Hive Pro®

White Paper

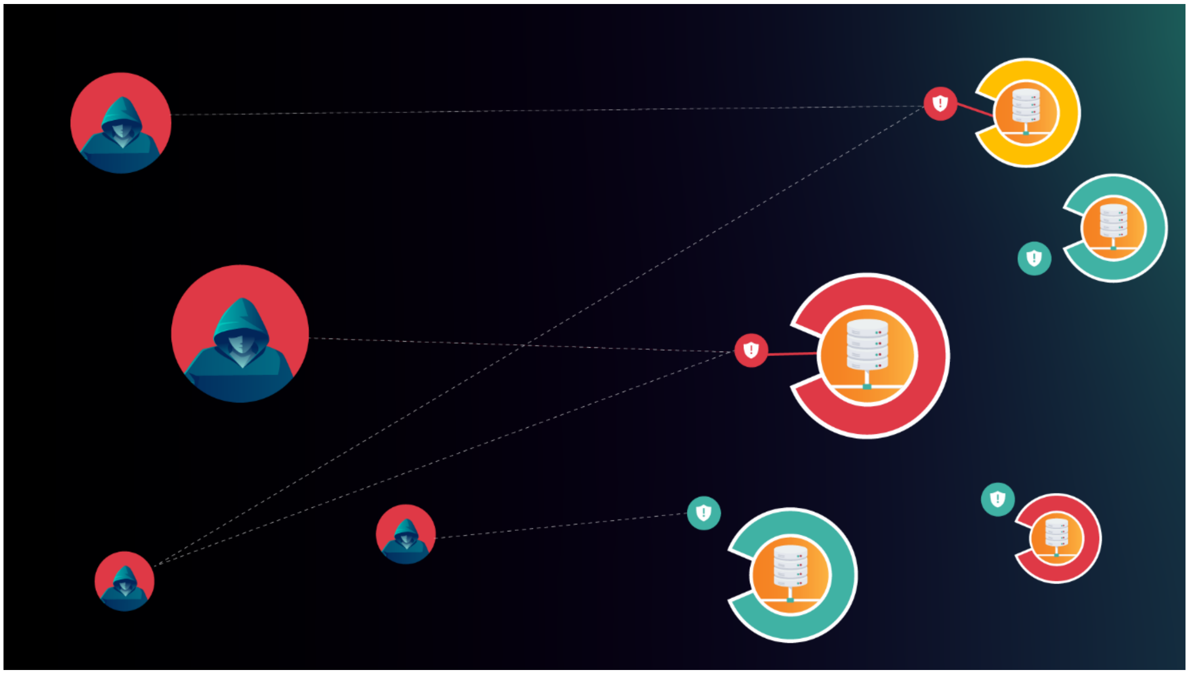
Stop Putting Out Fires: It is Time to Change Vulnerability Management for the Better

From outdated practices to an evolved vulnerability management approach: The key to a resilient security posture.

13800 Coppermine Road,
Dulles Corner, 1st – 3rd
Floors, Herndon, VA
20171, United States

info@hivepro.com
www.hivepro.com

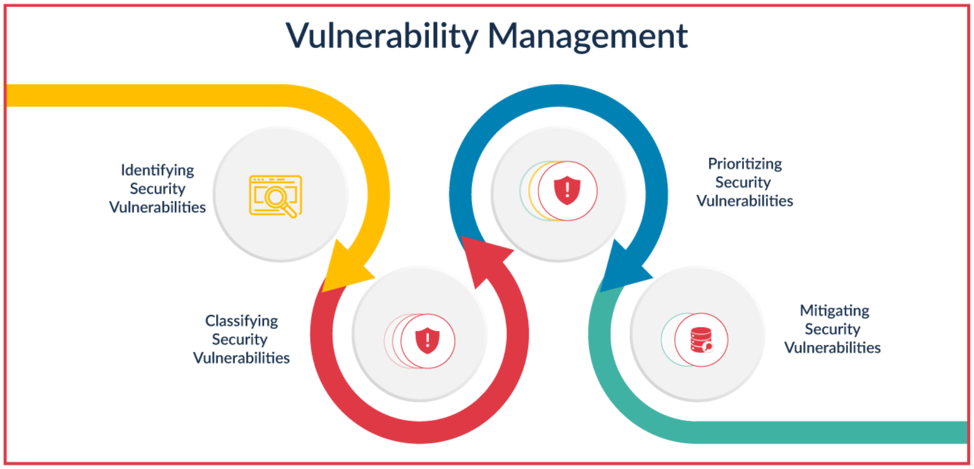
Abstract



This whitepaper explores modern day Vulnerability Management (VM) practices, the shift to risk-based vulnerability management (RBVM) and related fundamental concepts with the objective to emphasize a critical need for improvement. Outdated VM practices and gaps in RBVM are shown to have dire consequences where the absence of complete asset, threat and vulnerability intelligence can lead to severe repercussions. To improve on outdated VM practices, this whitepaper proposes recommendations for enterprises to manage vulnerability risks more efficiently through dynamic threat exposure changes, business-specific risk outlooks, and evolving budgetary needs. We conclude this whitepaper by outlining the benefits of an evolved RBVM approach, which when combined with enhanced asset visibility and Threat Exposure Management, will yield an enhanced security posture, a reduction in technical debt, and a more resilient enterprise.

Table of Content

Introduction


Vulnerability Management
Identifying Security Vulnerabilities
Classifying Security Vulnerabilities
Prioritizing Security Vulnerabilities
Mitigating Security Vulnerabilities

Background and Purpose

At its core, VM is the systematic process of identifying, classifying, prioritizing, and mitigating security vulnerabilities within an organization's infrastructure, applications, and systems. It is a cornerstone of proactive cybersecurity, and without it, organizations would fail to be resilient in the face of mounting and increasingly more costly cyberattacks.

As organizations grapple with an increasingly dynamic vulnerability and threat landscape and several security organization issues: workforce gap, siloed security tools, security data sprawl, asset blind spots, vulnerability scanning blinds pots, and poorly focused vulnerability and threat intelligence, current VM practices are proving outdated and unhelpful. What VM needs is a shift towards resilience in the face of security budget and workforce constraints among the other security organization issues listed above.

This shift must at its core, minimize an organization's attack surface by addressing weaknesses specific to an organization that could and most likely will be exploited by malicious actors. Such a perspective shift will enable Security teams to properly focus their limited resources on their most pressing needs as they continuously evolve and mature. Inherently, this shift is asking for VM to evolve its risk-based approach to integrate the attacker's perspective, which is asking a lot of VM as we will expand upon in later sections.

In sum, this whitepaper explores the multifaceted realm of VM, its significance, current practices, and the outstanding need for evolution. We will assert that the future of VM lies in evolving a risk-based perspective in VM to integration the Threat Exposure Management (TEM) outlook. The proposed way forward will clarify how this shift will yield enhanced security functions, cost savings, reduced dependence on full-time employees, and more optimized technology investment. Ultimately, this shift will build resiliency into any Security organization.

What is Vulnerability Management?

Defining Vulnerability Management

Vulnerability Management (VM) is a strategic and systematic approach to identifying, assessing, prioritizing, and mitigating security vulnerabilities within an organization's information technology infrastructure, applications, and systems. VM practices encompass the processes, tools, and practices used to proactively monitor, detect, and remediate vulnerabilities with the objective of safeguarding critical assets housing sensitive data. Additionally, VM practices support regulatory compliance mandates and the maintenance of a robust security posture by ensuring that potential weaknesses are promptly identified and addressed according to business needs and objectives, thus minimizing the likelihood of security breaches and data compromises.

The Evolution to Risk-Based Vulnerability Management (RBVM)

Compliance-Driven VM

235%
decrease in global ransomware attacks in 2022
(Source: parachute)

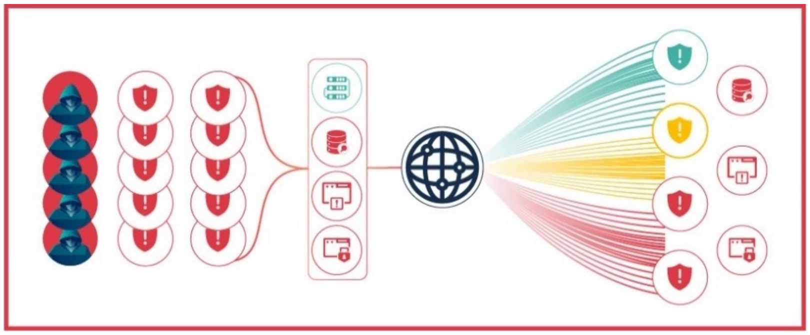
65%
of organizations who experienced a ransomware attack faced more than 6 days of downtime afterward
(Source: parachute)

Compliance is essential for ensuring that organizations meet the requirements of regulatory and industry standards lest they incur penalties, fines, and sanctions. Compliance also facilitates in building and maintaining customer trust. Most organizations are eager to comply; however, they oftentimes find compliance requirements too complex, everchanging and difficult to understand. Nonetheless, they are held to many regulatory and industry standards, such as PCI DSS, HIPAA, NIST, ISO 27001, SOC2, FISMA, and GLBA, and these regulatory and industry standards all have in common a requirement for organizations to implement vulnerability management practices.

For example, PCI DSS (Payment Card Industry Data Security Standard) requires organizations that accept credit card payments to conduct regular vulnerability scans and penetration testing to identify vulnerabilities in their systems. GLBA carries the same requirement for wide-reaching financial institutions, and in similar fashion, so does HIPAA (Health Insurance Portability and Accountability Act) in its requirements for the healthcare industry to implement security measures to protect personal health information, including vulnerability management. Although these regulatory and industry standards promote a good, generic practice and miss the idea of risk-based vulnerability management, this doesn't matter much for many organizations who have not yet suffered a severe loss from a breach. Until they do, most organizations default to security for compliance's sake rather than security for security's sake. The continuous process of evaluating risks is inherent to the security practice, but it doesn't carry teeth like compliance, just the possibility without accurate probability of compromise.

Things are slowly changing now, though. And this is mostly because the rate of attack and breaches are globally wreaking havoc. The little weight that the possibility of attack and tenuous probability of compromise carried in the past is no longer applicable.

The Shift to Risk-Based VM



Because it is entirely impractical to resolve all vulnerabilities and meet compliance-measures in a bullet-proof manner, risk-based vulnerability management provides a tailored and responsible approach to risk reduction and vulnerability management by proposing the prioritization and remediation of vulnerabilities based on their potential impact on an organization's security posture and business operations. Ideally, by aligning vulnerability management efforts with the organization's risk tolerance and strategic objectives, risk-based vulnerability management helps security teams focus their resources and attention on addressing the vulnerabilities that pose the greatest threats. This approach ensures that remediation efforts are prioritized effectively, ultimately reducing the organization's overall risk exposure, and enhancing its cybersecurity resilience.

We define **"risk"** below to surface several issues that have been widely noted regarding **current-day RBVM practices.**

RISK = THREAT [likelihood] x VULNERABILITY x PROBABILITY of occurrence x IMPACT / CONTROLS in place

(NIST 800-30 2002)

Threat Likelihood	How motivated and capable is the threat source?
Vulnerability	How sufficient are your controls in place, and can they outweigh the risk factors on their shoulders? Is the vulnerability exploitable in the wild, and how easily?
Probability of Occurrence	What is the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities in your environment specifically?
Impact	What do you stand to lose if the threat materializes?
Controls in place	How sufficient are your controls in place, and can they outweigh the risk factors on their shoulders?

Current risk-based vulnerability management practices put all of their weight on only two parts of the whole equation above: "vulnerability" and "controls in place". What takes over in risk scoring are CVSS scores aligned to just those vulnerabilities logged in CVE databases and not much more. Most organizations largely miss everything else either because they lack sufficient threat intelligence, testing mechanisms to assess the most accurate impact, and other factors to rate subjective probability of occurrence, or because all of these capabilities and intelligence is present in their Security organization however the intelligence is siloed due to siloed Red and Blue Teams with non-existent efforts to consolidate intelligence.

The ideal of risk-based vulnerability management is to prioritize and remediate risks based on business-needs balanced against outstanding threats. Unfortunately, this ideal is missing a ton of context around threats, the probability of their occurrence, and the true impact if they happen to materialize.

The Gaps in Today’s Risk-Based Vulnerability Management

Over-Reliance on CVSS Scores

The over-reliance on Common Vulnerability Scoring System (CVSS) scores has emerged as a significant hindrance in effective vulnerability management practices. This over-dependence on CVSS is primarily attributed to its generic nature, subjective scoring perspective, and the absence of evolving score rankings. CVSS scores, while a valuable tool, tend to provide a one-size-fits-all approach to vulnerability prioritization, often failing to capture the nuanced context of specific organizational environments. The subjective nature of scoring, where different assessors might assign different scores for the same vulnerability, introduces inconsistencies. Moreover, CVSS scores lack the ability to evolve alongside the dynamic threat landscape, leaving security teams with static metrics that may not reflect the actual risk posed by vulnerabilities in real-time. These limitations underscore the critical need for a more holistic and adaptable approach to vulnerability management that considers factors beyond CVSS scores to make informed decisions and prioritize remediation efforts effectively.

Lacking a True Risk-Based Perspective

Enterprises that neglect to adopt a business-risk-based perspective in their vulnerability management practices are inadvertently undermining their ability to achieve successful outcomes in cybersecurity. This shortsightedness leads to a significant disconnect between technical vulnerabilities and the organization's overarching business priorities and risk profile. It is imperative to recognize that a risk-based approach to vulnerability management integrates business priorities, risk appetite, and tolerance levels into the decision-making process. As highlighted by industry experts and cybersecurity thought leaders, this approach aligns security efforts with the organization's strategic objectives, ensuring that resources are allocated to address vulnerabilities that pose the most substantial business impact rather than merely focusing on technical severity. Without this alignment, organizations may find themselves investing disproportionately in areas that do not effectively safeguard critical assets or align with their risk management strategies. In today's rapidly evolving threat landscape, taking a risk-based approach to vulnerability management is not just a recommendation; it's a strategic imperative for any organization seeking to fortify its cybersecurity defenses intelligently and efficiently.

Absence of Business-Specific Asset Intelligence

Effective VM requires an understanding of an organization's assets and their importance to the business. Without this critical information, vulnerability management practices can fall short of meeting an organization's unique risk tolerance and operational requirements. The absence of business-specific asset intelligence results in a one-size-fits-all approach that fails to account for an organization's distinct infrastructure, assets, and priorities. This generic approach can lead to misallocated resources, where vulnerabilities with minimal impact on the organization's core operations may be given undue attention, while critical vulnerabilities remain overlooked. Furthermore, it hampers the ability to assess vulnerabilities in the context of the organization's specific business processes and critical assets. To achieve robust vulnerability management, organizations must continuously update and integrate asset intelligence, ensuring that risk assessments are aligned with their specific operational landscape and security needs. This tailored approach is essential to effectively prioritize and remediate vulnerabilities, enhancing overall security posture and resilience.

The Need for Up-to-Date Threat Intelligence

VM should not operate in isolation from the evolving threat landscape. Without access to up-to-date threat intelligence, VM teams may miss vulnerabilities that are actively being targeted by threat actors, leaving the organization exposed to real-world threats. It serves as the cornerstone for identifying, prioritizing, and mitigating vulnerabilities in a proactive and informed manner. Without timely and accurate threat intelligence, vulnerability management practices risk being outdated and reactive, leaving organizations vulnerable to emerging threats. Current threat intelligence provides critical insights into the tactics, techniques, and procedures employed by threat actors, enabling security teams to anticipate and defend against potential exploits. Up-to-date threat intelligence is the linchpin that transforms vulnerability management from a mere checklist into a dynamic and adaptive security strategy, capable of safeguarding organizations against an ever-changing threat landscape.

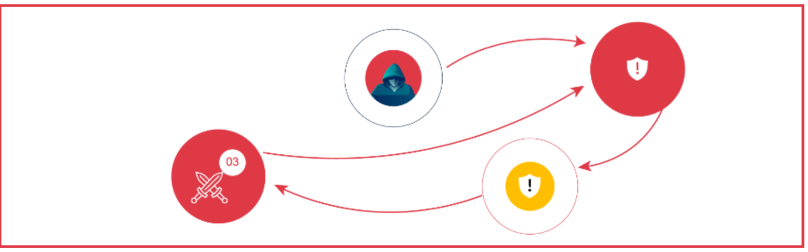
Compounding Issues in Vulnerability Management

Silos and Fragmentation

Average Patch Delay ≥ 12 days

VM often operates in isolation from broader security functions, leading to fragmented efforts and a lack of integration with overall risk management. Operating vulnerability management in isolation and as a fragmented function disconnected from broader security functions and risk management can be highly detrimental to an organization's cybersecurity posture; such isolation can lead to critical vulnerabilities going unnoticed and unaddressed, resulting in increased exposure to cyber threats. According to a Ponemon Report, "silo and turf issues delay patching. 88% of respondents say their team is not fully responsible for patching vulnerabilities and they have to coordinate with other teams. As a result, patching is delayed an average of 12 days."[1] Siloed vulnerability management lacks the lacks the necessary context to prioritize vulnerabilities effectively, as it may not consider an organization's unique risk profile or the potential impact of vulnerabilities on critical business processes. Furthermore, the absence of integration with broader security functions can lead to disjointed efforts, duplicated work, and a failure to align vulnerability management with the organization's overall risk management strategy. In today's dynamic threat landscape, where cyberattacks continually evolve in sophistication and scale, fragmented vulnerability management operations leave organizations vulnerable to emerging threats and undermine its ability to respond proactively to security challenges.

Siloed Tools, Lacking Integration, and Security Tool Sprawl in Vulnerability Management

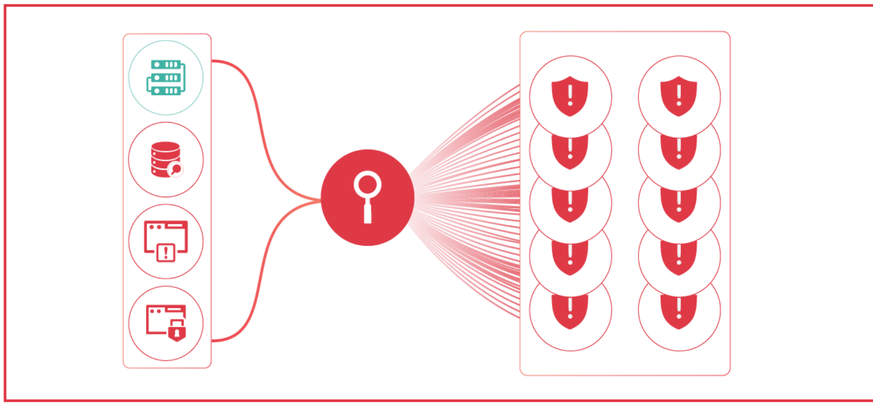


Organizations often deploy a multitude of security tools and solutions in isolation, each serving a specific purpose but rarely communicating or sharing critical information with one another. This is not a fault of organizations as much as it is of vendors vying for niche spaces without offering robust integration capabilities. This lack of integration creates silos where data remains fragmented, hindering the ability of organizations to gain a holistic view of their security posture. Subsequently, VM teams are left grappling with disjointed data, leading to inefficiencies in vulnerability detection, prioritization, and remediation. Security tool sprawl exacerbates the "cyber workforce gap" problem in that organizations amassing an ever-growing arsenal of disparate tools have not as many hands to operate them to full potential and with ease. The result is not only increased operational complexity but also a heightened risk of overlooking critical vulnerabilities, misallocating resources, and burning out the Security workforce.

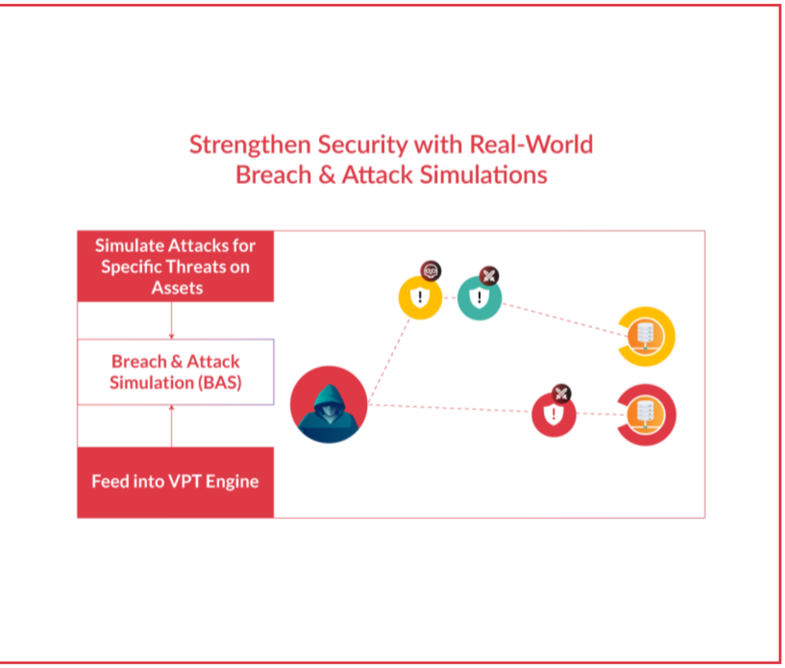
[1] *https://media.bitpipe.com/io_15x/io_152272/item_2184126/ponemon-state-of-vulnerability-response-.pdf*

False Positives and Negatives

Automated scanning tools often generate false positives (identifying vulnerabilities that don't exist) and false negatives (missing real vulnerabilities). False positives can lead to wasted time and resources in investigating and addressing non-existent issues. False negatives are even worse in that when real vulnerabilities are missed during scans, critical security weaknesses remain unaddressed and expose organizations to potential cyber threats. The only way forward in minimizing these inaccuracies is improved tooling, but more specifically improved validation and the integration of multiple vulnerability sources and contextual intelligence.



Where Is Security Control Testing and Optimization?


Strengthen Security with Real-World Breach & Attack Simulations
Simulate Attacks for Specific Threats on Assets
Breach & Attack Simulation (BAS)
Feed into VPT Engine

Performing effective vulnerability management without "breach and attack simulation," "security control posture management" will be an uphill battle for any enterprise. These tools provide a continuous and critical layer of assurance, allowing organizations to verify that their security controls are configured correctly and are capable of withstanding real-world threats. Without them and only with point-in-time testing conducted by PTaaS vendors or Red Teams for audit purposes, organizations are left with a significant blind spot in their security posture. Vulnerability management becomes a precarious task as it relies on the assumption that controls are adequately configured, and that the data collected during assessments accurately represents the security readiness. This lack of real-world testing and validation can lead to misinformed decisions, missed vulnerabilities, and an increased risk of security breaches, ultimately jeopardizing the organization's security and resilience. Incorporating these tools is essential to bridge the gap between vulnerability identification and effective risk mitigation, providing the confidence and agility needed to protect against modern cyber threats.

Without Automating VM, Enterprises Are Outpaced by Threat Actors

Companies are often faced with a backlog of 100,000 vulnerabilities within their systems. Although not all vulnerabilities are exploitable—say 85% of them not being exploitable, still 15,000 remain and surely, they are. The root cause of this problem is time. There is not enough time to manually detect, prioritize, and remediate each vulnerability. This process takes 21 minutes alone for each vulnerability. That means, 430 working days of 12 hours each day to clear this backlog considering the 15,000 vulnerabilities. More new vulnerabilities are reported each day. Enterprises must turn to automation to manage the sheer volume of vulnerabilities coupled with the rapidly advancing threat landscape. There are automated scanning, prioritization, and patch management tools, though the current security tool landscape is as fragmented and siloed as VM practices are, which makes sense considering the interconnected nature of people, process, and technology.

Clearing this backlog of **15,000 vulnerabilities** would require **430 working days,** assuming **12-hour workdays.**

The Overall Impact of Outdated Vulnerability Management

Security Implications

The security implications of poor or outdated vulnerability management practices are profound and can have devastating consequences for organizations. Failing to address vulnerabilities in a timely manner can leave systems and data exposed to cyberattacks, resulting in data breaches, financial losses, reputational damage, and regulatory penalties. Attackers often target known vulnerabilities because they represent low-hanging fruit. As a result, organizations relying on outdated VM are at a higher risk of security breaches, data leaks, and financial losses.

According to the Verizon Data Breach Investigations Report (DBIR) (2021), 85% of data breaches involved vulnerabilities that were over a year old, highlighting the persistence of outdated vulnerabilities in attack vectors.

→

Verizon's latest DBIR (2023) found that exploits peaked 17 days after attackers discovered a flaw. Take this statistic, for example, Log4J according to the DBIR: Over 32% of all Log4j vulnerability scanning occurred in the first 30 days after release.

The immediate exploitation of **Log4j vulnerabilities** shows why organizations must **respond faster to new threats.** Additionally, it emphasizes the critical importance of timely vulnerability management in safeguarding against cyber threats and the severe consequences that can arise from negligence in this area.

Costs of Outdated VM Practices

Outdated VM practices can have a detrimental impact on an organization's overall cybersecurity posture, financial stability, and reputation. In a world where cyber threats are constantly evolving, failure to adapt to evolving best practices in VM can result in dire consequences and costs that are never immediately projected for due to those costs being whim to the erratic nature of threat actors.

The costs associated with outdated VM practices can be substantial.

Remediation Costs

Delayed vulnerability remediation often requires more extensive and costly efforts to mitigate the associated risks.

Regulatory Fines

Non-compliance with data protection and cybersecurity regulations can result in significant fines.

Reputation Damage

Security incidents stemming from unaddressed vulnerabilities can tarnish an organization's reputation and lead to customer attrition.

Legal Consequences

Security breaches may lead to legal action and lawsuits, further increasing costs.

Loss of Competitive Advantage

Organizations that cannot demonstrate robust security practices may lose business opportunities or partners.

Necessary Changes in Vulnerability Management

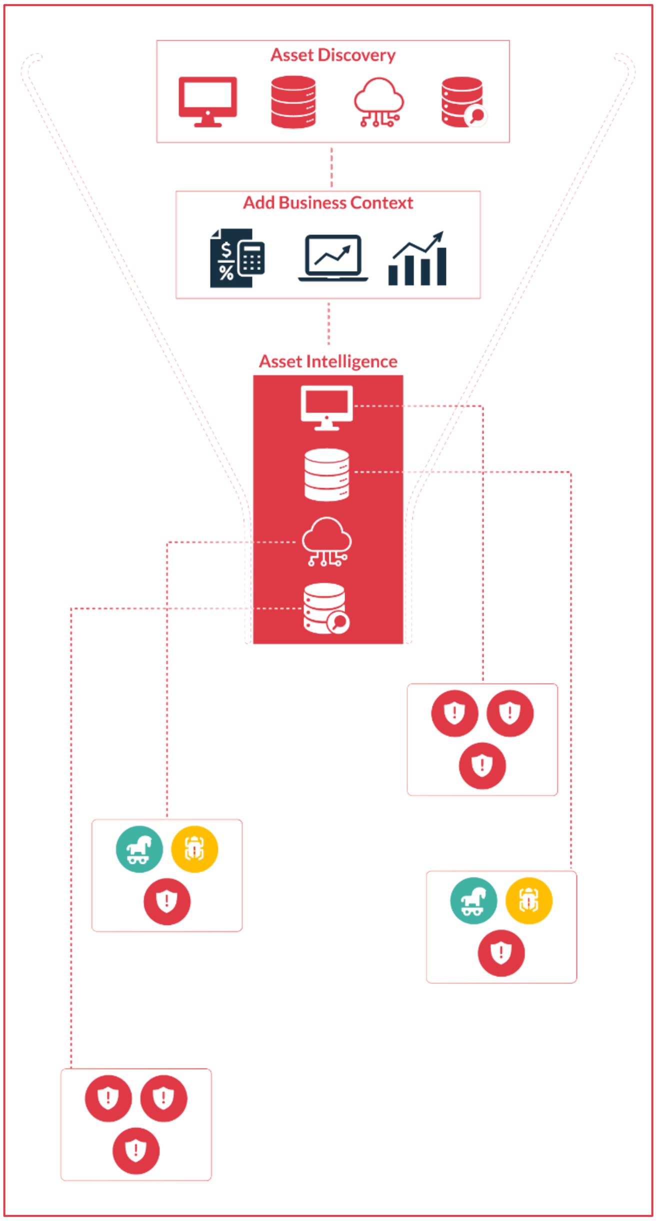
Shifting Towards a Risk-Based Perspective

To address the limitations of current VM practices, organizations must shift towards a risk-based perspective. This approach involves:

Understanding Business Context and Asset Criticality

Identifying critical assets, business processes, and their dependencies to prioritize vulnerabilities that pose the greatest risk to the organization. Up-to-date asset intelligence and effective asset management are integral components of a robust vulnerability management program. These elements play a crucial role in aligning vulnerability management with an organization's business risks and context.

Here's why they are so important:



Risk Prioritization:

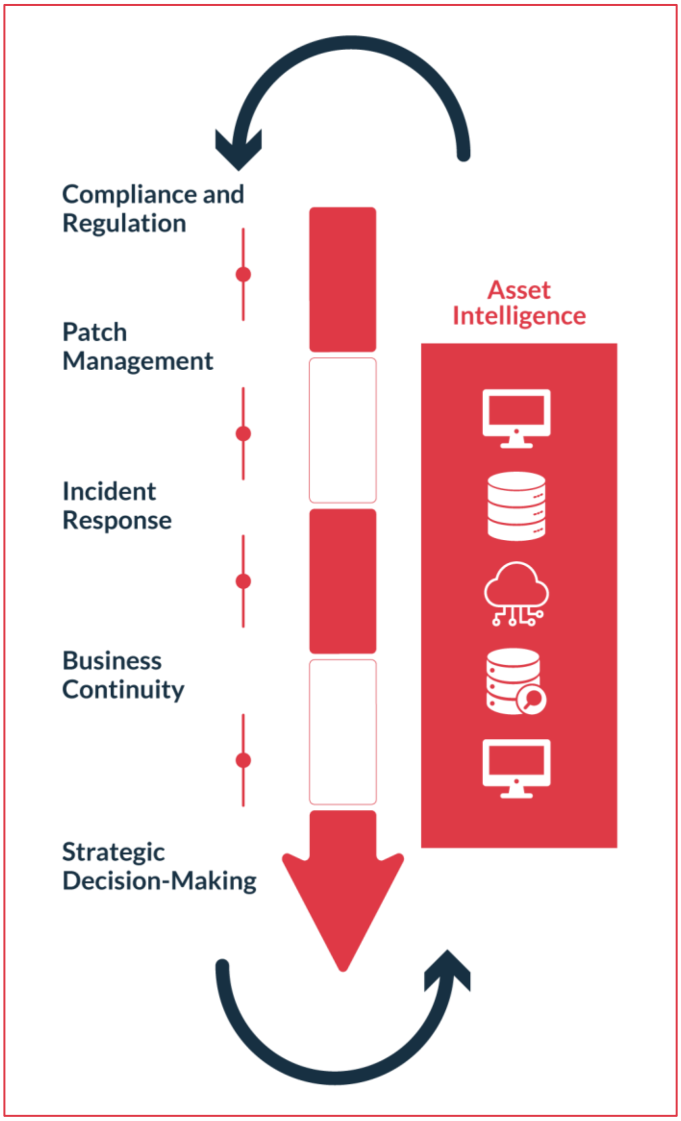
Businesses operate in dynamic environments, where the importance and criticality of assets can change rapidly. Effective asset intelligence and management allow organizations to understand the business impact of each asset. This, in turn, helps prioritize vulnerabilities based on their potential impact on business operations. For example, a vulnerability in a critical customer database should take precedence over one in a less vital system.

Resource Allocation:

Resources, including time, budget, and personnel, are finite. Asset intelligence enables organizations to allocate these resources more effectively by focusing on the most critical assets and vulnerabilities. Without this insight, vulnerability management efforts can become dispersed and inefficient, leading to an inability to address high-risk vulnerabilities in a timely manner.

Contextual Awareness:

Vulnerabilities should not be addressed in isolation. Asset intelligence provides context by helping organizations understand how assets are interconnected and how they support various business processes. This contextual awareness enables security teams to assess the potential ripple effects of a vulnerability in the broader business context.



Compliance and Regulation:

Many industries are subject to regulatory requirements that mandate the protection of specific types of data or systems. Up-to-date asset intelligence is essential for ensuring compliance. Failure to do so can result in regulatory fines and legal consequences.

Patch Management:

Asset intelligence informs patch management strategies. Knowing which assets are most critical allows organizations to prioritize patching efforts. This is especially important when dealing with a large number of assets and limited patching windows.

Incident Response:

In the event of a security incident, understanding the business context of assets is invaluable. It helps incident response teams make informed decisions about containment and remediation. For instance, they can quickly identify which assets require immediate attention to minimize the impact on critical business operations.

Business Continuity:

Asset intelligence also supports business continuity and disaster recovery planning. It allows organizations to identify which assets are essential for maintaining core business functions and develop contingency plans to protect those assets in case of disruptions.

Strategic Decision-Making:

Beyond day-to-day vulnerability management, asset intelligence feeds into strategic decision-making. It enables organizations to plan for future investments in security technologies and controls based on the evolving business landscape.

Tailored Prioritization

Customizing vulnerability prioritization based on the organization's unique risk profile, rather than relying solely on CVSS scores. The importance of vulnerability prioritization as both a process and technology within vulnerability management cannot be overstated in today's complex cybersecurity landscape. Vulnerability management involves dealing with a multitude of vulnerabilities, each potentially posing a different level of risk to an organization.

Here's why prioritization is crucial:

Resource Optimization:

Not all vulnerabilities are created equal. Some have a higher potential for exploitation and could result in severe consequences, while others may be less critical. Prioritization helps organizations allocate their limited resources – such as time, personnel, and budgets – to address the most pressing vulnerabilities first. This prevents wasting effort on low-risk issues and ensures that critical vulnerabilities are addressed promptly.

Risk Reduction:

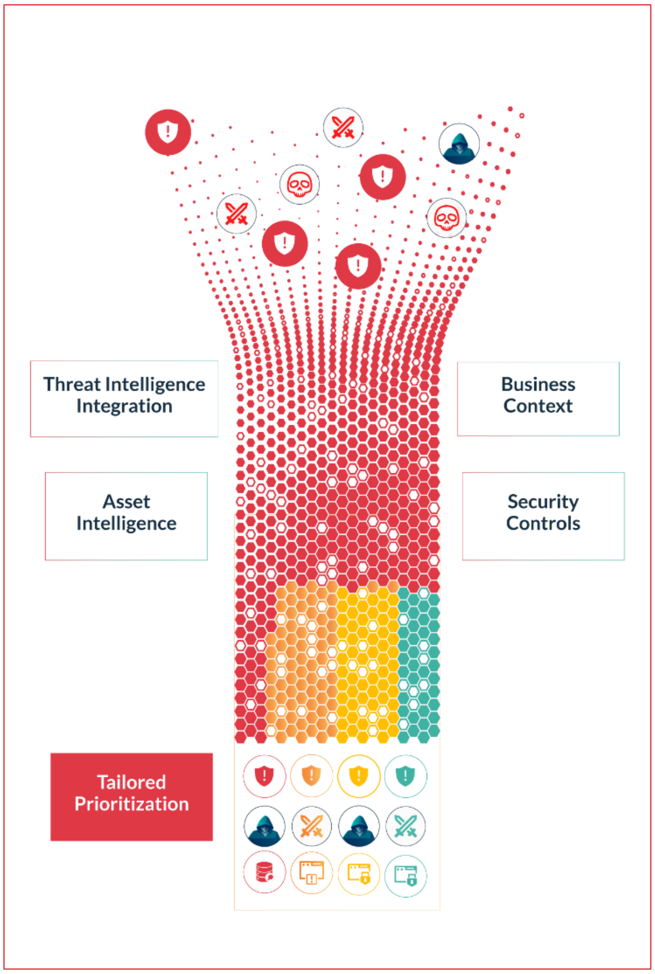
Vulnerability prioritization is fundamentally about risk management. By focusing on vulnerabilities that present the greatest risk, organizations can effectively reduce their overall risk exposure. This reduces the likelihood of a successful cyberattack and the potential impact of such an event.

Efficiency:

Modern vulnerability management solutions leverage technology, such as vulnerability scanners and risk assessment tools, to automate the identification and prioritization of vulnerabilities. This streamlines the process and ensures that security teams are focusing their efforts where they matter most. Without technology, manual assessment and prioritization can be time-consuming and prone to human error.

Adaptation to Evolving Threats:

The threat landscape is constantly evolving, with new vulnerabilities and attack techniques emerging regularly. Vulnerability prioritization should not be a one-time effort but an ongoing process that adapts to changing circumstances. Technology can help organizations stay current with the latest threat intelligence and adjust their prioritization accordingly.

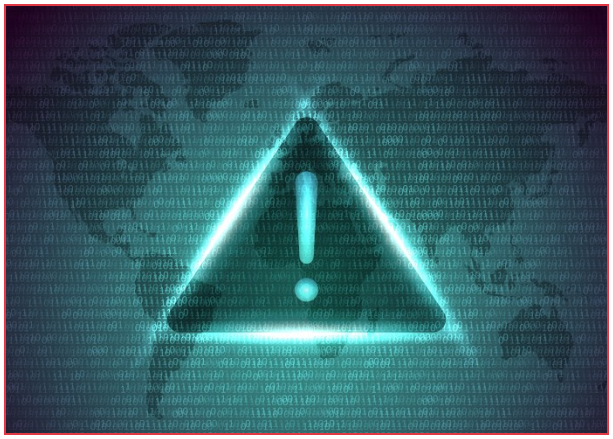


Compliance and Reporting:

Many regulatory frameworks require organizations to have a structured vulnerability management program in place. Prioritization plays a crucial role in demonstrating compliance by showing that the organization is actively addressing high-risk vulnerabilities.

Incident Prevention:

Effective prioritization helps prevent security incidents by addressing vulnerabilities before they can be exploited. This proactive approach is far more desirable than dealing with the aftermath of a successful breach.



Business Continuity:

Cyberattacks can disrupt operations and impact an organization's ability to serve its customers. By prioritizing vulnerabilities that could lead to business-critical systems being compromised, vulnerability management helps protect business continuity.

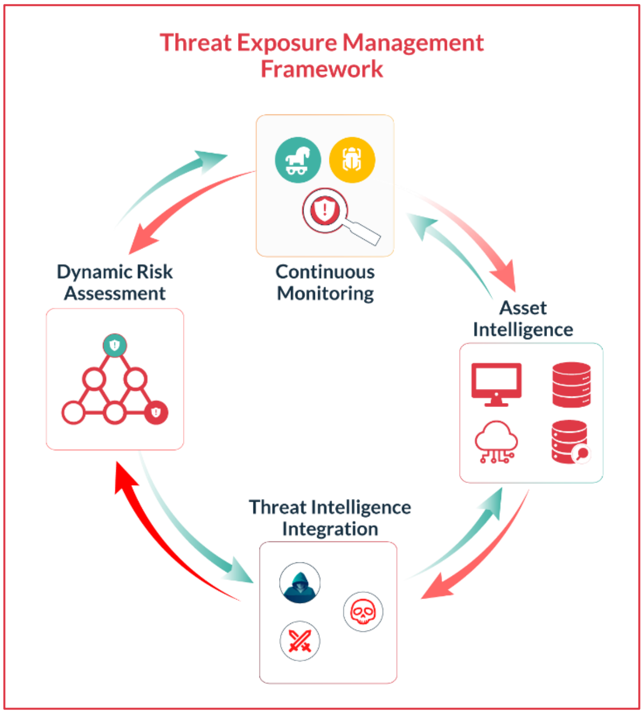
Embracing a Threat Exposure Management Framework

Threat Exposure Management (TEM) is an emerging framework that complements VM by providing a holistic view of an organization's exposure to threats.

Key elements of TEM include:

Continuous Monitoring:

Real-time monitoring of vulnerabilities and threats, allowing organizations to respond promptly to changing conditions.


Threat Exposure Management Framework
Continuous Monitoring
Asset Intelligence
Threat Intelligence Integration
Dynamic Risk Assessment

Asset Intelligence:

Gaining a deep understanding of an organization's assets, the criticality of those assets, their importance in everyday business operations, and their external exposure and weaknesses.

Threat Intelligence Integration:

Incorporating up-to-date threat intelligence into vulnerability assessments to prioritize vulnerabilities that are actively targeted. According to a recent Cyber Risk Alliance's Threat Intelligence Survey[2]: 80% of respondents appreciate having an early warning feed of the newest attacks. 78% of respondents find actionable reporting and relevant context to be integral to a threat intelligence program. 65% of respondents in the study say threat data improves their incident response, 50% say it helps them keep proactive. Threat intelligence is an integral add to current day VM programs, at least according to practitioners.

Dynamic Risk Assessment:

Assessing risk dynamically with consideration of the evolving threat landscape, the proximity of threats considering open vulnerabilities, and changes to an organization's infrastructure.

[2] *https://www.scmagazine.com/research-article/threat-intelligence-the-gold-standard-for-21st-century-cybersecurity*

Adopting A Cost-Optimized, Platform Approach with Integration-Friendly Vendors

Investing in platform-based cybersecurity products that are designed to seamlessly integrate with a wide range of vendor solutions is the way forward when managing shrinking cybersecurity budgets and still, higher expectations. This strategic shift allows organizations to consolidate their security data, streamline their security operations, meet the workforce with an adequate number of tools, and leverage the strengths of all solutions while reducing redundancy and complexity. As it applies to vulnerability management specifically, there are several ways such an approach could help.

Resource Optimization

With a unified platform, security teams can optimize resource allocation. They can allocate personnel, time, and budgets more efficiently to address critical vulnerabilities, reducing the chances of a successful cyberattack.

Continuous Improvement

All-in-one platforms often incorporate machine learning and artificial intelligence to continuously improve their functionality. This means that the platform can become more effective over time, adapting to new threats and vulnerabilities.

Resource Complexity

By consolidating multiple security functions into one platform, organizations can reduce the complexity of their cybersecurity infrastructure. This can lead to cost savings, as fewer tools and resources are required to manage and maintain the environment.

User-friendly Interface

These platforms often come with user-friendly interfaces that make it easier for security professionals to navigate and perform their tasks. This reduces the learning curve and improves the overall efficiency of vulnerability management processes.

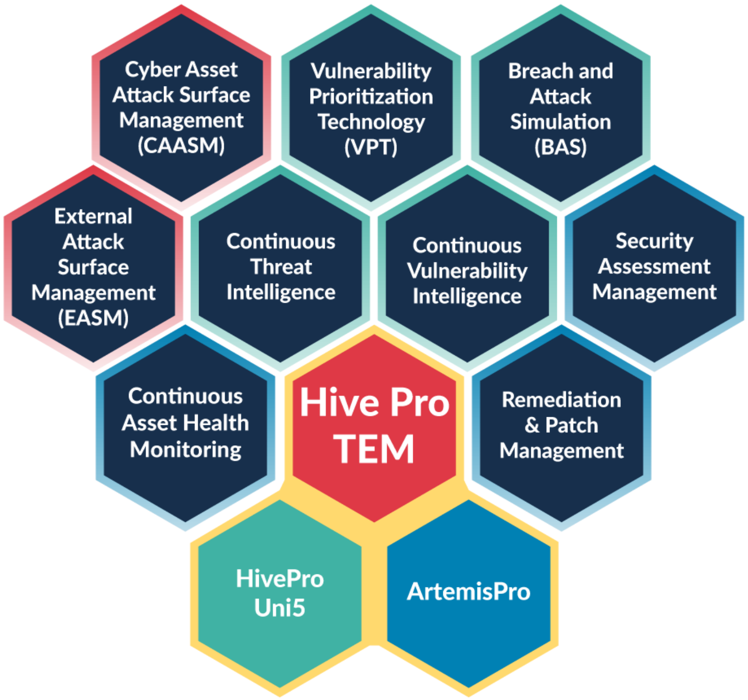
Scalability

All-in-one platforms can often scale with the organization's needs. Whether an organization is small or large, these platforms can adapt to accommodate the growing complexity of the network and the increasing volume of vulnerabilities.

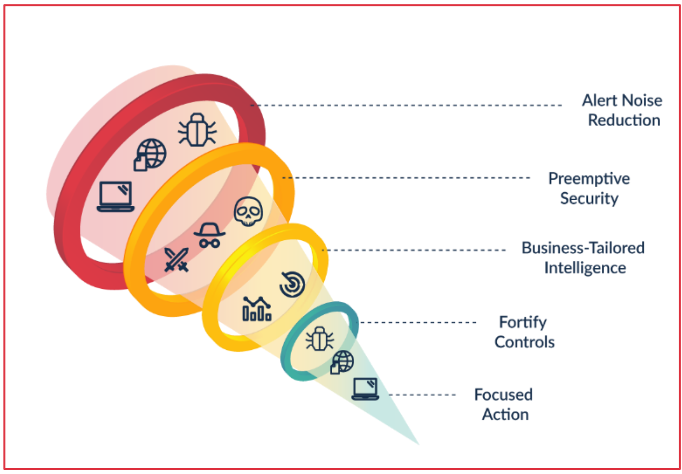
Automating Vulnerability and Threat Management from One Platform

Automation in vulnerability management and threat management empowers enterprises to enhance their security posture, reduce response times to threats, and optimize resource allocation. It helps organizations stay ahead of evolving threats, minimize the risk of human error, and operate more efficiently, ultimately contributing to a stronger and more resilient security environment.

At Hive Pro, we meet all of the benefits above and additionally do all of the following with our Threat Exposure Management Platform. It is a prime example of security optimization, efficiency, and scalability.


Cyber Asset Attack Surface Management (CAASM)
Vulnerability Prioritization Technology (VPT)
Breach and Attack Simulation (BAS)
External Attack Surface Management (EASM)
Continuous Threat Intelligence
Continuous Vulnerability Intelligence
Security Assessment Management
Continuous Asset Health Monitoring
Hive Pro TEM
Remediation & Patch Management
HivePro Uni5
ArtemisPro

The Benefits You Can Expect with Hive Pro



> "By 2026, organizations prioritizing their security investments via a continuous threat exposure management program will suffer two-thirds fewer breaches."
>
> - *Gartner*

Centralized Management

We provide a user-friendly and integration friendly, consolidated platform for vulnerability and threat management. Our TEM platform empowers organizations to view, assess, and manage all organizational vulnerabilities—from code to cloud. This centralization makes it easier to oversee and coordinate vulnerability assessments, remediation efforts, and reporting. Our platform scales with any organization's needs. Whether an organization is small or large, their diverse needs will be met across asset discovery, vulnerability management, and threat management needs. We accommodate the growing complexity of any one organization's infrastructure and their increasing volume of vulnerabilities and security data.

Business-Risk Focused Vulnerability, Asset Health, and Threat Prioritization

We employ advanced algorithms and intelligence to prioritize vulnerabilities based on their potential impact on your organization. Our prioritization factors include but are not limited to asset criticality, environmental factors such as severity and potential impact, likely threats, and highest-risk vulnerabilities. CVSS is but a metric among many, and the metrics of greatest importance apply directly to your organization. This ensures that security teams can focus their efforts on addressing the most critical vulnerabilities first, reducing the overall risk.

Efficient Scanning and Security Assessment Data Integration

We integrate a number of popular and proprietary automated scanning capabilities so that you can consider a wide breadth of vulnerability intelligence and never miss a beat. Our automation capabilities with your tools of choice, and/or ours allows for continuous, scheduled vulnerability scans across the entire IT infrastructure, ensuring that no assets and related vulnerabilities are missed from code to cloud. Whether you are scanning for vulnerabilities as granular as in your code repository to as far reaching as your AWS buckets, we ensure that vulnerabilities are discovered promptly and consistently, reducing the window of exposure to threat actors or otherwise potential for persistent, embedded weaknesses.

Real-time Attack Surface, Threat, and Vulnerability Intelligence and Monitoring

We embed near real-time monitoring of vulnerabilities, threats, attacks, and the affairs of threat actors in our platform. Additionally, we alert you on how all of this intelligence affects your assets and attack surface. This proactive approach enables security analysts to rapidly response to emerging threats and vulnerabilities without struggling from analysis paralysis or analysis fatigue.

Security Control Validation and Fortification

We enable enterprises to simulate the full attack cycle continually and consistently, including insider threats, lateral movement, and data exfiltration, against enterprise infrastructure – using software agents, virtual machines, and other means. Their role is to assess validity and efficacy, such as which types of vulnerabilities are accessible. Their other role is to ensure that security tools are operating as designed. Our BAS tool provides a view of multiple, if not all, stages of the cyber kill chain, as well as of those areas where threat campaigns will likely be successful. Additionally, our BAS surfaces security control misconfigurations, which empowers Security teams with means to fortify their controls and defenses.

Integration Friendly

We integrate seamlessly with other security tools and systems, such as patch management, threat intelligence, and security response tools like endpoint detection and response (EDR), security information and event management (SIEM), security orchestration and response (SOAR), and more. This integration enhances the organization's overall security posture by providing a holistic view of security-related data. We ingest security data like that from automated threat detection systems with their continuous monitoring of network traffic, system logs, and user behavior for signs of suspicious or malicious activity so to immediately alert you of potential threats, enabling faster response times to mitigate risks before they escalate.

Automated Patch Intelligence, Management, and Remediation

We identify and apply security patches to vulnerable systems. Vulnerabilities with known patches will be automatically flagged, and patch deployment can be scheduled during non-business hours to minimize disruptions.

Compliance Management Friendly

We embed features for managing compliance with industry-specific regulations and standards, integrations with ticketing systems to bridge communication gaps during audit season and in general, and internally built collaboration mechanisms. This simplifies the process of demonstrating compliance during audits and assessments.

Reporting and Analytics

We provide robust reporting and analytics capabilities, allowing organizations to generate detailed reports on their vulnerability management efforts. This data-driven approach helps in making informed decisions and communicating the status of security to stakeholders.

The Future of Vulnerability Management

The Evolution of VM

The future of VM lies in its evolution. VM will no longer be solely about identifying and patching vulnerabilities but will transform into a proactive, intelligence-driven process.

Key aspects of the future of VM include:

Risk-Based Vulnerability Management

Organizations will prioritize vulnerabilities based on their unique risk profiles, considering business context, integrating threat intelligence, and the potential impact on critical assets.

Threat Exposure Management

TEM will become a standard practice, allowing organizations to dynamically assess their asset estate and exposure to threats to make necessary shifts in vulnerability management priorities and remediation response. Adaptive risk assessment, meaning assessing risk based on real-time threat data, asset importance, and vulnerability exposure to external threat actors (i.e., monitoring the attack surface) will be core to TEM.

Automation and Orchestration

According to a Ponemon report titled *Costs and Consequences of Gaps in Vulnerability Response*, “too much time is spent navigating manual processes rather than responding to vulnerabilities.” Automation will play a more significant role in VM, streamlining vulnerability assessment, prioritization, and remediation.

Benefits of an Evolved Vulnerability Management

Enhanced Security Functions

An evolved VM approach offers several benefits to security functions across organizations:

Better Risk Mitigation

Prioritizing vulnerabilities based on their specific impact on the organization ensures that resources are focused on the most critical areas with the greatest Security returns.

Reduced Attack Surface

Continuous monitoring and dynamic risk assessments help organizations reduce their attack surface and respond to emerging threats swiftly.

Improved Compliance

Aligning VM with risk management practices ensures better and more defensible compliance with regulatory requirements while not compromising on the core tenants and purpose of security.

Cost Savings

An evolved VM approach can lead to significant cost savings:

Efficient Resource Allocation

Resources are directed towards mitigating vulnerabilities that pose the greatest risk, reducing unnecessary spending on low-impact vulnerabilities.

Reduced Remediation Costs

Prompt identification and remediation of vulnerabilities reduce the costs associated with security incidents.

Reduced Full-Time Employee Costs

Automation and orchestration in VM reduce the reliance on full-time employees for routine tasks, allowing security teams to focus on more strategic activities.

Reduced Technology Costs

An evolved VM approach may help organizations rationalize their technology investments by ensuring that security tools and solutions align with the organization's risk profile and threat exposure.

The Road Ahead for Vulnerability Management

Vulnerability Management is at a crossroads. Current practices, while valuable, fall short of addressing the dynamic and evolving threat landscape. Organizations must embrace a risk-based perspective and adopt Threat Exposure Management to ensure their security postures are resilient and adaptive.

Recommendations for Organizations

To thrive in the ever-changing cybersecurity landscape, organizations should consider the following recommendations:

Embrace a risk-based vulnerability management while integrating Threat Exposure Management as a complementary framework.

Prioritize asset intelligence to better understand business context and stay informed about the latest threat intelligence to assess real-time risks.

Invest in a one-platform approach to automation and orchestration built to integrate threat intelligence, asset criticality, and streamline VM processes.

Continuously update vulnerability assessments based on evolving threats.

By following these recommendations, organizations can position themselves to effectively **manage vulnerabilities, reduce risks, and enhance their overall security posture** in an increasingly challenging cybersecurity landscape.

About Hive Pro

The Hive Pro Threat Exposure Management (TEM) Platform is a comprehensive, all-in-one platform designed to track threats, streamline vulnerability management, enhance collaboration, and improve security posture. From security assessment workflow orchestration to actionable AI-driven threat prediction and vulnerability remediation, TEM empowers organizations to build their organizational resilience by identifying, prioritizing, and resolving security threats and vulnerabilities. We automate and orchestrate the security remediation process dynamically and at scale, so you have one less thing to worry about.

Hive Pro's corporate headquarters are located in Herndon, Virginia, with presence across the US, EMEA, and APAC. To learn more, visit www.hivepro.com.

All trademarks contained herein are the property of their respective owners.

To learn more, visit www.hivepro.com

Hive Pro®

Get in Touch

Hive Pro Inc. | info@hivepro.com | www.hivepro.com

Start your Free Trial

Read our Blog