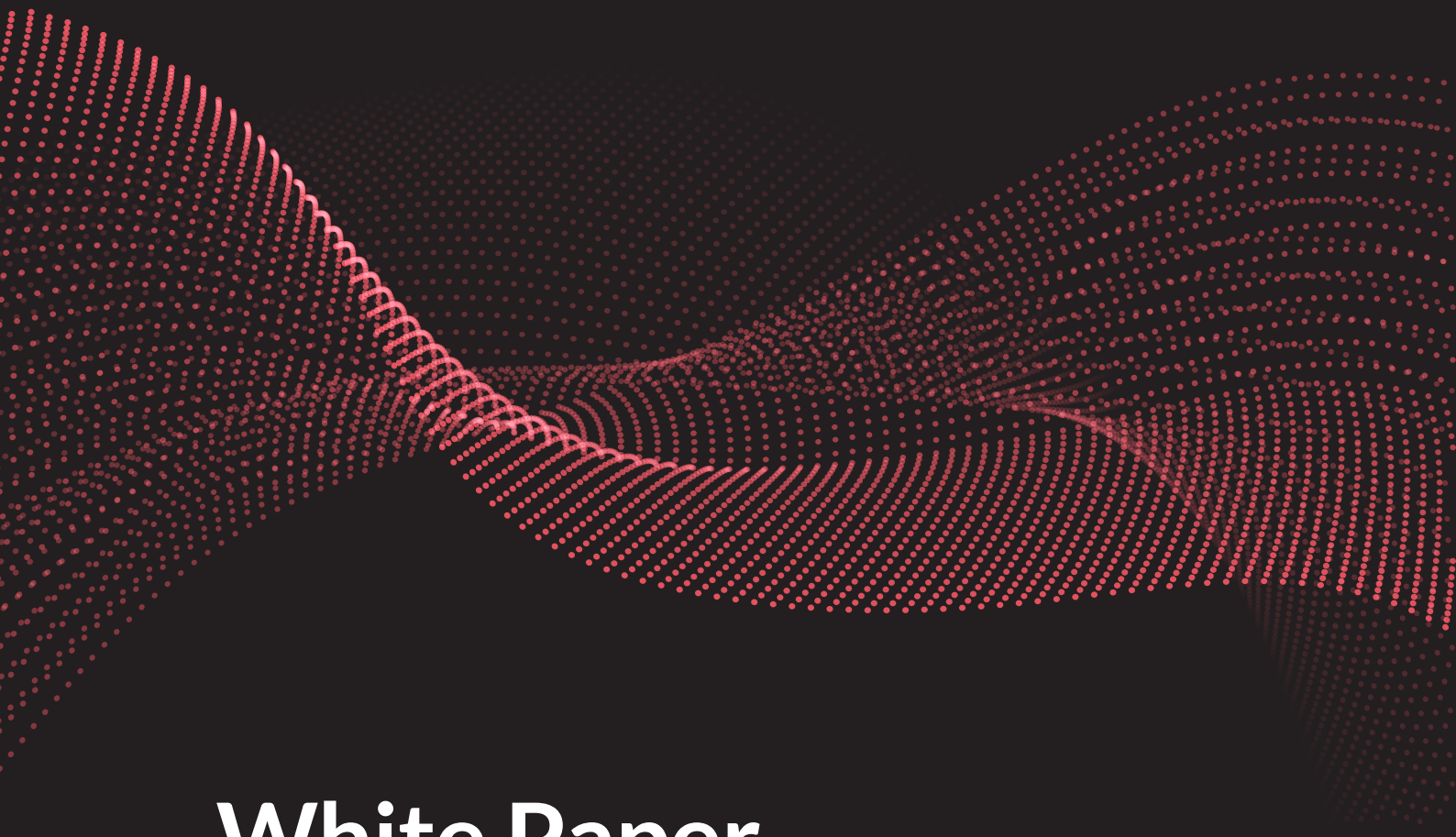
Hive Pro®



White Paper

Seeing the Full Threat Exposure Picture with Uni5 Xposure

Table of Content

Introduction

In the world of cybersecurity, understanding the attacker's viewpoint is essential for developing proactive defense mechanisms. With the exponential growth of cyber threats targeting organizations at an unprecedented rate, many enterprises grapple with numerous challenges that prevent them from taking as proactive an approach as adopting the "attacker's perspective". Most enterprises are stuck in continuous reactive cycles with hopes of avoiding severe breaches while facing other significant cybersecurity challenges such as asset and risk blind spots, insufficient vulnerability prioritization, and misconfigured or weak compensating controls. It's now imperative for organizations to adopt strategies and tools that offer comprehensive threat visibility and proactive threat management, ensuring they have the ability to outmaneuver their potential adversaries and ensure cyber resiliency.

In fact, Gartner predicts that by 2026, those organizations prioritizing their security investments based on a "continuous threat exposure management program will realize a two-thirds reduction in breaches". Much of their initial success will hinge on reforming their vulnerability management programs to accommodate the "attacker's point of view".

The Attacker's Viewpoint: Why It Matters

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."

– "The Art of War", Sun Tzu

Sun Tzu's words still ring true 2,500 years after his publication. In his seminal work, "The Art of War", Sun Tzu examined asymmetric warfare and therein, the importance of preemptive, informed defense. Today, all state and non-state actors rely on adversarial intelligence to plan offensive operations and to fortify their defensive posture. If military strategy finds the adversary's perspective a necessary element of intelligence, then surely cybersecurity strategies must also account for the same. By adopting this approach, cybersecurity functions can proactively identify threats and prevent the likelihood of exploitation. The proposed approach alone is ideal; however, in practice it's incredibly trying for the modern cybersecurity function.

Problems That Plague Modern-Day Cyber Defenders

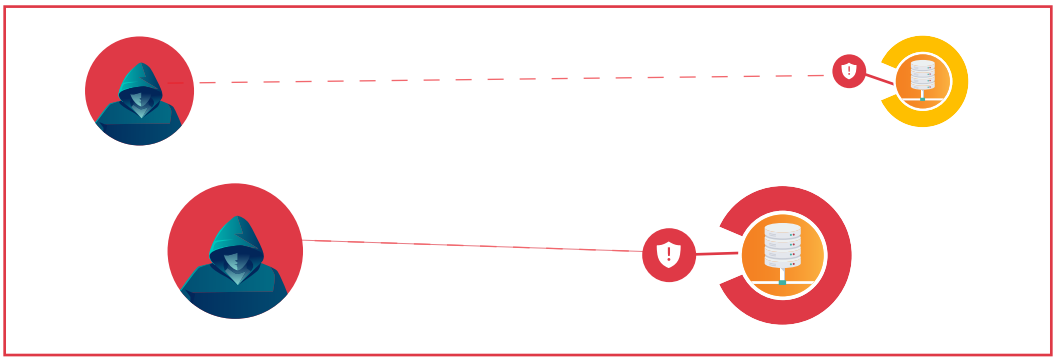
The volume, velocity and variety of cyber threats aimed at enterprises daily paired with an ever-expanding enterprise attack surface result in several issues that inhibit proactive cyber defense and the liberty to adopt the attacker's viewpoint. The major problems are as follows:

Blind Spots

Mid-market enterprises have between 500 to 5,000 endpoints on average, and large corporations have over 100,000 endpoints. Moreover, most modern enterprises have remote workers, engage with contractors, and with expansive networks of suppliers and partners. All these factors contribute to an organization's expanding attack surface, which is increasingly difficult to manage and now more susceptible to Security oversight.

Insufficient Risk Assessment & Weak Controls

To conduct a thorough cyber risk assessment, the impact of all assets, potential threats, and vulnerabilities must be considered. Many organizations struggle with this due to incomplete asset discovery, poor vulnerability prioritization, and insufficient threat intelligence, resulting in miscalculated risks. Additionally, Security teams seldom test the efficacy of implemented security controls, leaving them susceptible to threats.



Deficient Prioritization

Even though less than 30% of all vulnerabilities are exploitable, Security teams still face issues in weeding them out from the constant vulnerability noise and prioritizing them by true business-risk for remediation. In an effort to prioritize vulnerabilities, they conduct manual spreadsheet analysis with limited knowledge or rely on generic prioritization calculators. The result is usually contextless prioritization and the misallocation of resources while threats loom elsewhere.

Too Many Tools & Not Enough Analysis

Mid-market enterprises typically use around 10 cybersecurity tools, while larger ones utilize over 76, yet they employ only an average of 4 and 6 cybersecurity staff respectively. This tool proliferation leads to overwhelming data, causing alert fatigue and the risk of missing crucial warnings. Such an environment has led to increased stress, with 77% of cybersecurity professionals feeling it impacts their ability to protect data, and a third considering leaving their jobs within two years due to burnout.

Where to From Here? Proactivity vs. Reactivity

> "You can ensure the safety of your defense if you only hold positions that cannot be attacked. Supreme excellence consists in breaking the enemy resistance without fighting..."
>
> – Sun Tzu

The future of cybersecurity is in proactive defense, wherein the "attacker's viewpoint" is integral to provide strategic leverage over threat actors, break their resistance, and ultimately eliminate threats. It no longer serves any cybersecurity function to be reactive, putting out a fire at every corner. So how do we get there, considering the many hurdles in the way?

Step 1: Eliminate Blind Spots With Thoroughly Scoped, Discovery Processes

To eliminate blind spots, cybersecurity functions must ensure that they run vulnerability scans against a comprehensive asset inventory. Compensatory controls are included in this asset inventory and should also be documented. Combined data from attack surface management tools, configuration management database (CMDB) tools and asset management tools have the power to provide a holistic outlook; although 45% of IT professionals believe that the absence of a unified view across cybersecurity and IT functions majorly delays the vulnerability patching process, so a centralized and normalized view of all outputs would be beneficial. Asset fingerprinting and classification capabilities are also paramount to add the necessary risk context. It is only rational to get a holistic perspective on the state of your assets and vulnerabilities before pursuing a holistic risk analysis.

Step 2:
The Risk-Management Calculator & The "Attacker's Perspective"

$$\text{Risk} = \frac{(\text{Threat} \times \text{Vulnerability} \times \text{Probability of Occurrence} \times \text{Impact})}{\text{Compensatory Controls}}$$

(NIST 800-30 2002)

47% of DevSecOps professionals attribute their backlog to prioritization issues—it's time to reduce the vulnerability backlog that need not exist due to insufficient prioritization. For organizations to really understand the 'threat' factor, the 'probability of occurrence', and 'impact', they require sufficient threat intelligence and a means to test it. For threat intelligence, combining several threat intelligence feeds with attack and threat actor context will help to put high-risk vulnerabilities into perspective. To test impact, we suggest you use a breach and attack simulation tool. These tools run real-world TTP simulations in a controlled environment, which is as close to the "attacker's perspective" that an organization can get while eliminating the overhead and time required in PTaaS exercises and Red Teaming. With these combined efforts, prioritizing vulnerabilities should be an easier feat.

Step 3:
Align Your Tools To Your Needs. Never Set and Forget.

Over 73% of organizations have at least one security control misconfiguration. Proper controls hygiene is easily one of the trying practices in maintaining cybersecurity resilience. Your vulnerability scanners, configuration auditing tools, breach attack simulation tools, PTaaS service, and a host of other tools can surface misconfiguration alerts. The most important part is to follow up on them and to configure your tools not only according to best practice, but also to what meets your risk baseline. Never set and forget. Additionally, every tool in your security architecture must fit a purpose for the organization and not the other way around. Force-fitting tooling is never a benefit for cybersecurity functions looking to manage real-world threats.

Step 4:
Good Tools Are Only As Good As Their Analysis. Invest in Analysis.

60% of successful data breaches occur due to unapplied patches, even when they're available. Your tools should carry you forward all the way from intelligence and discovery to testing and remediation. Invest in tools that don't just spout data, but produce proper, actionable analysis. Risk scores must not just be empty numbers, they must be supported by an evidence-based approach that is explainable, trustworthy and can be defensible no matter the outcome. Invest in analysis. If cybersecurity practitioners follow this guidance, they'll be sure to outmaneuver cyber threat actors, and eliminate pressing risks.

The Hive Pro Uni5 Xposure Approach

The proactive cybersecurity approach is what we at Hive Pro have always championed with our platform HivePro Uni5 and now, with our newest offering, Uni5 Xposure platform, we take this vision one step further. We walk you through both platforms below, detailing with great transparency the core features and benefits you can expect.

The HivePro Uni5 Flagship

The core principle of HivePro Uni5 is to eliminate genuine business threats before they turn into full-blown attacks. By leveraging cutting-edge threat intelligence, precise vulnerability insights, assets' context, and countless environmental factors, HivePro Uni5 predicts imminent attacks, prioritizes vulnerabilities, tests security measures, and offers an integrated solution for end-to-end vulnerability management and remediation.

Core features of HivePro Uni5 include:

Comprehensive Asset Discovery: identifies, fingerprints and classifies all managed and unmanaged assets continuously across the IT, cloud, mobile, and remote environments.

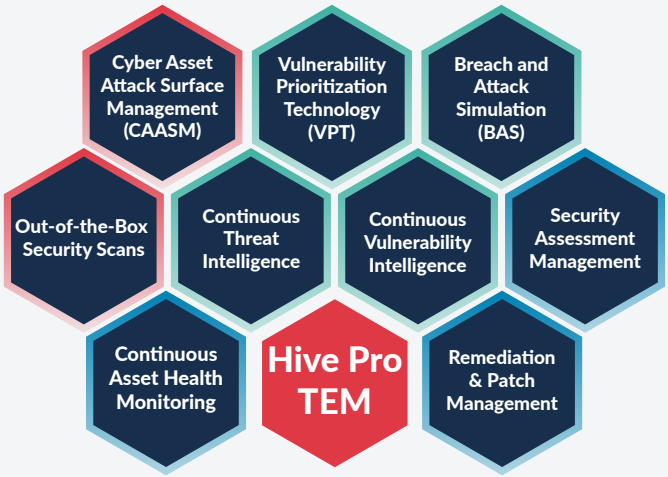
Vulnerability, Threat, IoC, Patch Intelligence: tailors thousands of threat and vulnerability intelligence data points including TTPs and indicators of compromise (3,368), threat actors (269), CVEs (223,152) and CVE intelligence (106,129) with over 42,680 patch intelligence data points to your business-critical assets.

AI-Powered Vulnerability Prioritization: factors in parameters such as exploitability, attack path, patch availability, geography, vertical, ease of exploitation, vulnerability age, asset criticality, actors, compensatory controls, and more.

Breach and Attack Simulation: simulates real-world TTPs against your organization in a controlled (sandbox) environment to evaluate your security posture, surface potential control misconfigurations, and blind spots.

Vulnerability Remediation: bi-directional integrations with ITSM and patch management tools helps to collaborate and streamline necessary remediation actions and automate patches in-platform.

Customizable Reporting : Generate technical or non-technical reports to showcase progress and necessary calls to action.



Enter Uni5 Xposure

Taking forward the legacy of HivePro Uni5, Uni5 Xposure inherits everything above and adds to the sum a plethora of new core capabilities, enhancing the entire threat exposure management narrative:

Comprehensive Asset Discovery

Continuous, unified asset visibility across the IT, cloud, mobile, and remote asset estates to remove asset blind spots.

Total Infrastructure Scanning

Out-of-the-box, detailed scanning for vulnerabilities, security findings and misconfigurations across code, container, web, application, cloud, network, and mobile environments to remove security risk blind posts across all assets.

Unified Security Assessments

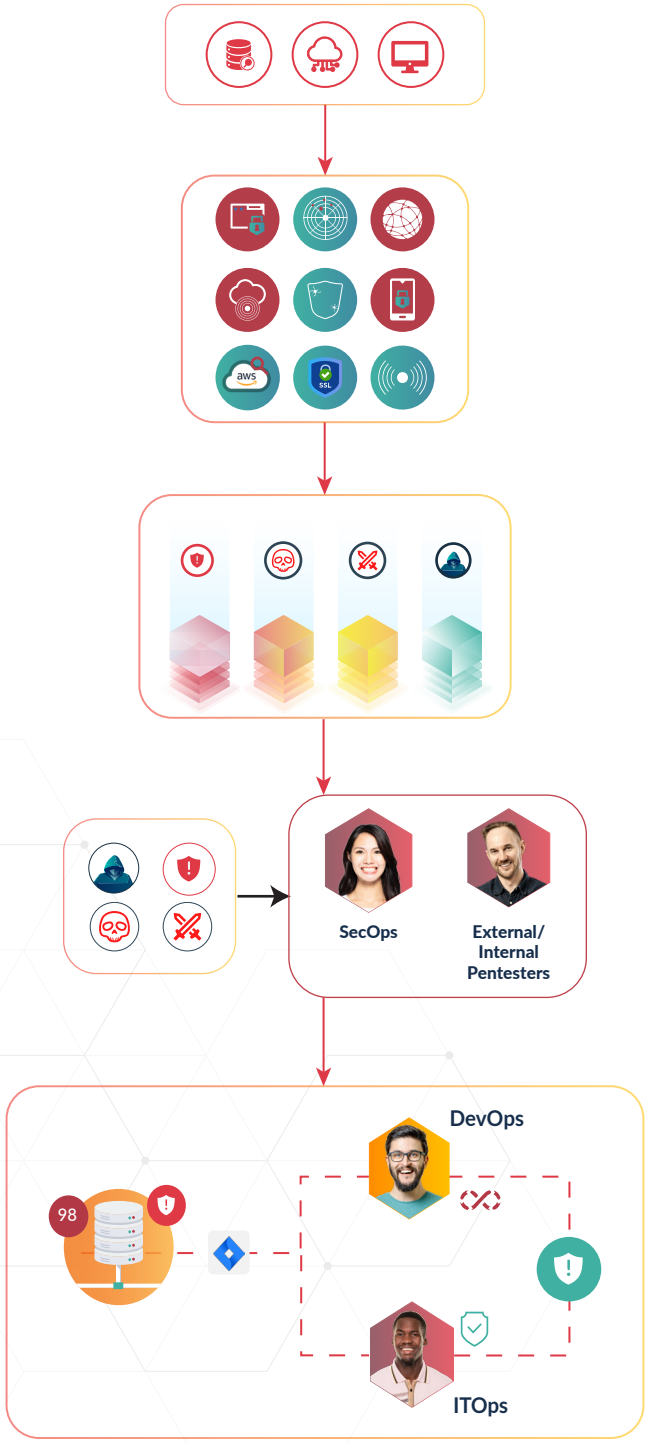
Consolidate diverse assessments into a single platform to reduce data sprawl issues. Initiate and manage new security assessments from the same plane to streamline workflows from one place.

End-to-End Workflow Management

Comprehensive management, audit, and report capabilities aligned with security tests, assessments, and PTaaS workflows to speed up remediation processes and to enrich compliance and audit needs.

Built-In Cross-Functional Collaboration

Collaborate on every workflow including asset risk decisions, remediation actions, compliance needs, and assessment feedback across functions to strengthen communication and build for efficiency.



The Net Effect

Uni5 Xposure solves for the issues posed by siloed tools, asset and vulnerability blind spots, manual spreadsheet processes, stagnated vulnerability remediation, and miscalculated security risks. 60% of data breaches are caused by inadequate and untimely patch intelligence–eliminate this risk with Uni5 Xposure's automated patch intelligence (42,600+ data points), IoC intelligence, and actionable remediation recommendations. As an added and integral benefit, HiveForce Labs, our in-house threat, vulnerability, and patch intelligence research teams, continuously update both platforms to drive the most effective threat exposure prevention strategy.

The volume, velocity and variety of cyber threats aimed at enterprises daily paired with an ever-expanding enterprise attack surface can be proactively managed, and at Hive Pro we know because Uni5 Xposure does just that. Uni5 Xposure offers clear visibility into your organization's threat exposure, empowers you with the "attacker's perspective" and provides the tools needed to manage your threats effectively to enhance cyber resilience.

We encourage you to trial Hive Pro Uni5 for free, any time. And we welcome you to demo the new Uni5 Xposure platform today to see the whole story in action.

About Hive Pro

Hive Pro is recognized as a trusted vendor by leading analyst firms Gartner, Inc. and Forrester, affirming their industry expertise and reliability. Their flagship product HivePro Uni5 is now complemented by the Uni5 Xposure platform. Uni5 Xposure enables total asset exposure visibility and management by combining the strength of the HivePro Uni5 platform (asset discovery, AI-driven VPT, BAS, threat intelligence, patch intelligence and multiple integrations) with additional core capabilities like out-of-the-box total infrastructure scanning (code, web, mobile app, network, cloud, container), security assessment orchestration and workflow management, and actionable recommendations for remediation. Uni5 Xposure presents a unified and actionable view of threat exposure and risk across various evaluations to enable continuous cybersecurity assurance and resilience.

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

Hive Pro®

Get in Touch

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

Book a Demo

Read our Blog