

**THE
TERRIBLE,
HORRIBLE,
NO GOOD,
VERY
BAD
TRUTH
ABOUT**




**Vulnerability
Management**

The Truth

ABOUT VULNERABILITY MANAGEMENT

You have a vulnerability management program which is perhaps the cornerstone of your cybersecurity strategy. Your vulnerability scanner runs once a month (or more/less depending on how cybersecurity-mature your organization is). Each time a scan is run, it spits out a mile-long list of vulnerabilities and then you start questioning yourself:

- 
- Are these noise or are they real?
 - Did this scan cover all my assets including mobile devices, cloud services and IoT?
 - Do I know which assets are at risk for compromise due to password issues or misconfigurations?
 - Am I being protected against zero-days?
 - What is the riskiest area of my attack surface?
 - How do I fix these vulnerabilities?
 - Which ones should I fix first?
 - What's my real risk?

Sound familiar? You're not alone. Across the board, irrespective of the vulnerability management tool being used, information security professionals have the same pain.

While almost all popular frameworks like the **NIST Cybersecurity Framework** or **CIS Controls** advocate a layered, defense-in-depth approach with vulnerability management at its foundation, they neglect to disclose the terrible, horrible, no good, very bad truth about vulnerability management.



TRUTH #1

Vulnerability
management
only covers about

5%

of your
attack surface
and misses a
number of
important risks
that should be
on your radar.

THE VULNERABILITY in vulnerability management

According to the [MITRE's CVE website](#), a vulnerability is a mistake in software code that provides an attacker with direct access to a system or network. If it goes undetected, it could allow an attacker to pose as a super-user or system administrator with full access privileges.

Vulnerability management, by its very definition, only considers an application defect as a vulnerability so traditional tools only look at Common Vulnerabilities and Exposure (CVEs) –known security

vulnerabilities and exposures in publicly released software packages – due to unpatched software.


However, if you consider the broader, dictionary definition of a vulnerability, it is anything that exposes you and puts you at risk. So, bad password hygiene – using weak or default passwords, reusing passwords, and not storing passwords correctly – is also a vulnerability. And so are misconfigurations, encryption issues, and risky online behavior of employees, and countless other risky issues.



V

Vulnerability management tools do NOT look for vulnerabilities or flaws across a range of attack vectors, missing many really important risks such as:

- Password issues like weak passwords, clear text passwords and password reuse
- Device/network/application misconfigurations
- Propagation risk
- Phishing and ransomware
- Incorrect or incomplete implementations of encryption, and more

A man with a beard and short dark hair, wearing a plaid shirt, stands against a grey wall. He is holding a large white sign in front of his chest. The sign has the text "I am not a CVE" written on it in a bold, black, sans-serif font. To the left of the man, there is a vertical orange bar that transitions from a darker orange at the top to a lighter orange at the bottom.

**I am
not
a CVE**

Enterprise **attack surface** is **exploding** with assets including thousands of devices, apps and users, susceptible to hundreds of attack vectors, ranging from simple things like weak passwords, to more

complex things like phishing, unpatched software, encryption and configuration issues, etc. CVE-based known vulnerabilities are only a small subset of most enterprises' overall attack surface.

THE SECRET LIVES of passwords

According to the **2019 Verizon Data Breach Investigations Report**, 80% of hacking-related breaches involved compromised and weak credentials and 29% of all breaches, regardless of attack type, involved the use of stolen credentials. And this has been the case for years.

This serious vulnerability is not related to software or applications at all, but rather human beings and our habits. When even one admin uses the same password on every router, switch, server, application, helpdesk account, or even social media, the entire enterprise is at risk. Moreover, this vulnerability will not be flagged by your vulnerability scanner.

GO FIGURE the misconfigurations

Misconfiguration is when there is an error in system configuration. For example, if setup pages are enabled or a user uses default usernames and passwords, this can lead to breaches. If setup/app server configuration is not disabled, the hacker can determine hidden flaws, and this provides them with extra information. Misconfigured devices and apps present an easy entry point for an attacker to exploit.

Numerous misconfigurations in application, cloud, and OS settings exist across the enterprise. According to Gartner, through 2025, **99% of cloud security failures** will be due to the customer's own fault, owing to **misconfigurations** and mismanaged credentials, not cloud provider vulnerabilities.



TO ENCRYPT or NOT TO ENCRYPT

Data encryption translates data into ciphertext, another form that only people with access to a secret key or password can read. The purpose of data encryption is to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks. Strong encryption must be applied to data at rest, in-motion, and where suitable, in-processing.

Missing / poor encryption leads to sensitive information including credentials being transmitted either in plaintext or using weak cryptographic ciphers or protocols. This implies that an adversary

intercepting data storage, communication, or processing could get access to sensitive data using brute-force approaches to break weak encryption.

THE BOTTOM LINE

We need to acknowledge that vulnerabilities are not just CVEs. Any breach methods that put your enterprise at risk are dangerous. Enterprise security teams need to go beyond the traditional vulnerability management tools and invest in a risk-based vulnerability management system that goes beyond just monitoring unpatched software and covers a **broad range** of other attack vectors and vulnerabilities as well.





TRUTH #2

Vulnerability
management
does not
prioritize output
by business
criticality,
leaving you
drowning
in a sea of
vulnerabilities
with no idea
how to proceed.



Today's security teams are literally drowning in a sea of unprioritized vulnerability data. They are unable to assess which threats are the most serious, which ones need to be acted upon, and in what order they need to implement fixes to effectively protect the enterprise.

THE MANAGEMENT in vulnerability management

Conceptually, a typical vulnerability management program consists of 4 steps:

- 1** Identify software vulnerabilities
- 2** Sort them in some order of priority
- 3** Mitigate them by patching or accepting risk
- 4** Rinse and repeat in a continuous cycle

Understanding and acting on data output from your vulnerability tool is a critical component of your vulnerability management program. However, if your tool is spewing out vulnerabilities in the thousands every time a scan completes, your team is bound to be left overwhelmed and struggling with how to proceed. This inability of the security teams to address the vulnerabilities in a timely manner due to a vast number of action items is in fact a significant shortcoming of the traditional vulnerability management program.

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 periodic scans will return the same list of vulnerabilities each time.

Moreover, legacy vulnerability tools use primitive risk metrics to prioritize vulnerabilities. Their calculation is typically based on CVSS scores and a simple business impact model (high, medium, low), which leads to untold amounts of efforts being spent on solving low impact issues.

For comprehensive risk-based prioritization of vulnerabilities, you need to factor in 5 elements— vulnerability severity, threat level, business criticality, exposure due to usage and the risk-negating effect of compensating controls. Learn more about the essential pillars of prioritization [here](#).

5 ESSENTIAL PILLARS for prioritization

1 VULNERABILITIES ACROSS 100+ ATTACK FACTORS

Vulnerabilities are not just unpatched software CVEs. Any attack vectors that put your enterprise at risk are dangerous. Vulnerabilities arising from weak or stolen passwords, phishing, misconfigurations, ransomware, and encryption issues can be equally damaging and all types of vulnerabilities need to be considered while prioritizing.

2 THREATS

New threats emerge almost on a daily basis and it is key to understand which ones are important from an organization's standpoint. Mapping real and emerging threats - what is currently fashionable (or possible) for the adversary – to specific assets and then observing and prioritizing them is critical.

3 BUSINESS CRITICALITY

With a myriad of assets in your network, it is important to understand the impact of each on your business. To properly estimate the adverse effect to the enterprise if an asset were to be breached, take into account both inherent (e.g. asset category, business unit) and contextual properties of the asset (roles, applications, user privilege, and interaction with other assets).

4 ASSET EXPOSURE

Exposure due to asset usage is multi-dimensional, encompassing factors such as duration for which the asset has been present on the network, availability and frequency of use, as well as type of use. A device with unpatched IE is not necessarily a critical risk if the default browser of the user is Chrome and they never use IE. Similarly, risky behavior of privileged users increases exposure.

5 MITIGATING CONTROLS

Investments into security controls like firewalls, anti-phishing systems, and EDR successfully mitigate risk. Get an inventory of existing security controls scored by their effectiveness. Combine it with a mitigated risk model to users prioritize actions that preferentially focus on critical, highly used, and vulnerable assets that are ineffectively mitigated or unmitigated.



TRUTH #3

Vulnerability
management
output is
typically
more than

30
DAYS
OUT OF DATE



Most organizations perform quarterly scans, some monthly, some less than that. However, as vulnerabilities are patched or remediated, new ones are discovered even in relatively static IT environments, making periodic scanning ineffective.

THE PROBLEM of outdated data

Your enterprise asset inventory is dynamic with devices being added and retired, physical machines migrating to virtual and various stakeholders constantly installing and updating software. Traditional vulnerability management scanners are typically configured to run periodically – quarterly, monthly, or weekly – which, given the dynamic nature of the enterprise, makes managing compliance and cyber-risk very difficult. Continuous monitoring of all assets should be the goal for every enterprise. Enterprises should strive for continuous monitoring of all assets to keep pace with their dynamic environments. Continuous monitoring not Achieving this goal not only helps organizations determine whether they are actually fixing the flaws they discover, but also helps security teams identify trends in the performance of the vulnerability management program.

Vulnerability management is a foundational technology, thus needs to be executed as a continuous process and not done quarterly or monthly. Today's enterprise network environment is a living breathing space and anything short of near real time and continuous monitoring is not sufficient.

What makes the enterprise network dynamic?

- **Network devices being continuously on-boarded**
- **Virtual computing, whether on-premises or in the cloud, leading to new system hosts continuously being provisioned or deployed**
- **BYOD and other mobile devices are constantly logging into the network**

VULNERABILITY MANAGEMENT needs a refresh

Traditional vulnerability management is the approach many security teams rely on to keep their organizations safe. Yet it falls woefully short in a number of important areas. It misses many assets because of poor discovery. It's periodic rather than continuous, which means that it's almost always out of date. It produces a list of potential vulnerabilities that is miles long, leaving security teams scratching their heads on where to even begin. And perhaps the most serious of all, it only covers about 5% of the attack surface because

out of 100+ attack vectors – all very real and scary – it only covers unpatched software vulnerabilities.

In order to truly enhance cybersecurity posture and improve resilience, organizations need a risk-based vulnerability management approach that not only identifies vulnerabilities across all assets, but also prioritizes the action items based on business criticality and risk. Prescriptive insights into what to fix first can help security teams maximize breach risk reduction in the most efficient manner possible.

HOW BALBIX CAN HELP



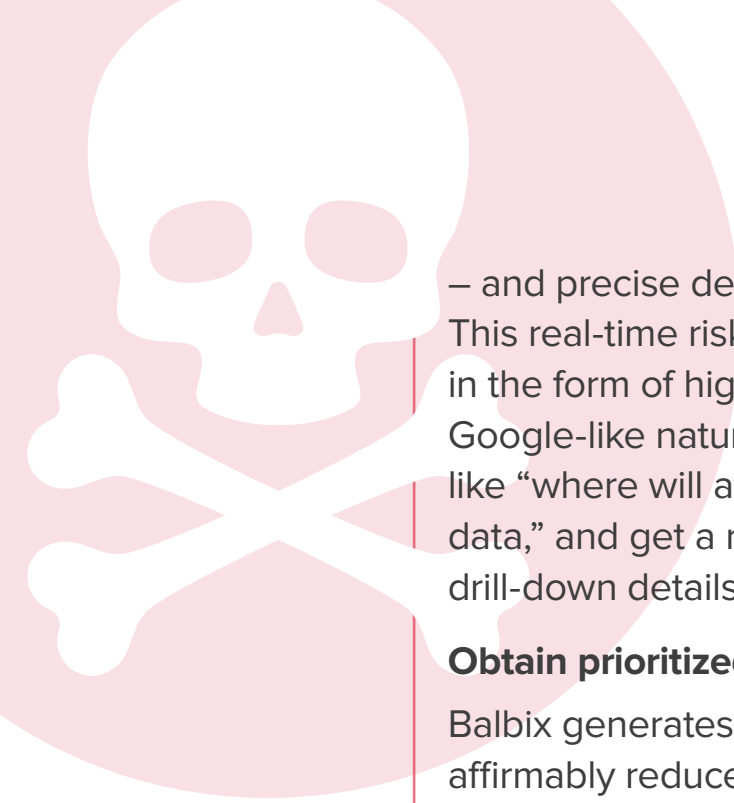
Balbix uses deep learning and advanced AI algorithms to enable you to:

Understand your attack surface

Balbix continuously observes your extended enterprise network inside-out and outside-in, to discover the attack surface and analyze the hundreds of millions (or more) of data points that impact your risk.

Get an accurate read on your risk

Balbix calculates your enterprise's real-time risk, taking into account open vulnerabilities, business criticality, applicable threats and the impact of compensating controls. Analysis of all possible breach scenarios – the various combinations of attack starting points, target systems and propagation paths



– and precise determination of the riskiest scenarios is key. This real-time risk model is surfaced to relevant stakeholders in the form of highly visual drill-down risk heatmaps and Google-like natural-language search. You can ask questions like “where will attacks start” or “what is the risk to customer data,” and get a relevant, highly visual answer, along with drill-down details on how to mitigate the risk.

Obtain prioritized action items with prescriptive fixes

Balbix generates a prioritized list of actions that will affirmably reduce risk. Security posture issues with the greatest risk are addressed first before working down the list of smaller contributors. For each issue, responsible owners for the corresponding assets are identified and then prioritized tickets containing all relevant context are generated and assigned to these owners. Progress is closely tracked and fed back to relevant stakeholders.