Threat Exposure Management (TEM) is a continuous, risk-based program that aims to manage your security vulnerabilities and minimize your threat exposure. For TEM to be effective, it requires wide visibility, strong security controls and timely, actionable fit-for-business intelligence. Unfortunately for many organizations, TEM is disrupted by various factors impacting threat, vulnerability and probably scores.

Problem: Force-Fitting Poor Intel

$$\text{THREAT} \times \text{VULNERABILITY} \times \text{PROBABILITY} \times \text{IMPACT} = \text{RISK}$$

Unpersonalized
Point Solutions

Generic
Compliance/Asset
Oriented
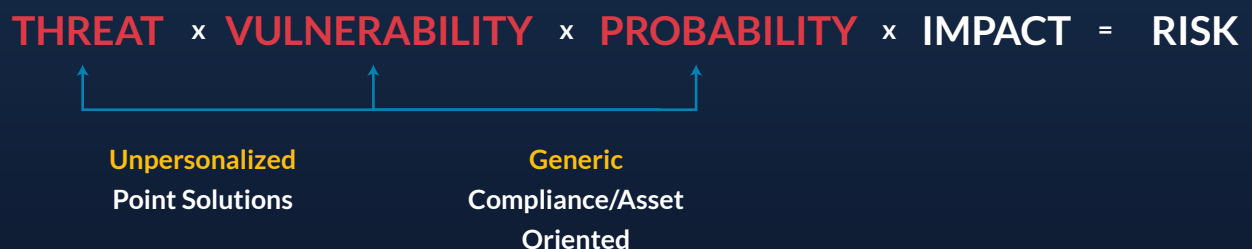
Compounding on these Outstanding Problems

Poor exposure visibility, mounting vulnerabilities and threat alerts, and long list of unactioned, generic remediations.

In the wake of compounding annual cyber attacks, Hive Pro believes that it is integral for all organizations to have an effective TEM program.

This is why we created the Hive Pro Threat Exposure Management platform, wherein our product HivePro Uni5 takes on the challenge of providing your organization actionable, tailor-fit threat and vulnerability intelligence and remediating your top vulnerabilities and security misconfigurations. From HivePro Uni5, your organization will remediate vulnerabilities that matter most, keep track of proximal threats, test outstanding security controls, and reduce overall security risks. Our All-in-One Platform is true to its name and frees you from the burdens of multiple consoles and substantial overhead costs associated with deployment, analysis, and operations.
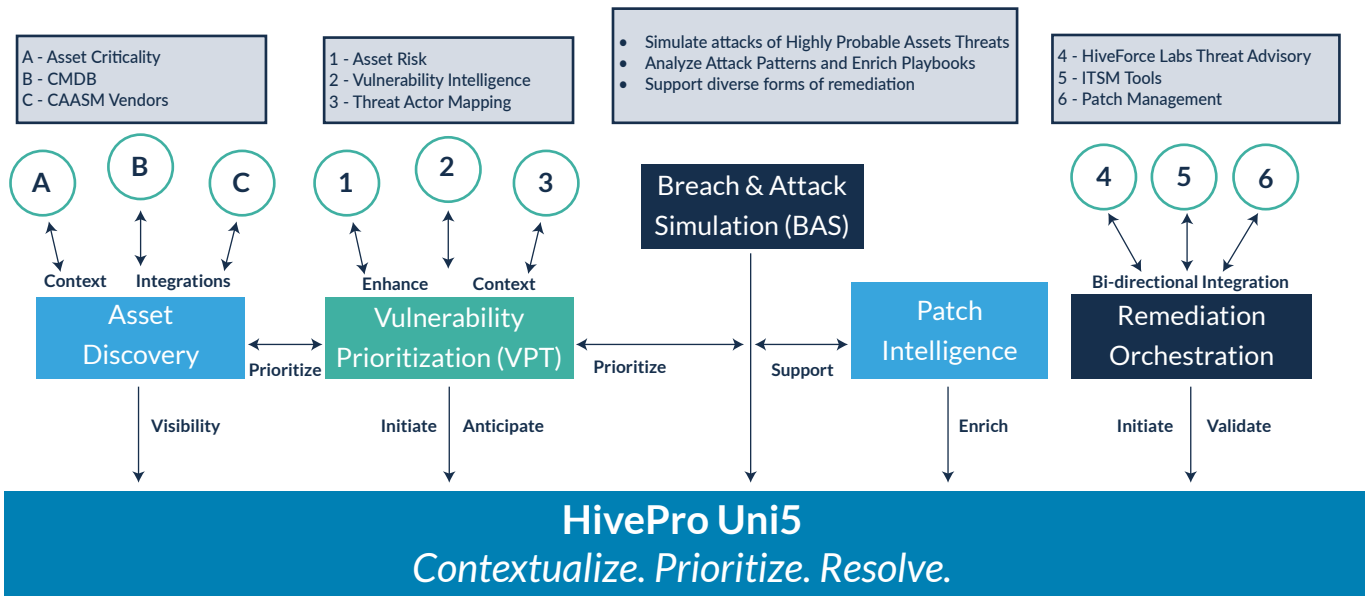
HivePro Uni5

HivePro Uni5 works in three parts:

Contextualizes threats and vulnerabilities according to your business-critical of assets.
*Prioritizes* vulnerabilities according to your business context, asset exposure, and likely threats.
Resolves vulnerabilities exposure points, and security misconfigurations according to priority.

HivePro Uni5: Vulnerability & Threat Exposure Remediation

A - Asset Criticality
B - CMDB
C - CAASM Vendors

1 - Asset Risk
2 - Vulnerability Intelligence
3 - Threat Actor Mapping

- Simulate attacks of Highly Probable Assets Threats
- Analyze Attack Patterns and Enrich Playbooks
- Support diverse forms of remediation

4 - HiveForce Labs Threat Advisory
5 - ITSM Tools
6 - Patch Management

A   B   C   1   2   3   Breach & Attack Simulation (BAS)   4   5   6

Context   Integrations   Enhance   Context   Bi-directional Integration

Asset Discovery — Prioritize — **Vulnerability Prioritization (VPT)** — Prioritize — Support — **Patch Intelligence** — **Remediation Orchestration**

Visibility   Initiate   Anticipate   Enrich   Initiate   Validate

HivePro Uni5
### *Contextualize. Prioritize. Resolve.*

Contextualize

HivePro Uni5 ingests cloud and on-prem asset information from a number of tools (e.g. CMDB, ASM, csv upload) and sorts them into categories based on business asset owner and criticality. Your asset owners have relevant access and visibility from the very beginning to define critical assets and make agile risk decisions. HivePro Uni5's wide-reaching asset discovery integrations enrich our native-vulnerability prioritization technology with visibility into all of your internal and external risks.
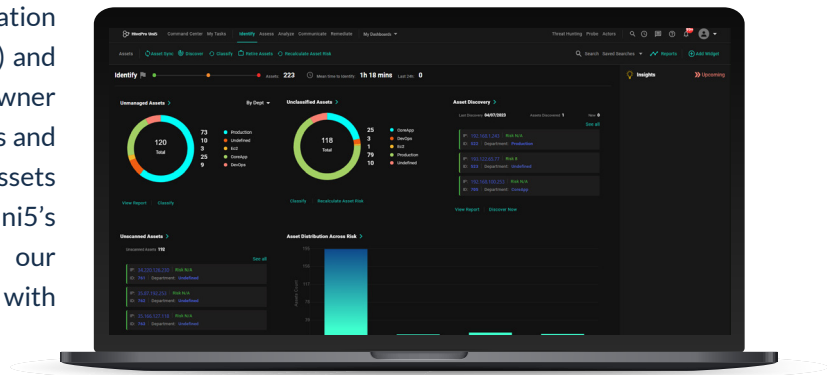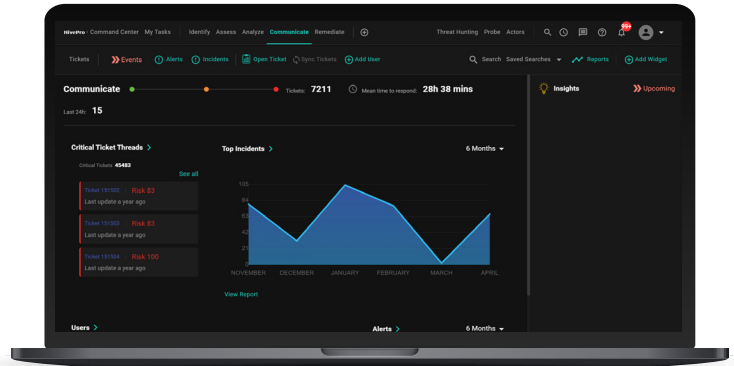

Prioritize

We combine your internal IT and business intelligence with our in-house and external environmental, threat and vulnerability intelligence, filter through the noise and false-positives, and prioritize your critical vulnerabilities. Additionally, our ML predictive modeling algorithms continuously add velocity and intelligence enrichments to your output. This big data effort ingests thousands of your vulnerabilities and open-source and proprietary closed-source threat intelligence resources to predict which vulnerabilities will most likely be weaponized against your organization.
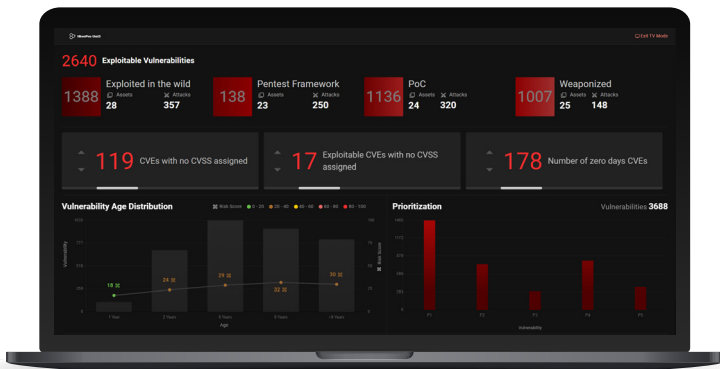
As you manage your vulnerabilities, HivePro Uni5 empowers your Security team to test the strength of your security controls with our native and fully-integrated Breach and Attack Simulation to conduct simulated, real-world attacks against your organization's security infrastructure and find weak points. HivePro Uni5 automatically suggests security tool configurations, patch intelligence, and potential compensatory controls.

Resolve

HivePro Uni5 enables remediation orchestration through immediate patch intelligence, recommended configuration changes and rich bi-directional integrations with Asset Management, CMDB, and ITSM platforms. To help you monitor your progress, the HivePro Uni5 platform keeps track of all workflows, actioned remediations, and the status of your security posture. HivePro Uni5 also provides you with options beyond automated patching, including exceptions granting and manual patching. Our goal is to communicate a consistent, actionable and understandable security posture and remediation improvement plan(s) to you and all of our users. HivePro Uni5 also helps you tell your Security story to any relevant stakeholder on a click of a button. Generate actionable strategic, tactical and operational reports for all cross-functional stakeholders.

Key Benefits

Tailor-Made For
Your Organizations

HivePro Uni5 tailors thousands of threat and vulnerability intelligence resources to your business-critical assets, filters through the noise and prioritizes the vulnerabilities that matter the most. Our all-in-one platform aligns all risk decisions to the proper business-unit and owners in-platform so you can collaborate and reach resolution faster.

Manage and Audit Your
Workflows

Security Operations teams can track workflows to remedy gaps in out-of-sync periods, and ensure that newly initiated workflows are occurring at optimal frequencies, in line with several factors: remediation cycles, organizational risk tolerance, audit and compliance mandates, and other business-critical events.

Fully Customizable
Dashboards

In one easy-to-read interface, HivePro Uni5 maps all of your critical assets, associated vulnerabilities, and the threats most likely to exploit them. Every in-platform user can customize HivePro Uni5's rich intelligence dashboard to their needs.

Strong Cross-Function
Collaboration

Hive Pro TEM enables collaboration in-console through strong bi-directional ITSM and Collaboration platforms, enabling your Security, ITOps, and GRC teams to stay on top of risk-based threat and vulnerability management.

Strengthen Your Security Controls

HivePro Uni5's Breach and Attack Simulation Module tests your security controls with real-world simulationed attacks from your most likely threats. Our BAS Module surfaces your control misconfigurations, weak or blind spots, and suggests room for improvement.

Boost Your ROI with Effective Threat Exposure Management

30%

Faster Detection & Remediation

33%

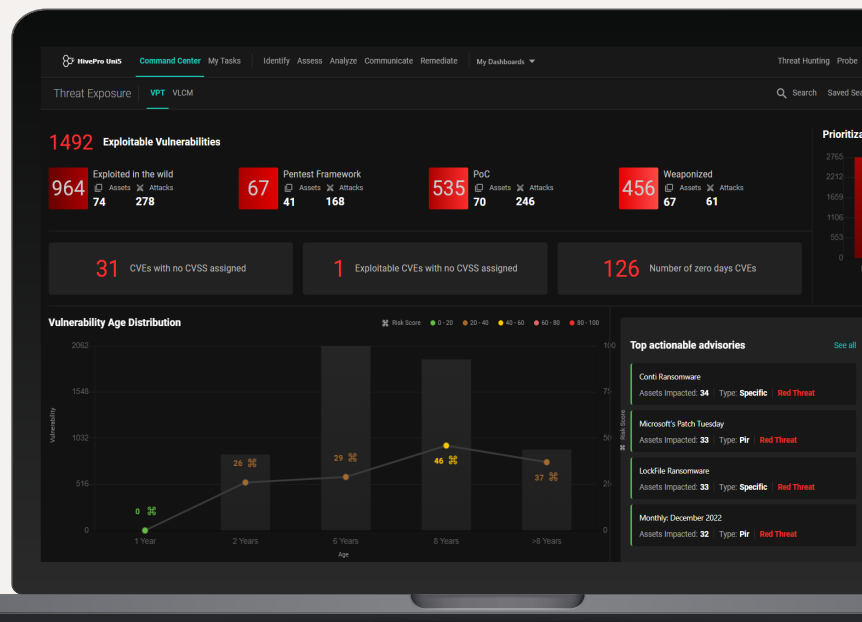Reduced Critical Asset Risk

70%

Increase in Operational Efficiency

HivePro Uni5 now supports
27+ out of the box integrations

tenable.io
vulnerability management

insightVM

servicenow

nessus

Qualys

CROWDSTRIKE

Experience the Power of HivePro Uni5

Deploy in less than an hour to permanently manage your threats and vulnerabilities.

Request a demo today!

Contact Us   **Schedule a Demo**   **Read Our Blog**