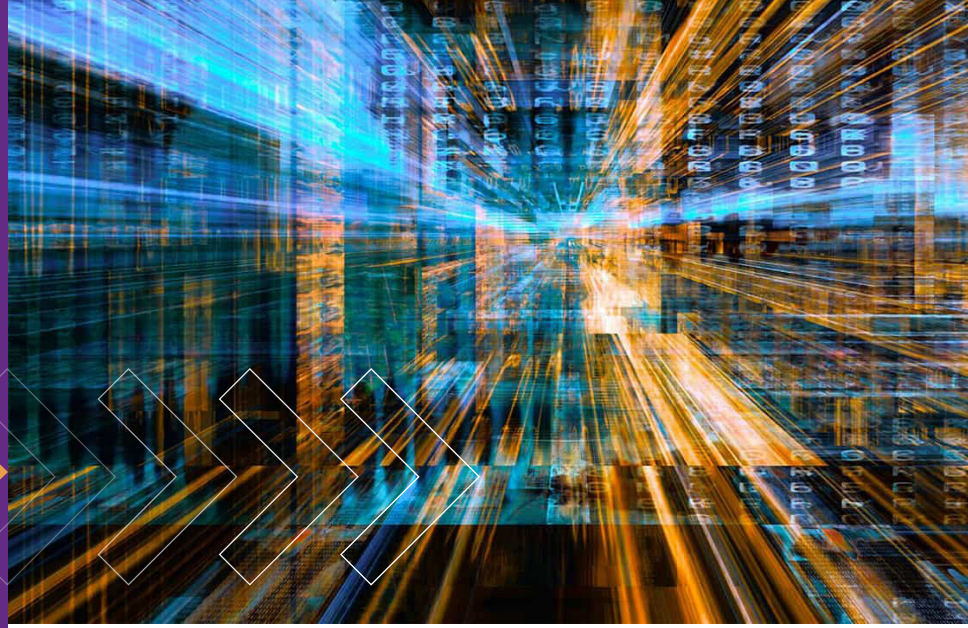
Risk-based VM should be able to discover, monitor, and scan *all types of devices and assets* – including BYOD, IoT, cloud, and third party – to automatically and continually predict breach risk through a single integrated system. Risk-based VM will also let you locate critical devices (including BYOD and third party) and apps that, due to their vulnerability and exposure history, are most susceptible to zero-day exploits.

Balbix®

#3: Covering the Multi-Dimensional Attack Surface

Q: Does your VM only look at unpatched vulnerabilities? How about the risk to your business from 200+ other attack vectors like weak or shared passwords, malware, incomplete encryption and more?

Traditional VM tools have limited coverage across the vast and rapidly expanding set of attack vectors. Phishing, ransomware, misconfigurations and credentials are just some of the vectors not covered by traditional VM. This is because VM tools were originally developed to scan unpatched systems only. The reality is that unpatched vulnerabilities represent just one vector among a plethora of attack vectors coming your way. You need a broad risk-based VM that goes way beyond your unpatched software vulnerabilities.



RISK-BASED VULNERABILITY MANAGEMENT

Next-generation VM needs to monitor and scan for many other attack vectors like device/network and application misconfigurations, risk from weak or no encryption, use of weak passwords & shared passwords, denial of service, password reuse, propagation risk, phishing and ransomware, zero-day threats, and more. Risk-based VM gives you the tools you need for breach prediction, and breach control across the multiple attack dimensions you face in the real world. In short, it lets you avoid breaches by providing continuous and real-time scanning across your entire spectrum of vulnerabilities.

Balbix

#4: Continuous and Real-Time Monitoring and Analysis

Q: Is interval-based scanning falling short of expectations? Wouldn't automated and continuous scanning and analysis of all assets across all attack vectors be a better strategy?

Traditional VM is episodic, with point-in-time scans that restart only once a previous scan completes. Thus, they are infrequent and focus on a fraction of your enterprise attack surface, providing only a point-in-time snapshot of your vulnerabilities. As such, these tools don't offer truly continuous, real-time scanning, which is a serious limitation in a world where threats are coming at you from all directions, all the time.

RISK-BASED VULNERABILITY MANAGEMENT

A next-generation risk-based VM should offer continuous and real-time monitoring and analysis of all attack surfaces, giving you the ability to quickly identify potential breach risk. New BYOD devices should be discovered and assessed minutes after they are plugged into your environment. Breach risk should be continuously calculated for every device, app, and user across your hyper-dimensional attack surface.

Balbix

#5: Contextualization

Q: Do you know how to best understand the business impact of each of your assets and which of their vulnerabilities pose the greatest risk to your business?

A key component in determining business cyber-risk is understanding the context around the role and criticality of each IT asset. Without this information, rationalizing mitigation activities becomes an uphill, often unsurmountable task. When your VM system doesn't provide this kind of context, vulnerabilities are prioritized based on standard rules and criteria (e.g. CVE status). Thus your team has no way of knowing which vulnerabilities to tackle first and are faced with an overwhelming volume of work, which often can't be completed.

RISK-BASED VULNERABILITY MANAGEMENT

Modern, risk-based VM needs to provide ***business risk for each asset*** by contextualizing information like role of that asset, the security state of that asset analyzed over multiple attack vectors, compensating controls already in-place, globally prevalent threats, and more. This is the only way organizations will have a ***comprehensive risk calculation*** when monitoring their exposures and putting their mitigation strategies in place.

Balbix

#6: Advanced AI and Machine Learning

Q: In the face of ever-increasing cyber-threats, can you afford to rely on legacy technology?

With the hundreds (and growing number) of attack vectors across a multitude of IT assets, the enterprise attack surface is massive and rapidly expanding. This, coupled with the propensity of bad actors to carry out ever more sophisticated multi-pronged attacks, amounts to a huge problem of scale. Observing and analyzing all this data is not a human scale problem any more.

RISK-BASED VULNERABILITY MANAGEMENT

With increasing number of attack vectors and asset types, how can you observe, parse, and analyze all the data and how do you figure out what to act on first? Modern, risk-based VM needs to leverage specialized artificial intelligence (AI) and machine learning to analyze 1000s of data signals to provide enterprises with a comprehensive assessment and prioritized fixes for their breach risk. Using AI to self-learn new targets, attack methods, and analyzing data from internal data feeds and external threat sources, risk-based VM systems are at the cutting edge of security innovation.

Balbix

#7: Prioritization

Q: How do you prioritize your list of actions? What do you tackle first?

Traditional VM tools only focus on identifying the severity of the findings and ranking them with a generic low, medium, and high rating (e.g. from CVEs). This level of granularity is not specific enough to use as the foundation for your vulnerability management efforts. In short, it presents you with inadequate data to make decisions about how to best address the overwhelming volume of identified vulnerabilities, and it doesn't tell you which ones pose the greatest risk to your business.

RISK-BASED VULNERABILITY MANAGEMENT

In order to increase your cyber-resilience, you need to focus your limited SecOps resources on the potential breaches that may have the most business impact. Risk-based VM needs to be able to comprehensively assess the ***business risk*** of all assets, presenting a prioritized list of mitigation actions and prescriptive fixes for each prioritized action. With these capabilities, your organization will be able to prioritize actions and get better at remediating its most important and at-risk assets quickly and efficiently.

Balbix

#8: Prescriptive fixes

Q: Does your team know how to remediate the flagged security issues?

Traditional VM tools only focus on identifying security issues and flagging them for you. It then falls on your resource-constrained security team to figure out how to patch or otherwise fix the vulnerability and resolve the problem. Your security team not only needs to see the issues, but also understand them in detail and be able to quickly fix them.

RISK-BASED VULNERABILITY MANAGEMENT

Best-in-class risk-based VM not only provides a list of prioritized action items, it also guides you on how to fix the issues. Prescriptive fixes that speed remediation are a key feature of more advanced risk-based VM systems, and significantly increase the productivity and agility of security and SOC teams. In addition, risk-based VM also offers the ability to integrate with your ticketing and security orchestration systems and allow you to automatically incorporate vulnerability remediation into your existing enterprise security workflows.

Balbix

Risk-Based Vulnerability Management with Balbix BreachControl™

Balbix BreachControl is a powerful risk-based vulnerability management platform. It enables organizations to adopt a risk-based VM strategy by continuously discovering and monitoring *all points in the attack surface*, analyzing this information to predict likely breach scenarios, and helping organizations take appropriate mitigation steps by producing a prioritized list of action items and prescriptive fixes to address identified issues.

BreachControl is the industry's first system to leverage specialized artificial intelligence (AI) and machine learning to provide enterprises with comprehensive and continuous predictive assessments. Visualized via a searchable risk heat-map, Balbix BreachControl is designed for CISOs and IT security teams who want to proactively understand and control the security of their environments.

BreachControl provides:

- Discovery and inventory of all devices, users, and applications
- Scanning across 200+ attack vectors, not just unpatched software
- Real-time monitoring and analysis of all attack surfaces
- Calculations of business risk for every asset
- Actionable lists of proactive mitigations based on business criticality
- Prescriptive and comprehensive fixes for each prioritized action

As a best-in-class platform for risk-based VM, BreachControl offers:

- **Automatic discovery** and **inventory** of IT assets
- Visibility on **all types of assets** including BYOD, IoT, cloud, and third party
- **Coverage** of attack vectors beyond just scanning for vulnerabilities in unpatched software
- **Continuous** and **real-time monitoring** of all assets across all attack vectors
- **Business risk** assessments for each asset, calculated using contextual information relevant to your environment
- Cutting edge technology using **AI and machine learning** to observe and analyze data collected from thousands of observations to create a complete picture
- **Prioritized** security actions based on comprehensive business risk assessment
- **Prescriptive fixes** to address the security issues in a manner integrated with the enterprise workflows

Balbix