Hive Pro

USE CASE

Fortifying Financial Services Cybersecurity with Hive Pro

INTRODUCTION

Financial services are under immense pressure to keep up with their competitors while faced with growing challenges like digital evolution, regulatory compliance and cybersecurity. To the latter point, the more financial services digitally advance, the greater responsibility they have to maintain the security of their assets. Cyber-attacks are growing in speed, sophistication, and scale. Financial services are being called to manage their risks, reduce their vulnerabilities and ward off potential threats lest they become a victim of a dangerous trend. While the competitive logic may seem different, the need for advanced technology that allows financial services to stay ahead of their competition is just as crucial as staying ahead of their potential cyber threats. Now more than ever, it is imperative that financial services build strong security defenses and a preventative outlook on security, financial services overwhelmed by the weight of their risks.

THE INDUSTRY

The financial services industry has always been at high risk for cyber-attacks due to the sensitive and valuable nature of the data they handle and because of the sale and profitability of their industry. Financial services companies spend a lot on cybersecurity; however, they largely maintain a reactive and defensive posture. It is time for cybersecurity functions everywhere to think ahead of attackers with a preemptive, proactive, and preventative stance to cyber threats. A Threat Exposure Management program is the way of the future for all cybersecurity functions. By taking this approach to cybersecurity, the financial services industry can shrink their attack surface, drastically reduce their vulnerabilities, and minimize their exposure to threats.

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

HIVE PRO: THREAT EXPOSURE MANAGEMENT PLATFORM

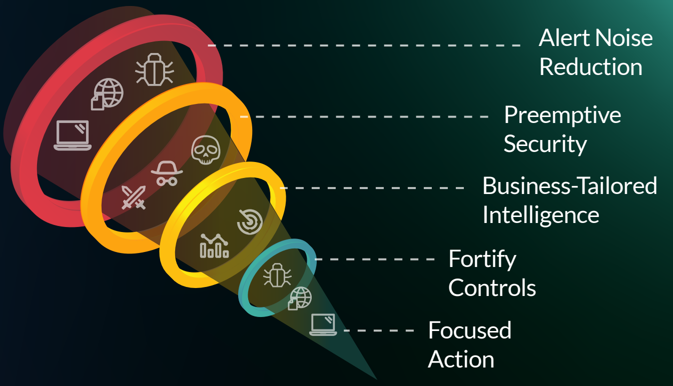
In Action

Common Challenges

- ☒ Continuous asset discovery across an expanding attack surface with limited visibility
- ☒ Combining, filtering, and correlating threat and vulnerability intelligence from thousands of feeds and sources from multiple, siloed tools with varying analytics and priorities
- ☒ Filtering through and prioritizing countless vulnerabilities by business-risk and relevance
- ☒ Frictioned collaboration between Security and IT Operations (or DevSecOps) yielding a slower mean-time-to respond, and greater risks
- ☒ Remediating vulnerabilities, managing workflows and tracking progress from one platform

The Solution

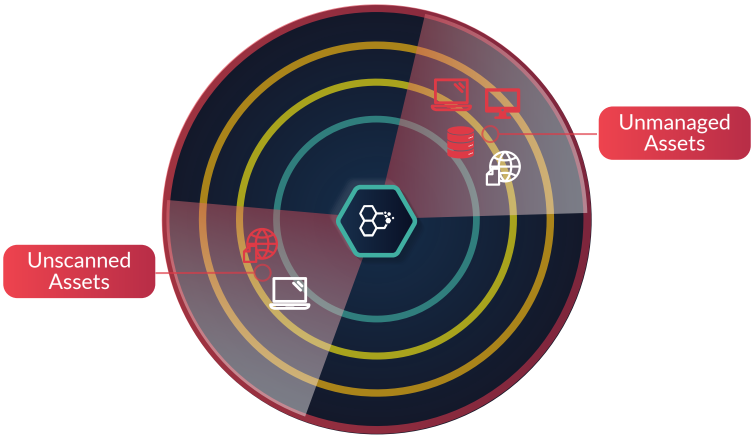
Hive Pro can be tailored to serve all of the world's largest financial services organizations. Our all-in-one, fully integrated platform defends against the full range of cyber-threats, fortifies assets, and strengthens security controls.



BENEFIT 1: WIDE ASSET DISCOVERY

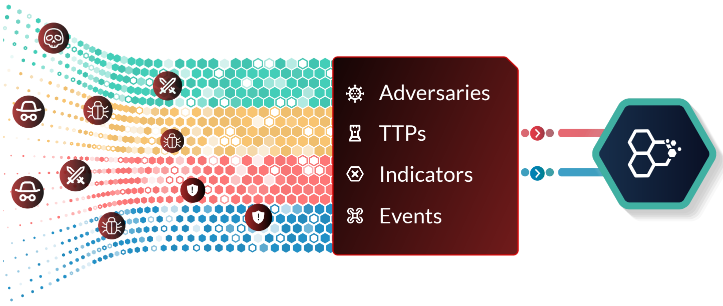
Hive Pro TEM starts with automatic asset discovery and classification, providing instant threat exposure visibility, including blind spots like unscanned and unmanaged assets. Most organizations are unaware of 20% of their total assets, but with HivePro Uni5, cybersecurity teams can easily identify and classify these assets, which is the first step towards securing them.

Automatic Asset Discovery



BENEFIT 2: PREDICTIVE THREAT AND VULNERABILITY INTELLIGENCE

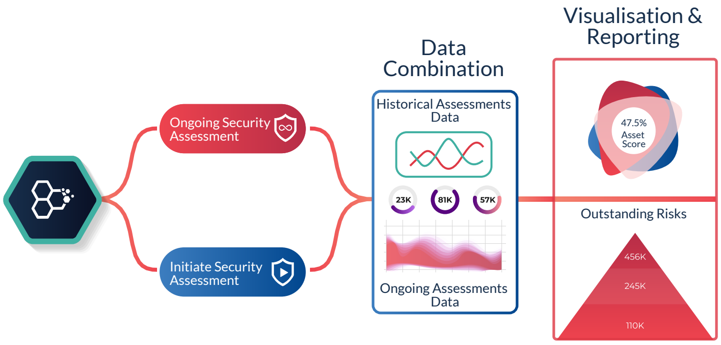
Real-Time Threat Intelligence



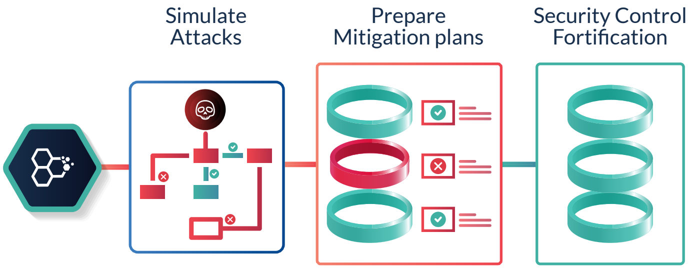
Hive Pro TEM gathers threat intelligence in near real-time and automatically feeds it into the platform, powered by an in-house team of security experts. This enables continuous management of threat exposure, instead of periodic assessments, which quickly become outdated due to the discovery of new vulnerabilities every day. On average, 100+ vulnerabilities were discovered every day in Q1 of 2022, with 80% of public exploits being published before CVEs are released, highlighting the importance of continuous threat intelligence.

BENEFIT 3: SECURITY ASSESSMENT ORCHESTRATION

Hive Pro TEM's deep workflow orchestration layer enables Security teams to initiate new security assessments and drive ongoing security assessments to completion. By combining your historical and ongoing assessment data all in one place, one platform, and one interface, Hive Pro TEM helps Security teams to visualize and report on their outstanding risks, asset health, and room for improvement.


Ongoing Security Assessment
Initiate Security Assessment
Data Combination
Historical Assessments Data
23K
81K
57K
Ongoing Assessments Data
Visualisation & Reporting
47.5% Asset Score
Outstanding Risks
456K
245K
110K

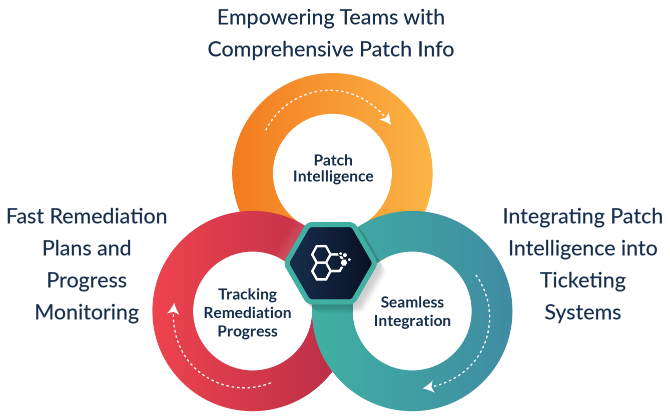
BENEFIT 4: SECURITY CONTROL & ASSET FORTIFICATION



Hive Pro TEM's advanced Breach and Attack Simulation capability allows cybersecurity teams to simulate attacks and identify gaps in their existing compensatory controls. This enables them to prepare mitigation plans in case of a real breach, ensuring that they are always prepared for any potential threat.

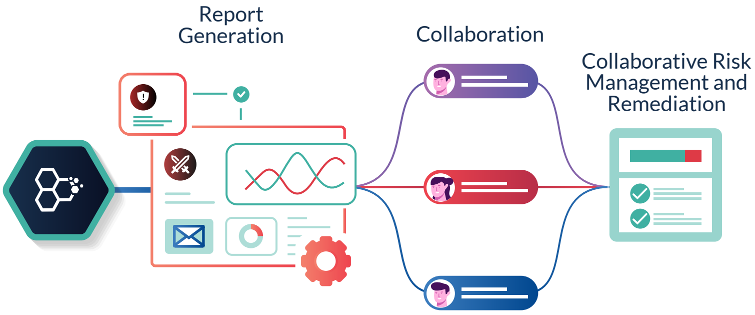
BENEFIT 5: STATE OF THE ART PATCH INTELLIGENCE

Hive Pro TEM'S state-of-the-art patch intelligence capability provides cybersecurity teams with comprehensive information about available patches, including which vulnerabilities do not have patches available and which attacks have patches available but lack a vulnerability signature. With access to over 115,000 patches, Hive Pro TEM allows teams to prepare remediation plans quickly and track their progress, all while integrating with existing ticketing systems. Additionally, the platform's ability to provide patch superseding and fuse this information with ticketing ensures that remediation teams have the best patch intelligence available, enabling them to effectively manage the vulnerability life cycle without the need for additional tools.


Empowering Teams with Comprehensive Patch Info
Patch Intelligence
Fast Remediation Plans and Progress Monitoring
Tracking Remediation Progress
Seamless Integration
Integrating Patch Intelligence into Ticketing Systems

BENEFIT 6: CROSS FUNCTIONAL COLLABORATION & REMEDIATION

Hive Pro TEM provides advanced reporting capabilities, allowing cybersecurity teams to generate contextualized reports for stakeholders, including CISOs, business leaders, and partners, to share their organization's threat exposure posture. This enables teams to communicate the organization's security posture effectively and ensure that stakeholders are aware of the potential risks and threats.



Hive Pro protects digital systems and supports financial services organizations in all global regions. Additionally, Hive Pro's features and capabilities support compliance with regulations such as **GDPR, SOX, PCI DSS, PSD 2, FFIEC, ISO 27001, NIST 800-53, CPPA, NYDFS 500, and more.**

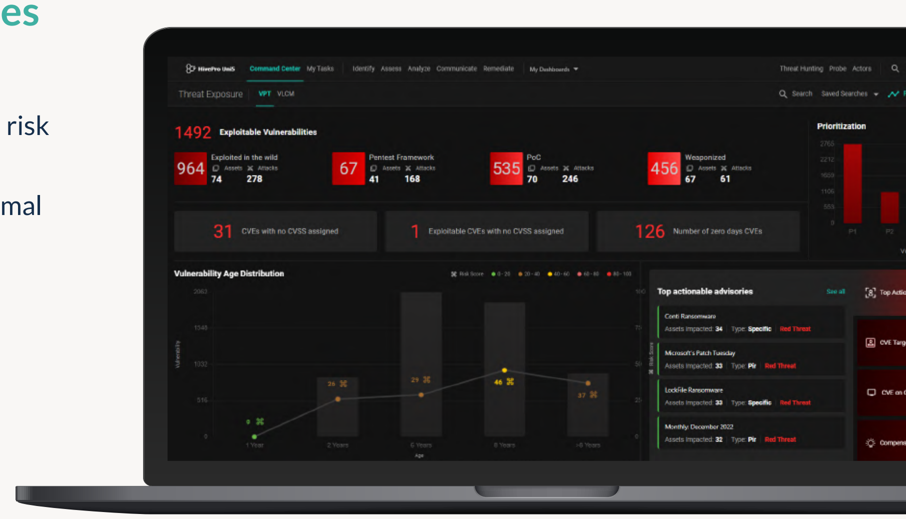
Hive Pro now supports 27+ out of the box integrations

tenable.io vulnerability management | nessus | insightVM | Qualys. | servicenow | CROWDSTRIKE

Fortifying Financial Services Cybersecurity with Hive Pro

Empower your financial services organization's risk management with Hive Pro. Gain continuous insights into vulnerabilities and threats for optimal cybersecurity effectiveness and fortify your defenses.

Start your Free Trial


HivePro Uni5
Command Center
My Tasks
Identify
Assess
Analyze
Communicate
Remediate
My Dashboards
Threat Hunting
Probe
Actors
Threat Exposure
VPT
VLCM
Search
Saved Searches
1492 Exploitable Vulnerabilities
964 Exploited in the wild Assets 74 Attacks 278
67 Pentest Framework Assets 41 Attacks 168
535 PoC Assets 70 Attacks 246
456 Weaponized Assets 67 Attacks 61
31 CVEs with no CVSS assigned
1 Exploitable CVEs with no CVSS assigned
126 Number of zero days CVEs
Prioritization
P1
P2
Vulnerability Age Distribution
Risk Score
0-20
20-40
40-60
60-80
80-100
Vulnerability
Age
1 Year
2 Years
6 Years
8 Years
>8 Years
Top actionable advisories
See all
Conti Ransomware Assets Impacted: 34 Type: Specific Red Threat
Microsoft's Patch Tuesday Assets Impacted: 33 Type: Pir Red Threat
LockFile Ransomware Assets Impacted: 33 Type: Specific Red Threat
Monthly December 2022 Assets Impacted: 32 Type: Pir Red Threat

Hive Pro

Get in Touch

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

Contact Us | Schedule a Demo | Read Our Blog