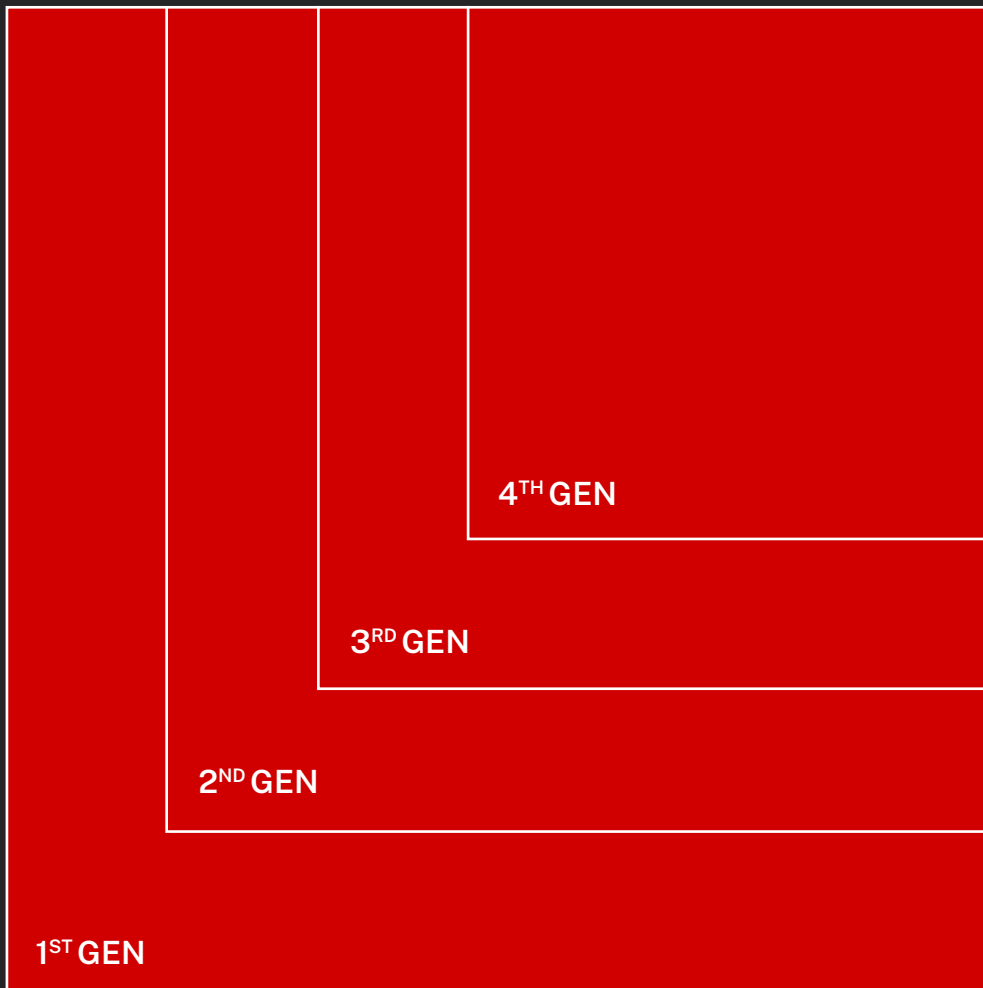
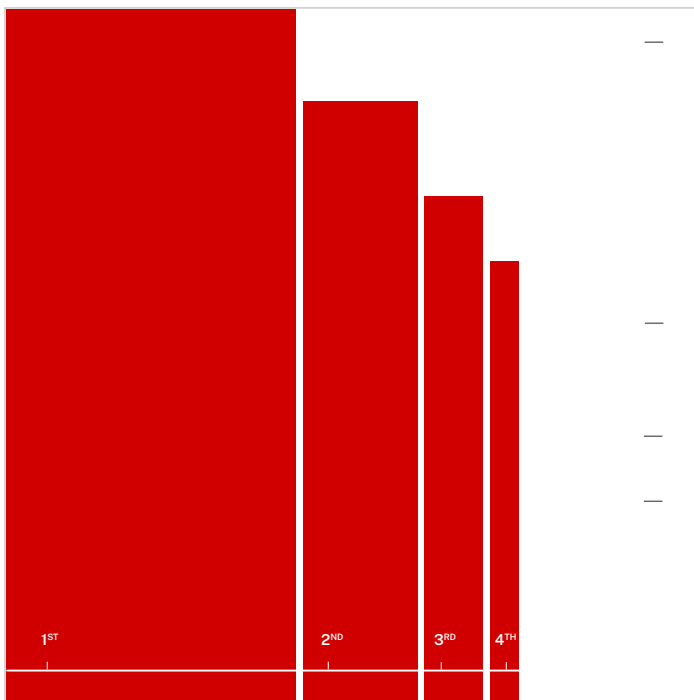


The Most Comprehensive Guide to Vulnerability Prioritization

From 1st to 4th Generation



The Most Comprehensive Guide to Vulnerability Prioritization



Staying ahead of threats requires more than reactive measures — it demands foresight and precision. Enter the 4th generation of vulnerability prioritization, a paradigm shift redefining how organizations approach their vulnerability management strategies. But what exactly is this new wave of prioritization, and why is it generating so much buzz?

In this ebook, we'll explore the principles of fourth-generation vulnerability prioritization, how it differs from previous methods, the cutting-edge technologies that power it, and why it might bolster your organization's defenses in an increasingly complex threat landscape.

Definitions and Objectives

Vulnerability prioritization is the process of identifying and ranking software or system vulnerabilities based on their potential risk to an organization. The goal is to focus remediation efforts on the most critical vulnerabilities that could lead to significant damage if exploited.

The concept of vulnerability prioritization has evolved through four generations, each reflecting technological advancements, threat landscapes, and the methodologies used to assess and manage vulnerabilities. Each generation builds on the previous one, adding more layers of context, intelligence, and automation to help organizations manage vulnerabilities more effectively and efficiently.

“

Each generation builds on the previous one, adding more layers of context, intelligence, and automation.”

1st Generation Severity-based Vulnerability Prioritization

Ranking Vulnerabilities Based on Severity Alone

1st generation vulnerability management focused primarily on identifying and cataloging vulnerabilities. This approach was largely reactive, relying on basic tools and scanners to detect known vulnerabilities in systems and networks. The process was often manual, with security teams running scans once every few months and then prioritizing vulnerabilities based on severity ratings provided by scanners before applying patches based on some acceptable rating criteria. 1st generation vulnerability prioritization relied heavily on the Common Vulnerability Scoring System (CVSS). CVSS provides a numerical score (0-10) that represents

the severity of a vulnerability, considering factors like exploitability and impact on confidentiality, integrity, and availability.

While CVSS is helpful in understanding vulnerability severity, it assumes worst-case scenarios and does not account for an organization's specific context. This approach often results in a large number of what appear to be high and critical-severity vulnerabilities that require immediate remediation, overwhelming security teams when, in reality, only a fraction are exploitable.

“

Common Vulnerability Scoring System (CVSS). CVSS provides a numerical score (0-10) that represents the severity of a vulnerability.”

1st Generation



Table 1: Severity-based Vulnerability Prioritization

**1st Gen
Vulnerability
Prioritization**

CVSS Based

	Windows Server	Windows Server	Windows Server	Windows Workstation	Windows Workstation	Linux Sever	Linux Sever	Networking Asset	Networking/Security	Linux Sever	Windows Server	Linux Sever	Storage	Storage	Storage	Windows Workstation
CVE: SW Vuln -1	C	C	C	C	C	C	C				C	C		C		C
CVE: SW Vuln -2	H	H	H	H	H	H	H	H	H	H	H	H		H		H
CVE: SW Vuln -3	H	H	H	H	H	H	H	H	H	H	H	H		H		H
CVE: SW Vuln -4			C			C		C	C	C	C	C		C		C
CVE: SW Vuln -5	H	H	H	H	H	H	H	H	H	H	H	H		H		H
CVE: SW Vuln -6	H	H	H	H	H	H	H	H	H	H	H	H		H		H
OS -EOL																C
Misconfigured Security Group Membership	L	L	L	L	L	L	L	L	L	L	L	L		L	L	
Self Signed Certificate	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C	C
Exposed S3 Bucket													H		H	

Table 1 shows the vulnerabilities (not just CVEs but misconfigurations, end-of-life OS and other exposure types) in the right-hand column for each asset listed in the top row. The CVSS score (L=low, H=high, C=critical) is then shown for each unique vulnerability (each row). In this typical example, the CVSS scores are identical for each asset, and nearly all (87%) are classified as critical or high.

CVSS-based prioritization makes several key assumptions that limit its accuracy:

Conditions for exploitability are met.

Exploitability assumes threat intent and maturity.

No consideration is given to the environmental context or existing security controls.

While CVSS v3.1 introduced configurations for temporal and environmental factors, manually adjusting these for millions of vulnerability instances proved impractical.

2nd Generation Threat-based Vulnerability Prioritization



Threat-based Vulnerability Management (TBVM) prioritizes CVEs based on the threat level.”

Adding Threat Information

2nd generation vulnerability prioritization introduced threat context. By incorporating external threat intelligence, organizations could focus on software vulnerabilities that were most likely to be exploited, thus making their vulnerability management processes more dynamic and responsive to the evolving threat landscape.

Threat-based Vulnerability Management (TBVM) prioritizes CVEs based on the threat level, reducing the number of vulnerabilities marked high or severe compared to severity-based models.

2nd Generation

Table 2: Threat-based Vulnerability Prioritization

2nd / 3rd Gen Vulnerability Prioritization
TBVM: Threat Based

	Production Domain Controller	Production Exchange Server	Web Server	Domain Admin Workstation	Front Desk Workstation	Staging Web Server	Dev Web Server	Core Router	WAF	Linux Compute Server (Java)	Windows Cloud Compute	Code Repository	Production S3	Database Server	Dev S3	Windows OT Controller
CVE: SW Vuln-1	C	C	C	C	C	C	C				C	C		C		C
CVE: SW Vuln-2	H	H	H	H	H	H	H	H	H	H	H	H		H		H
CVE: SW Vuln-3	M	M	M	M	M	M	M	M	M	M	M	M		M		M
CVE: SW Vuln-4			C			C		C	C	C	C	C		C		C
CVE: SW Vuln-5	M	M	M	M	M	M	M	M	M	M	M	M		M		M
CVE: SW Vuln-6	H	H	H	H	H	H	H	H	H	H	H	H		H		H
OS-EOL																C
Misconfigured Security Group Membership	L	L	L	L	L	L	L	L	L	L	L	L		L	L	
Self Signed Certificate	C	C			C	C	C	C	C	C	C	C	C	C	C	C
Exposed S3 Bucket													C		C	

Table 2 shows how adding threat information, such as risk scores and exploit prediction, refines the vulnerability scores so that only 60% of vulnerabilities are scored as high or critical, compared to 87% under the risk-based model

Threat-Based Vulnerability Prioritization evaluates factors such as:

- Known exploits in the wild.
- Adversary intent to exploit specific vulnerabilities.
- Effort involved in exploitation (adversary ROI).
- Availability of exploit kits.

However, TBVM overlooks business-specific environmental factors like exposure, security controls, and business impact. As a result, TBVM often misses critical context, leading to many high-severity, low-impact vulnerabilities being identified for immediate remediation instead of just those that are genuinely high-impact.

3rd Generation Enhanced Threat-based Vulnerability Prioritization

Adding More Context and EPSS

3rd generation vulnerability prioritization provides additional context. Instead of focusing on the vulnerabilities, this approach began to consider factors like asset criticality, exploitability, and potential business impact. Vulnerability management tools became more sophisticated, allowing organizations to prioritize vulnerabilities based on the risks they posed to critical assets. This generation shifted from treating all vulnerabilities equally to understanding which vulnerabilities could cause the most harm if exploited.

3rd generation vulnerability prioritization also incorporates the Exploit Prediction Scoring System (EPSS), which predicts the likelihood of exploiting a vulnerability based on historical data and statistical models.

EPSS is less relevant when a given vulnerability is already known to be exploited in the wild, as it's specifically designed to be an early-warning system for future exploitation. Furthermore, non-software vulnerabilities can not be prioritized because the EPSS prediction model does not focus on them.

“

This generation shifted from treating all vulnerabilities equally to understanding which vulnerabilities could cause the most harm if exploited.”

3rd Generation

4th Generation Risk-based Vulnerability Prioritization

Incorporating Severity, Threat Levels, Exploitability, Security Controls, and Business Impact

4th generation vulnerability prioritization addresses the shortcomings of previous models by integrating comprehensive risk assessment into the prioritization process and extends coverage to all exposure types beyond just

CVEs – from misconfigurations and outdated systems to weak credentials and user risks. This generation of prioritization leverages artificial intelligence and big data analytics to predict which specific exposure instances are most likely to be successfully exploited against the enterprise in the future and are material to the organization, even before they become active threats.

Risk-based prioritization evaluates exposures based on a combination of 5 factors: severity, threat level, exploitability, business impact, and the effectiveness of existing security controls. This ensures that prioritization is based not only on severity but also by specific risk context within the organization.

“


Risk-based prioritization evaluates exposures based on a combination of 5 factors: severity, threat level, exploitability, business impact, and the effectiveness of existing security controls.”

Table 3: Risk-based Prioritization


**4th Gen RBVM:
Exposure
Management
with CRQ**

	Production Domain Controller	Production Exchange Server	Web Server	Domain Admin Workstation	Front Desk Workstation	Staging Web Server	Dev Web Server	Core Router	WAF	Linux Compute Server (Java)	Windows Cloud Compute	Code Repository	Production S3	Database Server	Dev S3	Windows OT Controller
CVE: SW Vuln -1	H	C	M	C	L	L	L				H	H		M		L
CVE: SW Vuln -2	M	C	M	H	M	L	L	H	H	L	M	M		H		L
CVE: SW Vuln -3	M	H	M	M	L	L	L	C	C	L	L	H		M		L
CVE: SW Vuln -4			M			C	C		C	M	L	H		M		L
CVE: SW Vuln -5	M	H	H	H	L	L	L	M	M	L	L	H		M		L
CVE: SW Vuln -6	L	L	M	C	L	L	L	M	C	M	M	H		L		L
OS -EOL																L
Misconfigured Security Group Membership	M	M	L	L	L	L	L	H	L	L	L	L		L	L	
Self Signed Certificate	M	H	C		M	C	L	C	C	H	H	M	C	H	L	C
Exposed S3 Bucket													C		L	


In Table 3, the core factors added on top of exposure severity and threat levels include:

-  **Exploitability**

Exploitability measures how available an asset and its vulnerabilities are to adversaries for exploitation, with external-facing assets being more accessible. This assessment involves determining the ease with which attackers can discover and utilize vulnerabilities.

-  **Business Impact**

Impact refers to the expected loss the enterprise will incur in a successful breach of an asset or application.

-  **Controls Analysis**

Controls analysis involves evaluating the effectiveness and implementation of security controls to protect an organization’s assets from potential threats and vulnerabilities against all Techniques, Tactics, and Procedures (TTPs) used by attackers. This analysis assesses how well these controls can prevent, detect, and respond to attack vectors. It includes reviewing technical controls like firewalls, intrusion detection systems, and encryption and administrative controls such as policies, procedures, and training programs. Controls analysis helps identify gaps in the current security posture, ensuring that defenses are robust enough to mitigate identified risks and enhance the overall resilience of the organization against cyber threats.

One key point to note is that 4th-generation vulnerability prioritization focuses on individual instances of CVEs and other exposures since different instances of the same CVE or misconfiguration may have different levels of exploitability, control effectiveness and business impact.

4th generation emphasizes automation, reducing manual intervention and allowing for real-time prioritization that adapts as new information becomes available. It's a proactive approach that aims to stay ahead of threats by anticipating and mitigating risks before they can be exploited.

AI significantly enhances vulnerability prioritization by bringing advanced capabilities to the process, enabling more precise, efficient, and proactive security management. AI enhances vulnerability prioritization by predicting likely threats, dynamically adjusting risk scores, automating management tasks, providing contextual understanding, continuously learning, correlating threats, optimizing resources, and detecting anomalies.

Overall, 4th generation vulnerability prioritization (or exposure prioritization) transforms vulnerability prioritization from a largely reactive process into a proactive and predictive one, enabling organizations to stay ahead of attackers by focusing on the most relevant and impactful vulnerabilities. This leads to a more secure and resilient IT environment, with reduced risk of breaches and better protection of critical assets.

“

Overall, 4th generation vulnerability prioritization (or exposure prioritization) transforms vulnerability prioritization from a largely reactive process into a proactive and predictive one, enabling organizations to stay ahead of attackers by focusing on the most relevant and impactful vulnerabilities.”

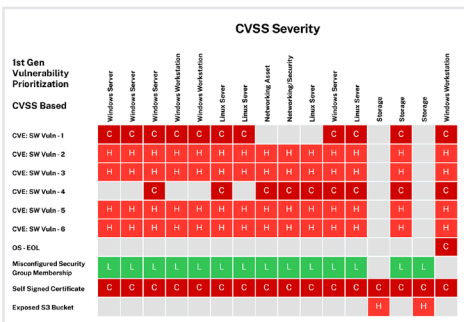
The Crucial Role of 4th Generation Vulnerability Prioritization in Exposure Management

4th generation vulnerability prioritization is key to evolving your vulnerability management strategy to effective exposure management because it offers a comprehensive scope that extends beyond just Common Vulnerabilities and Exposures (CVEs) to encompass a wide range of potential risks, including misconfigurations, outdated systems, weak credentials, and user-related threats. This holistic approach ensures that all security weaknesses are identified and addressed, not just those cataloged in vulnerability databases. Additionally, 4th generation prioritization integrates contextual risk assessment, evaluating factors such as exploitability, business impact, and the effectiveness of existing security controls. This enables a more precise and tailored determination of which exposures pose the greatest threat to an organization's unique environment, allowing for more targeted and effective remediation efforts.

Conclusion

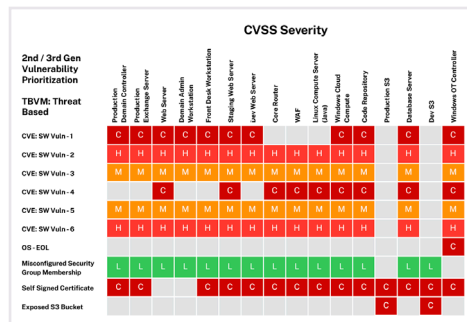
4th generation (i.e., risk-based) vulnerability prioritization allows organizations to identify and address the most risky exposures, not just high-severity or high-threat CVEs. This approach provides a thorough assessment of exposures across all assets in the enterprise.

By implementing risk-based prioritization, only 25% of exposures are classified as critical or high risk, a reduction of 60% from severity-based prioritization. These exposures have the highest impact on the organization and should be remediated first.



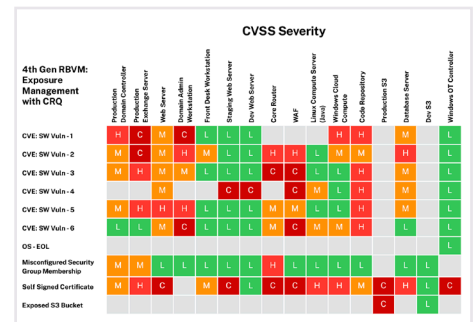
CVSS Based Prioritization
1st Gen VulnManagement

87%
Critical and High



TBVM: Threat Based
2nd/3rd Gen Vuln Management

60%
Critical and High



Risk Based Prioritization
4th Gen Vuln Management

25%
Critical and High

Impact of Vulnerability Prioritization Techniques on Critical and High Vulnerability Counts

The [Balbix exposure management platform](#) implements 4th generation vulnerability prioritization. Telemetry data from your cybersecurity tools is deduplicated, correlated, and then analyzed using [Balbix's AI models](#) to create a unified exposure and risk model. Vulnerability instances and findings (exposures) are prioritized based on severity, threats, exploitability or accessibility, the effectiveness of security controls and business criticality and risk is quantified in dollars (or other monetary

units). This prioritization information is fed into a “next best steps” computation that uses Shapely Econometric Models to calculate enterprise-wide priority for mitigation and remediation actions to burn down risk to acceptable levels. Next best steps are then subdivided into projects, tickets and automated orchestration steps and as issues are fixed, the system automatically performs validation and the cycle continues.



[Request a demo](#) to determine the effectiveness of your risk prioritization program.



About Balbix

balbix.com

Balbix is revolutionizing cyber risk management by providing businesses with the tools to effectively identify, prioritize, and mitigate their most critical security exposures. By integrating data from across the organization and leveraging advanced AI technologies, Balbix offers a unified platform for exposure assessment and risk quantification. Fortune 500 companies trust Balbix to protect their operations and ensure compliance in an ever-evolving threat landscape. Balbix was recognized in Forbes America's Best Startup Employers 2024 by CNBC in their 2022 Top 25 Startups for the Enterprise and ranked #32 on the 2021 Deloitte Fast 500 North America.

