Balbix®

How Risk-Based Vulnerability Management Beats Traditional Vulnerability Management

7 reasons customers are making the switch and adopting risk-based vulnerability management (VM) with Balbix BreachControl™

	Traditional VM	Balbix BreachControl™
Limitation 1: **Legacy technology** ? In the face of an ever-increasing onslaught of cyberattacks, do you want to rely on legacy technology?	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 themselves.	Using advanced AI and deep learning algorithms, BreachControl is able to self-learn new targets and attack methods by analyzing data from internal data feeds + external threat feeds.
Limitation 2: **Limited types of assets** ? Do you know how many devices – managed, unmanaged, BYOD, IoT, etc. – are plugged into your environment at any moment?	VM tools do not provide coverage for a wide range and scope of IT assets. 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?	BreachControl offers automatic discovery and inventorying of all applications, users, and IT assets including IoT, cloud, on-premises, and mobile, providing broad coverage across a wide range of assets types.
Limitation 3: **Limited visibility** ? You don't just have managed assets like your corporate laptops in your environment. So, would you want your VM tool to only scan the managed assets?	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, BYOD, cloud-based, IoT and others.	BreachControl discovers, monitors, and scans all devices and assets including BYOD, IoT, cloud, and third party, to automatically and continually predict their breach risk.
Limitation 4: **Per-cycle and not continuous** ? Would you say that "continuous scanning" is the same as "manually start another scan once the previous scan completes"?	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	BreachControl offers truly continuous and real-time monitoring and analysis of all attack surfaces for potential breaches. New BYOD devices are discovered and assessed minutes after they are plugged into your environment.

	Traditional VM	Balbix BreachControl™
Limitation 5: Lack of contextualization Do you know how to best understand the business impact of your assets and which vulnerabilities pose the greatest risk to the business?	Traditional VM does not provide any risk-based context around the business impact of each asset and the vulnerabilities, so your team has no way of knowing which action items to prioritize when faced with an overwhelming volume of work. Also,VM tools cannot understand the difference in business risk between an unpatched primary domain controller and an unpatched lab server using the same operating system.	Rationalizing mitigation activities becomes an uphill, often unsurmountable task without knowing the context and business risk of each asset. BreachControl provides business risk for each asset by taking into account the role of that asset, security state of that asset analyzed over 200+ attack vectors, global threat model, and your organization's existing mitigation controls to provide a real risk calculation.
Limitation 6: Lack of prioritization How do you prioritize your list of actions? When faced with generic priority rankings like high, medium, and low, do you start with the highs first? What if there are thousands of high vulnerabilities? How do you prioritize your list of actions?	Traditional VM tools 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.	BreachControl comprehensively assesses business risk of all assets to prioritize suggested security fixes. This helps your organization prioritize remediation and get better at patching the most important and at-risk assets quickly and efficiently.
Limitation 7: Covers only unpatched software attack vector Does your VM tell you anything about the risk to your business from 200+ other attack vectors like weak passwords and shared passwords, or incorrect or incomplete implementations of encryption?	VM tools have limited coverage of the vast and rapidly expanding enterprise attack surface. Phishing, ransomware, misconfigurations, credentials are some classes not covered by VM at all. This is because VM tools were originally developed to scan unpatched systems only.	The reality is that scanning for unpatched vulnerabilities in your network is just one vector amidst a plethora of attack vectors. BreachControl goes way beyond monitoring for only unpatched software vulnerabilities and scans for over 200 attack vectors like device/network and application misconfigurations, risk from weak/lack of encryption, Use of weak passwords, password reuse, propagation risk, phishing and ransomware etc.

Balbix BreachControl™, the predictive breach avoidance platform, enables organizations to deploy a risk-aware 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.

Balbix®

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

info@balbix.com
www.balbix.com

©2018 Balbix, Inc. All rights reserved.