Data Sheet

# Hive Pro Uni5 Xposure MSSP Tiered Service Model

## Hive Pro Technical Overview

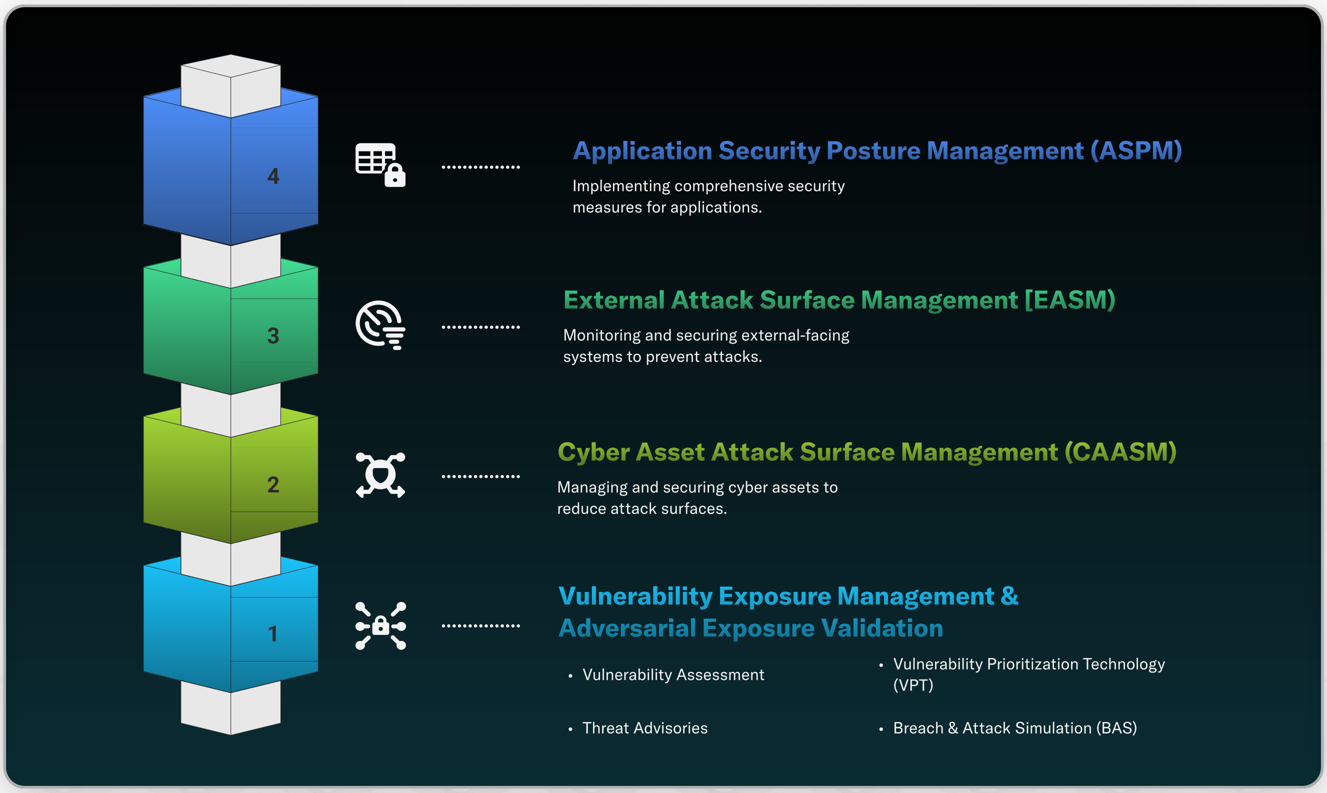
HivePro Uni5 Xposure is a unified, attack and intelligence powered Threat Exposure Management (TEM) platform. The Uni5 Xposure multi-tenant platform empowers MSSPs to deliver proactive and preemptive cybersecurity services with:

- **End to End Visibility:** Single Pane of Glass across Network Vulnerabilities & Misconfigurations(VA), Cloud Misconfigurations (CSPM), Container Vulnerabilities, Application Vulnerabilities (DAST), Source Code vulnerabilities (SAST) along with Cyber Asset Attack Surface Management (CAASM)
- **Code to Cloud Correlation:** The platform aggregates, de-duplicates, normalize and correlate data across first and third party sources across the layers
- **Unified Workflow:** Orchestrate scans across Vulnerability scanners across Tenable, Qualys, BurpSuite, Checkmarx, Veracode,etc, then use external factors such as threat intelligence and internal factors such as asset criticality, network position of the assets, existing security controls and threat simulation to assess the precise attackable exposures. These attackable exposures can then be mobilized for remediation using the platform.
- **Detection Augmentation and Zero Day Remedy:** Using built-in adversarial exposure validation (AEV), the IOCs and TTPs for a successful attack/ threat simulation/ Zero day exploits, is provided that can be leveraged by the SIEM/EDR/ XDR to block the attacks proactively. This eliminates the gap that exists between traditional Exposure Management platforms and Threat Detection and Incident Response (EDR/XDR/SIEM) platforms.
- **Less Engineering and more Risk Management:** With 100+ native integrations across ITSM, EDR, CMDB, vulnerability scanners, and cloud environments, the MSSPs will minimize the engineering work and scale service to deliver more security value to their diverse set of customers.

## MSSP Tiered Service Model Overview

The diagram on the next page illustrates HivePro's four-tiered service delivery framework tailored for MSSPs. Each ascending layer builds on the previous one, allowing service providers to progressively scale their offerings—from foundational internal threat exposure and vulnerability prioritization to complete application security posture management (ASPM).

This modular approach enhances exposure coverage across hybrid enterprise environments by aligning with customer maturity levels and budget flexibility, enabling MSSPs to upsell advanced services as clients evolve.



### Application Security Posture Management (ASPM)

Implementing comprehensive security measures for applications.

### External Attack Surface Management [EASM)

Monitoring and securing external-facing systems to prevent attacks.

### Cyber Asset Attack Surface Management (CAASM)

Managing and securing cyber assets to reduce attack surfaces.

### Vulnerability Exposure Management & Adversarial Exposure Validation

- Vulnerability Assessment
- Vulnerability Prioritization Technology (VPT)
- Threat Advisories
- Breach & Attack Simulation (BAS)

## Service Tier Feature Comparison Table

| Feature Level | Tier 1 | Tier 2 | Tier 3 | Tier 4 |
|---|---|---|---|---|
| Infrastructure Vulnerability Scanning | ✓ | ✓ | ✓ | ✓ |
| Vulnerability & Threat Prioritization | ✓ | ✓ | ✓ | ✓ |
| Threat Advisory Platform | ✓ | ✓ | ✓ | ✓ |
| Breach & Attack Simulation (BAS) | ✓ | ✓ | ✓ | ✓ |
| Cyber Asset Attack Surface (CAASM) | - | ✓ | ✓ | ✓ |
| External Attack Surface Discovery | - | - | ✓ | ✓ |
| Application Security Posture Management | - | - | - | ✓ |
| Pen Test Management | - | - | - | ✓ |

## Tier 1 – Infrastructure Security & Threat Exposure Foundation

Designed for foundational risk visibility, Tier 1 equips MSSPs to deliver vulnerability management for internal assets, enriched with real-time prioritization and advisory intelligence.

### Technical Components :

- **Internal Infrastructure Vulnerability Scanning:** Uses unauthenticated and authenticated scans to detect software flaws, misconfigurations, and CVEs across OS, network, and application layers. Supports dynamic and policy-based scanning templates.
- **Vulnerability Prioritization Technology (VPT):** Enriches vulnerability data with exploitability metrics (Exploited in the wild, Weaponised, PenTest Framework, EPSS, CISA KEV), asset criticality, and compensating controls. Leverages predictive analytics to score risk based on real-world threat activity.
- **Threat Exposure Management (TEM):** Correlates threat intelligence with known CVEs to identify exposures with adversarial relevance. Auto-tags vulnerabilities are part of active campaigns and nation-state toolkits.
- **Breach and Attack Simulation (BAS):** Simulates adversary TTPs (MITRE ATT&CK-aligned) within controlled environments. Measures EDR/NDR/WAF response efficacy and exposes security control gaps.
- **Whitelabeled Threat Advisories:** Delivers threat briefs tailored to industry (e.g., Telecom, BFSI), region, and geopolitical risks. Provides MSSPs with customizable PDFs and dashboards to brand and disseminate.

**MSSP Value:**

- Faster go to market with low integration overhead.
- Delivers high-volume, automated vulnerability lifecycle management.
- Differentiates MSSPs with contextual threat-aware remediation guidance.
- Provides structured entry-point for long-term managed security expansion.

## Tier 2 – Cyber Asset Attack Surface Management (CAASM)

CAASM delivers unified, cross-domain visibility by ingesting, deduplicating, and correlating asset data from multiple sources. It enhances vulnerability insights with user, device, and software context.

### Technical Components:

- **Multi-Source Asset Inventory:** Aggregates asset data from EDRs, vulnerability scanners, ITSM, AD, cloud APIs, and NAC systems. Normalizes metadata across sources into a federated asset model.
- **Software, User & Device Mapping:** Connects software packages to host assets, logged-in users, business owners, and exposure records. Aids in application accountability and risk ownership.
- **Risk Attribution Engine:** Assigns business risk scores to each asset based on asset type, exposure level, historical vulnerabilities, and exploitability.
- **Control Coverage Validation:** Detects assets lacking endpoint and network security controls, or using outdated protection agents. Provides asset-centric remediation blueprints.

**MSSP Value:**

- Delivers services aligned with CAASM mandates and compliance.
- High-margin advisory engagements for asset governance and segmentation planning.

## Tier 3 – External Attack Surface Management (EASM)

Tier 2 expands visibility to the organization's external-facing assets and digital perimeter. It mimics adversary reconnaissance to help MSSPs detect what attackers see from outside the firewall.

### Technical Components:

- **Internet-Facing Asset Discovery:** Continuously maps domains, subdomains, IPs, ports, certificates, and DNS records. Leverages passive DNS, reverse IP lookups, and HTTP fingerprinting.
- **Shadow IT Detection:** Identifies unregistered cloud services, forgotten dev/test environments, or SaaS apps exposing risk. Uses SSL fingerprints, WHOIS, ASN mapping.
- **Threat-Informed Prioritization:** Flags externally exposed vulnerabilities being exploited in the wild, tied to ransomware kits, APT groups, or exploit marketplaces.
- **Exposure Intelligence Dashboards:** Visualizes external risk trends, attackability scoring, and asset ownership hierarchies. Provides drill-down views of misconfigured public services and aging exposures.

**MSSP Value:**

- Enables premium 'Outside-In Risk Assessment' offerings.
- Helps clients reduce external footprint and shadow infrastructure.
- Provides clear ROI through visualized risk reduction.
- Upsell path to full attack surface lifecycle coverage (CAASM in Tier 3).

## Tier 4 – Application Security Posture Management (ASPM)

Tier 4 allows MSSPs to cover code-to-cloud risks across software pipelines. It unifies static, dynamic, container, and cloud misconfiguration insights under a risk-based application security framework.

### Technical Components:

- **SAST & DAST Integration:** Pulls findings from tools like SonarQube, Checkmarx, OWASP ZAP, and Burp Suite. Normalizes CVSS, CWE, and CVE tagging into the TEM framework.
- **CI/CD Security Validation:** Integrates with GitHub, GitLab, Jenkins, etc. to detect hardcoded secrets, open dependencies, and unvalidated inputs pre-deployment.
- **Container Image Scanning:** Analyzes Docker and Kubernetes artifacts for CVEs, root escalation paths, and misconfigured volumes or registries.
- **Cloud Posture Monitoring:** Inspects AWS, Azure, GCP configs for over-permissive IAM, public buckets, unencrypted storage, and idle services.
- **PenTest Management:** Onboard pen-testers and manage all pen test findings from one single dashboard. Generate PT reports with one-single click and manage all pentest activities.

**MSSP Value:**

- Offers comprehensive ASPM as-a-service for SaaS and DevOps clients.
- Ideal for MSSPs targeting regulatory-heavy or AppSec-mature markets.
- Positions MSSPs as full-stack security partners from infra to code.