WHITE PAPER

Deeper Look:

RISK-BASED VULNERABILITY MANAGEMENT

Balbix

Deeper Look:

RISK-BASED VULNERABILITY MANAGEMENT

Executive Summary

In the face of an ever-increasing onslaught of cyberattacks and their levels of sophistication, organizations are generally relying on decades-old core security technology, often cobbled together in multiple layers of point products (aka "security in depth"). Vulnerability management (VM) is one such area. Traditionally, vulnerability management vendor selection has centered around a vendor's ability to identify software vulnerabilities in an environment with low false-positive reporting. While acquisition of vulnerability data is an essential part of helping security teams understand their security posture, it's certainly not enough.

This is simply because while security vulnerabilities due to unpatched software are a serious risk factor, they represent only one category out of hundreds of known attack vectors. Other factors such as web browsing behavior, phishing, credential exposure, and access to sensitive networks/data are also essential to providing insight into identifying your breach risk. In order to truly know your risk posture, what is needed is a risk-based vulnerability management approach that not only identifies unpatched software vulnerabilities but also predicts and mitigates other attack vectors.

In this paper, we will discuss:

- Challenges and limitations of traditional VM tools
- What is risk-based vulnerability management
- Why traditional VM tools are not enough to stop breaches
- Advantages of risk-based vulnerability management

Understanding vulnerability management challenges

Vulnerability management is widely described as the practice of identifying security vulnerabilities in unpatched systems that if exploited by adversaries, can put your entire enterprise environment at risk. Typically, vulnerability management is a foundational practice, and an integral part of any standard cybersecurity initiative. However, constantly changing device demographics and increasing sophistication in cyberattack techniques, including an increase in recent multi-pronged attacks, are challenging the VM industry and the cyber defenders alike.

Limitations of traditional vulnerability management

While performing regular and ongoing scanning for unpatched vulnerabilities is a start in the right direction, it is woefully insufficient given the current breadth of attack surface and the pace of change in highly dynamic IT environment. Some of the fundamental limitations of vulnerability management solutions include:

- VM takes a rules-based approach and you can only scan for those vulnerabilities that you (or your vendor) has created rules for. Traditional tools are unable to learn new targets or attack methods by itself.
- VM tools do not provide accurate and up-to-date IT asset inventory data. Do you know how many devices – managed, unmanaged, BYO, IoT, etc. – are plugged into your environment at this time? Do you have an inventory of all assets – users, apps, and devices? Do you know which of these assets are highly critical for your business and which ones are less important? How much of this information is provided by your VM tool? Not much, obviously.
- VM tools typically only scan enterprise-owned managed IT assets. In modern enterprises today, the device demographics has changed dramatically with a proliferation of all kinds of assets including unmanaged, cloud-based, IoT and others.
- VM is episodic, with periodic point-in-time scans. These tools do not offer truly continuous, real-time scanning – in fact, once the scan stops, the security practitioner has to manually kick off another scan.
- Traditional VM tools generally spew out a large number of vulnerabilities, and unless you are able to stay up-to-date with your patching (which organizations typically struggle with due to a number of reasons) chances are that your team is facing an ever-growing to-do list.

4 Reasons Why Organizations Struggle with Patching

1	Overwhelming number of alerts with too many vulnerabilities to patch
2	Lack of prioritization to focus the security team's efforts towards patching most critical issues
3	Small, resource-constrained teams, with not enough people
4	Lack of guidance on HOW to fix the issues

Also, since traditional VMs don't provide any risk-based context around the business impact of each asset and the vulnerabilities, your team has no way of knowing which action items to prioritize and they are left with patching everything. And not only that, the traditional VM tools can only focus on identifying the severity of the findings and rank them with a generic – low, medium, and high – rating. This presents you with inadequate data to make decisions about how to best address the overwhelming volume of identified vulnerabilities, and which are the greatest risk to the business. Do you start with the highs first? What if there are thousands of high vulnerabilities? How do you prioritize your list of actions?

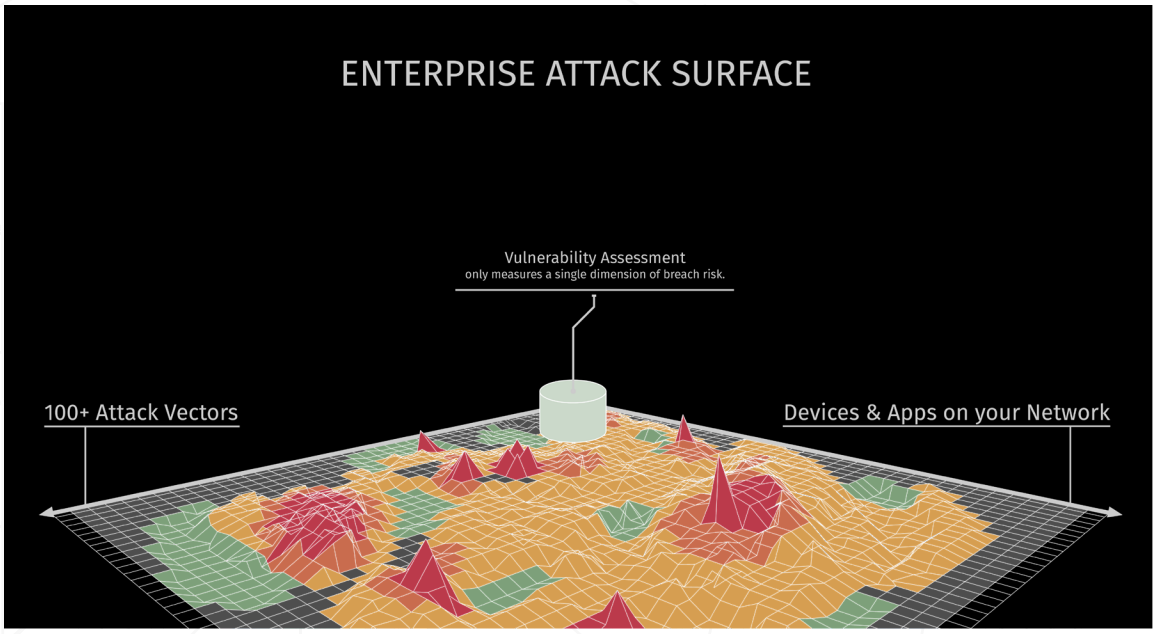
- VM tools have limited coverage of the vast and rapidly expanding enterprise attack surface. For example, vulnerability assessment does not tell you anything about the risk to your business from weak passwords and shared passwords, or incorrect or incomplete implementations of encryption. Similarly, VM cannot understand the difference in business risk between an unpatched primary domain controller and an unpatched lab server using the same operating system. This is perhaps the most important limitation of a VM tool.

7 Attack Vectors Classes Not Covered by Traditional VM Tools

1	Phishing and ransomware	5	Password reuse
2	Device/Network and application misconfigurations	6	Risk from weak/lack of encryption
3	Use of weak passwords	7	Propagation risk
4	Malicious Insiders		

The reality is that scanning for unpatched vulnerabilities in your network is just one vector amidst a plethora of attack vectors that can be exploited by cyber-criminals. Your IT infrastructure is ***not*** the only asset that needs to be secured. You have endpoints, applications, BYODs, managed and unmanaged assets, and users – all of who make up your entire asset list. On top of that, if you consider the following graph – with all your assets on x axis and all the things that can go wrong (or the ways you are susceptible to exploits) on y axis – you can get an idea of your vast attack surface. Unpatched vulnerabilities are just ONE small component here.

VM is limited in that it only enumerates systems likely to be compromised from just one attack vector – unpatched software.



Enter risk-based vulnerability management

Given that the volume of breaches, from both unpatched systems and the other 100s of attack vectors, is continually growing, VM tools must use risk-based analysis to provide a manageable volume of high quality alerts. With the hundreds (and growing) of attack vectors and propensity of bad actors to carry out multi-pronged attacks, VM 2.0, more than anything else, needs to be risk-based. A truly risk-based VM would have the following key capabilities:

Accurate inventory and categorization

First of all, a comprehensive, automated, and continuous inventory of all existing enterprise assets – managed, unmanaged, cloud, devices, IoT, apps, users – is needed. Without visibility into what you have and what needs protecting, you cannot have a comprehensive view of your security posture. Then, it is also important to categorize all the assets accurately. Any additional information about assets—such as the type of asset and the asset's location—gives you better insight into what needs to be fixed right now.

Asset contextualization based on business risk

Rationalizing mitigation activities becomes an uphill, often unsurmountable task without knowing the context and business risk of each asset. With a risk-based vulnerability management approach, each asset is analyzed using the context of the specific asset, its use in the business, the impact of a potential breach on it, and the likelihood of that happening. That calculation is then used to prioritize all suggested security fixes found based on overall business risk. This helps your organization prioritize remediation and get better at patching the most important and at-risk assets quickly and efficiently. Contextualization is based on your internal security findings, prevalent global threats, and currently deployed security controls.

Going beyond identifying vulnerable systems

Once you have identified the areas of weakness in your enterprise, you need a prioritized list of action items, unique to your environment, that can enable you to proactively tackle mitigation based on business criticality. Your team also needs mitigation guidance and prescriptive fixes to reduce your breach risk and maximize team productivity. This actionable list of mitigation actions along with actual fixes, all based on the risk posed by the various components in your organization's infrastructure allows vulnerability management to become truly risk-based.

With risk-based vulnerability management, mitigation tasks are prioritized and performed with a more rational approach, leading to higher efficiency in implementation, better security for your systems as you address actual risks, and an improved ROI on your initial assessment—and any subsequent vulnerability management activities you undertake.

Summary

It is unlikely that the number of attacks will abate over time. On the contrary, there is every reason to expect that their number will continue to grow. In fact, with the growing attack surface and increasing number of potential targets as we constantly increase the connections of various things to the Internet, breaches are inevitable.

The only way to stop reacting to attackers and get ahead of the game is to be proactive about the security your IT assets. Investing in emerging technologies that use AI and deep learning algorithms to monitor and predict your breach risk due to these myriad of attack vectors is an effective strategy. With prediction of breaches and insights into potential breach simulations, organizations can move towards a more robust security posture. Then, with a prioritized list of action items and prescriptive fixes for these action items, vulnerabilities can be fixed and closed before they can be exploited.

Balbix BreachControl™, the predictive breach avoidance platform, enables organizations to deploy a risk-based VM program to avoid breaches by continuously discovering and monitoring all points in your attack surface, analyzing this information to predict likely breach scenarios, and helping you take appropriate mitigation steps by producing a prioritized list of actions items and prescriptive fixes to address the issues.

Learn more about Balbix BreachControl now.

Balbix

3031 Tisch Way, St 800
San Jose, CA 95128
866.936.3180

info@balbix.com
www.balbix.com

072518