



WHITEHAWK

Cyber Risk Platform as a Service

Provide your Business and Organization Clients complete Digital Age Risk Services at scale, via a Virtual Consult, online Risk Profile, Maturity Model, Action Plan and Vetted Marketplace of Solutions

www.whitehawk.com

Copyright © 2021 WhiteHawk CEC, Inc. All Rights Reserved.

The information presented here is for general informational purposes only. All information is provided in good faith; however, we make no representation or warranty of any kind, expressed or implied, regarding the accuracy, adequacy, validity, reliability, availability, or completeness of any information presented. Under no circumstances shall we have any liability to you for any loss or damage of any kind incurred as a result of the use of the information provided.

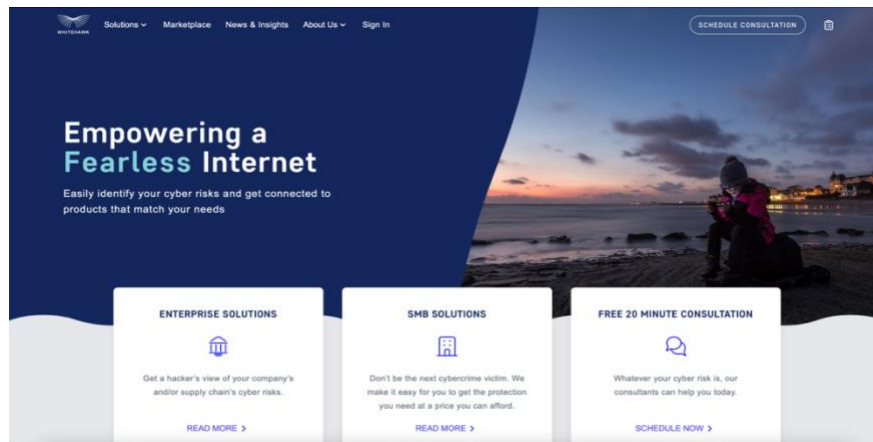
Executive Overview

In the Digital Age environment, all businesses and organizations are at risk daily from online crime, fraud and disruption. We have daily proof that global criminals and our economic and political adversaries continuously seek to steal, disrupt, and conduct industrial espionage across all Sectors, gaining and holding root-level access in critical business and government systems.

What is the role of Insurance Groups, Financial Institutions, Internet Service Providers (ISPs), Managed Service Providers (MSPs) and the Federal Government (as the Prime Client) to provide cyber risk identification/scoping, prioritization and mitigation to their business clients, organizations and suppliers - when the majority don't have the expertise and resources to protect themselves?

Our Cybersecurity Exchange Platform as a Service (PaaS) is an end-to-end Cyber Risk identification, prioritization and mitigation cloud-based ecosystem, that can effectively and affordably service thousands to millions of ISP, MSP, Bank and Insurance Group business, organization, state and local clients and their supply chains - continuously. Unique Features include:

- Complimentary Cyber Threat Readiness Questionnaire, Risk Profile, Cyber Risk Consult
- Automated & Documented Cyber Risk Prioritization and Scorecard matched to Solution Options – Action Plan
- Matching to Vetted Cyber Innovation Solution Partners for Enterprise & SMB Clients – updated continuously
- Tailored Risk Platform of Online Services and Business Models to meet the objectives of Prime Client
- Grounded on publicly available risk data sets, proven AI-based Cyber Risk analytics, models & solutions
- Ability to seamlessly incorporate additional features to meet any business or mission objectives
- Co-branding, white labeling, annual licensing, revenue sharing and platform O&M services



The Platform

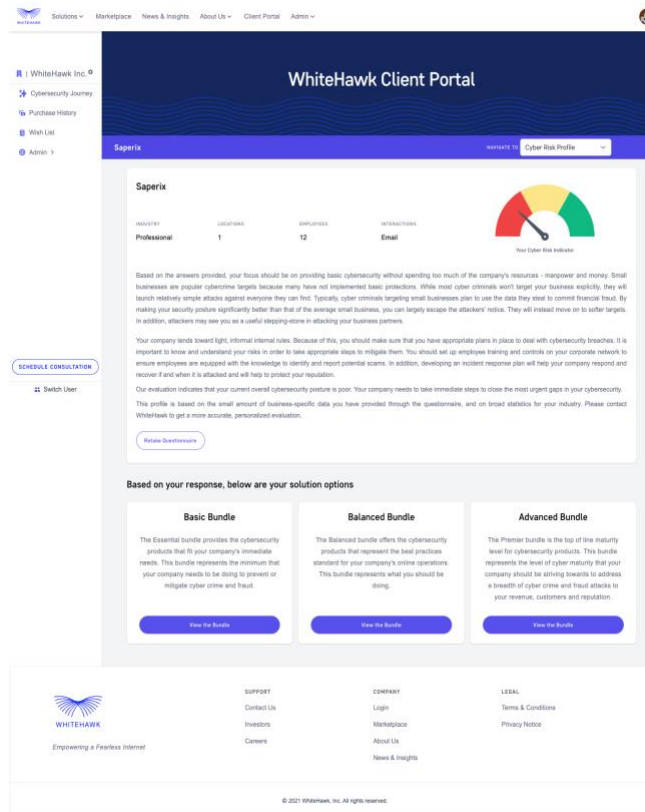
Deliver within 90-days a tailored version of the Cybersecurity Exchange Platform as a Service (PaaS), as an end-to-end Cyber Risk identification, prioritization and mitigation cloud-based ecosystem, that can effectively and affordably service thousands to millions of your business or organization clients and their supply chains - continuously.

Platform enablement for the Prime Client include:

- Sophisticated in-house cyber team can effectively service thousands of business or government clients simultaneously, continuously and affordably
- Differentiated Digital Age Risk Services, Solutions with real impact
- Insight into cyber risk trends across client portfolio on a quarterly basis
- Easy introduction of innovative products and services tailored to client needs

Why WhiteHawk - Value Proposition:

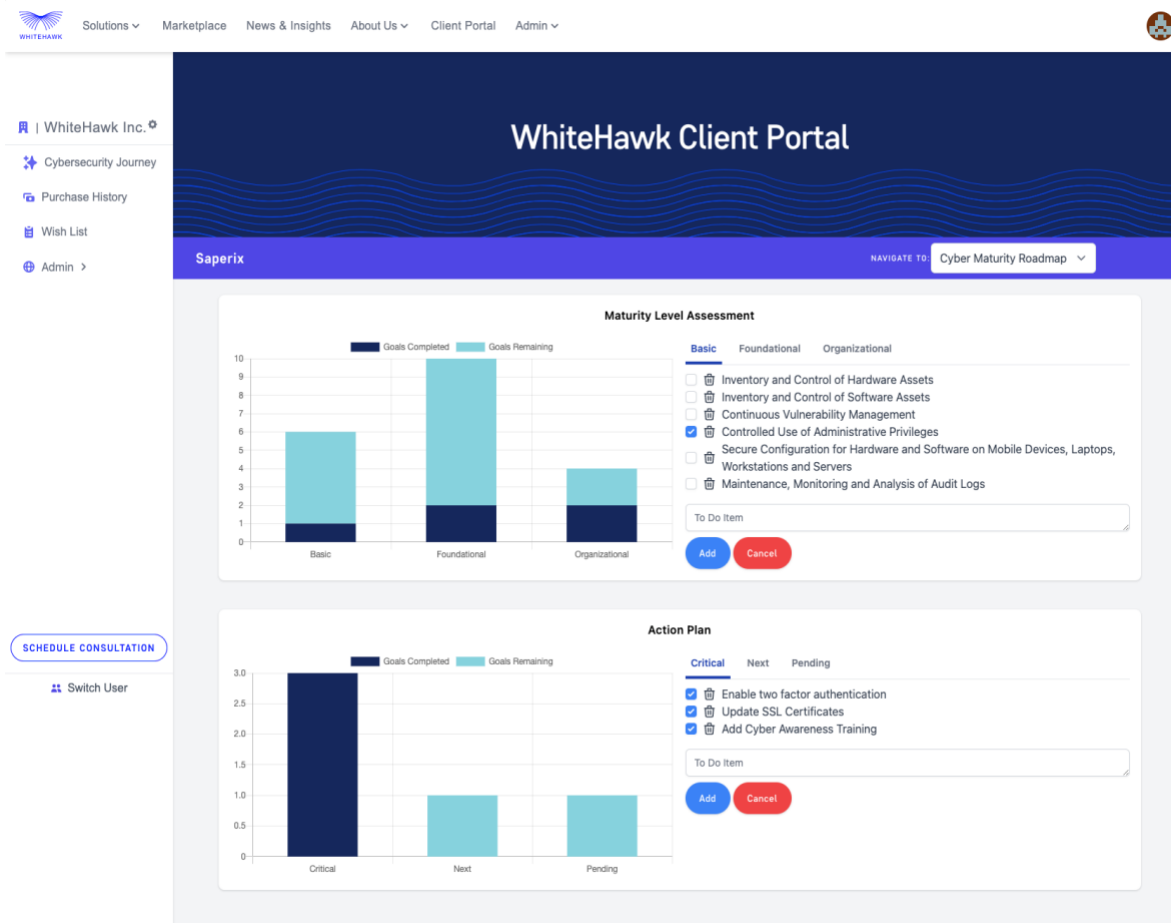
- 4 years of R&D, product line testing, evolution and lessons learned with Private & Public Sectors
- Our cybersecurity online exchange is a best of breed proven commercial commodity and no need to custom build
- Cutting edge Digital Age Risk Services with revenue share



Tailored Cyber Risk Journey

Clients start their [Cyber Risk Online Journey](#) with a virtual consult with a Cyber Analyst who walks them through the 30min to 1 hour process that includes an online Cyber Threat Readiness Questionnaire, 10 quick non-technical, non-intrusive questions generating:

1. A Cyber Risk Profile that outlines a client’s threat landscape of their sector and peers of the same size and scope.
2. An online living cyber risk account that includes the baseline of their maturity model, built upon best of breed cyber risk frameworks and standards (NIST, CIS, ISO, CMMC).
3. A Cyber Risk Scorecard (Action Plan) with prioritized risk areas of focus, their Risk Baseline (mapped to CIS/CMMC), and Risk Mitigation solution options, providing an understandable and actionable plan maturity model and plan (both in an online accessible account and a PDF report).
4. Innovative, impactful, easy to implement and affordable solution options that map directly to the clients’ priority risks, from a continuously updated, vetted marketplace of over 400 products and services.



The screenshot displays the WhiteHawk Client Portal interface. The main header reads "WhiteHawk Client Portal" and "Saperix". A navigation bar includes "Solutions", "Marketplace", "News & Insights", "About Us", "Client Portal", and "Admin". A left sidebar contains "WhiteHawk Inc.", "Cybersecurity Journey", "Purchase History", "Wish List", and "Admin". The main content area features a "Maturity Level Assessment" chart and an "Action Plan" chart.

Maturity Level Assessment

Maturity Level	Goals Completed	Goals Remaining
Basic	1	6
Foundational	2	8
Organizational	2	2

Action Plan

Priority	Goals Completed	Goals Remaining
Critical	3	0
Next	0	1
Pending	0	1

WhiteHawk Client Portal

Saperix NAVIGATE TO: Cyber Risk Rating



The Cyber Risk Rating measures a company's relative security effectiveness. Saperix falls into the Basic category, meaning its relative security effectiveness is moderate, having a weak security performance and high risk.



Risk Vector Analysis

- Compromised Systems B
- Public Disclosure A
- System Patching A
- Application Security C
- Communications Encryption B
- Email Security A
- User Behavior D

Recommended Focus Areas

- Focus Area 1: User Behavior
- Focus Area 2: Application Security
- Focus Area 3: Compromised Systems

CIS Control-Based Maturity Level Assessment Based on Externally Observed Risk Rating



CIS Controls Mapped to CMMC Maturity Levels

CIS CONTROLS	CMMC MATURITY LEVELS	CMMC MATURITY LEVELS			
		L1	L2	L3	L4/L5
Penetration Tests and Red Team Exercises #20					
Email and Web Browser Protections #7					
Limitation and Control of Network Ports, Protocols, and Services #9					
Application Software Security #18					
Inventory and Control of Software Assets #2					
Continuous Vulnerability Management #3					
Controlled Use of Administrative Privileges #4					
Maintenance, Monitoring and Analysis of Audit Logs #6					
Data Recovery Capabilities #10					
Secure Configuration for Network Devices, such as Firewalls, Routers and Switches #11					
Implement a Security Awareness and Training Program #17					
Incident Response and Management #19					
Inventory and Control of Hardware Assets #1					
Secure Configuration for HW & SW on Mobile Devices, Laptops, Workstations and Servers #5					
Malware Defenses #8					
Boundary Defense #12					
Data Protection #13					
Controlled Access Based on the Need to Know #14					
Wireless Access Control #15					
Account Monitoring and Control #16					
		7/8	10/16	5/19	0/20

Solution Options Based on Risk Rating

Essential Bundle

The Essential bundle provides the cybersecurity products that fit your company's immediate needs. This bundle represents the minimum that your company needs to be doing to prevent or mitigate cyber crime and fraud.

[View the Bundle](#)

Balanced Bundle

The Balanced bundle offers the cybersecurity products that represent the best practices standard for your company's online operations. This bundle represents what you should be doing.

[View the Bundle](#)

Premier Bundle

The Premier bundle is the top of line maturity level for cybersecurity products. This bundle represents the level of cyber maturity that your company should be striving towards to address a breadth of cyber crime and fraud attacks to your revenue, customers and reputation.

[View the Bundle](#)

[Download Scorecard](#)

Cyber Risk Scorecard

WhiteHawk’s Cyber Risk Scorecard provides businesses and organizations a topline cyber risk report and summary of a company’s effectiveness at addressing the impacts of online crime, fraud and disruption. We start with cyber global threat trend analytics, providing powerful threat landscape sector context, then the cyber risk profile and with add cyber risk continuous monitoring data sets. These inputs to our automated Cyber Risk Scorecards, enable companies to take smart action to mitigate cyber risks to their revenue, reputation, and operations. To learn more about WhiteHawk’s Cyber Risk Scorecard action plan report, view this link to the [WhiteHawk Cyber Risk Scorecard](#).

Cyber Risk Scorecard Results Summary

We are pleased to present the results of the WhiteHawk Cyber Risk Scorecard. This section is an executive overview. Subsequent sections provide associated descriptions and context to our findings and recommendations.

Company	Domain	# IP Addresses
Midsize Data Management Company	https://www.test.com	19,610
Security Rating		Risk Vector Performance
<i>Ratings measure a company's relative security effectiveness.</i>		<i>Risk Vector grades show how well the company is managing each risk vector.</i>
640	Advanced: 900 – 740	Compromised Systems: B
	Intermediate: 740 – 640	Communications Encryption: D
	Basic: 640 – 250	User Behavior: A
		Systems Patching: C
		Application Security: C
		Email Security: C
		Public Disclosure: A
Prioritized Areas of Focus		
<i>WhiteHawk Cyber Analyst recommendations for top-3 Focus Areas the company should consider</i>		
Recommended Focus Area 1:	Communications Encryption	
Recommended Focus Area 2:	Systems Patching	
Recommended Focus Area 3:	Email Security	
Solution Options		
<i>Solution options that address primary business risks identified in the Cyber Risk Scorecard</i>		
Basic Bundle	Balanced Bundle	Advanced Bundle
<ul style="list-style-type: none"> - Sophos: Sophos Email Protection - KnowBe4: 1 Year - Security Awareness Training 	<ul style="list-style-type: none"> - Symantec: Symantec Desktop Email Encryption - StorageCraft: ShadowProtect IT Edition V5.x Subscription - 1 Year - Micro Focus Software Inc.: ZENworks Patch Management 	<ul style="list-style-type: none"> - Forcepoint: SURVIEW Insider Threat Core - Micro Focus Software Inc.: Sentinel Enterprise - Verodin: Security Implementation Platform (SIP) - D3 Security: D3 SOAR

WhiteHawk designed the Cyber Risk Scorecard to provide clients with actionable information to:

- Facilitate budget-based and impactful, risk reduction decision making, based upon real cyber risk indicators and sector wide threat vectors
- Enable smart and timely action
- Prevent online crime and fraud from disrupting operations

WhiteHawk Cyber Analysts perform customized analytics to:

- Deliver affordable and impactful options to mitigate cyber risks of small and midsize businesses and organizations, prioritized to reduce the most significant risks
- Track key actions and mitigations to accept or address known risks
- Provide maturity planning in the form of an achievable risk reduction roadmap, enabling data-driven decision making in terms of business risk and budget constraints
- Maintain informed and enabling engagement.

Additional Services

Cyber Risk Portfolio Analytics and Reports

The WhiteHawk The Cyber Risk Portfolio Report is an aggregated, anonitized risk view across all your clients, revealing current vulnerability trends and changes over time, across all included companies or organizations.

View Executive Level Trend Reporting:

- Gather and analyze cyber risk data and analytic outputs for each company and organization in your portfolio
- Perform data collection, assessment, and analytics using externally available open data

Cyber Risk Portfolio Reporting contains:

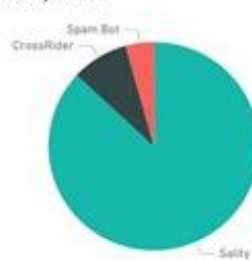
- Analytic summary across the entire client company or organization portfolio
- Summary of top findings for prioritization & risk mitigation action
- Report of all company: security ratings and top risk vectors
- Historical context for Risk Monitoring trends and insights for all companies in the portfolio
- Analyst Notes that summarize all of the above

Compromised Systems

Source Host Geo IP Location



Count of Infection by Infection



Count of Infection by Month



Compromised Systems

Risk Type	GeoIP Location	Infection	Detection Mechanism	Days	Year	Month	Day
Botnet Infections	United States	Salty	p2p	1	2018	August	25
Botnet Infections	United States	Salty	p2p	6	2018	November	21
Botnet Infections	United States	Salty	p2p	1	2018	November	25

Spam Propagation - Most Recent

Vendors	Infection	Email Subject	Month
	Spam Bot		March

Platform & Business Model Flexibility

White Labeling & Co-Branding: The www.whitehawk.com platform uses open technologies that cleanly decouple UI/UX and the backend business processing services. We have branding/theming configurations that take place only in the UI. We do this through template components, interpolating branding data from centralized configuration files. The branding includes theming elements such as colors, fonts, images, logos, and slogans, enabling us to establish a white labeled instance for any brand quickly.

Marketplace Vendor Solution Vetting & Onboarding: WhiteHawk maintains an in-house dedicated Vendor Management team that scouts, vets, and onboards innovative solution vendors onto the online Marketplace. We will work closely to meet the Prime Client's business objectives and collaborate on the identification and onboarding of solutions for its. WhiteHawk's mature vendor process onboards on average 1 to 2 cyber risk, security, and analytics vendors a week, with consistent and repeatable business processes. The Vendor Management team at WhiteHawk conducts vendor technology demonstrations and follow-up business model discussions including the appropriate revenue sharing agreements. [Top 12 Innovative Cyber & Analytics Companies](#) and [Innovative Vendors Focused on Enterprises](#)

Security: Our platform is hosted in a secure and stable cloud-based environment, provided with commercial levels of uptime, quality of service, and cybersecurity protection. WhiteHawk maintains separate development and production environments. Our infrastructure instances reside on multiple AWS regions behind high-availability firewalls that detect and prevent security threats. Automated tools are deployed within the network to support near-real-time analysis of events to detect system-level attacks. WhiteHawk maintains and continuously updates our cybersecurity policies, processes and technologies.

Platform Assessment Mapping to Security Standards: The NIST and ISO controls are daunting even for sophisticated cyber professionals. With that in mind, our in-house cyber analysts have performed deep analysis and mappings of NIST and ISO controls to automate mapping to solution options. WhiteHawk initially built our maturity models based on the CIS framework, which maps to the NIST framework and is impactful and actionable for the vast majority of companies and organizations. We also map the risk vector data to our maturity models, delivering an easy-to-understand documented path to resilience. Using this approach, we have implemented the CIS and CMMC frameworks as a foundation to our virtual client consultations. By aligning multiple frameworks, WhiteHawk delivers an uncomplicated and documented path to CIS and CMMC compliance. With our flexible and open architecture, we are able to customize and integrate any additional security frameworks selected by the client.

Cyber Risk Continuous Monitoring Integration into Platform, Customer Journey and Assessments: We have integrated best of breed Partner Cyber Risk Continuous Monitoring API's (that use publicly available global risk data sets, cybersecurity risk standard algorithms and AI based analytics) into our online customer consult, online account and Cyber Risk Scorecard as desired, providing real-time view of a gamut of risk vectors that are impacting any company or organization with a URL/IP Address. This "satellite view" of cyber risk dramatically advances the customer services that can be delivered and their impact.

About Us



Easily find out where the biggest risks are



In near real time make the changes you need to protect your organization



Get alerted to new threats that are targeting you



Track how your network vulnerabilities change over time

WhiteHawk, Inc., is the first online Cybersecurity Exchange based on a platform architecture that is Artificial Intelligence (AI)-driven, with a focus on identifying, prioritizing, and mitigating cyber risks for businesses of all sizes. WhiteHawk continually vets and assesses risk-focused technologies, methodologies, and solutions that are impactful, affordable, and scalable to stay up to date on current cyber threat vectors to businesses, organizations, family offices, and individuals. We have an online approach to determining your key cyber risks through a Cyber Threat Readiness Questionnaire, and as appropriate, a cyber risk assessment. Using this information, we then match tailored risk mitigation solution options to companies and organizations based on current threat trends across key sectors. Our Cyber Consultants on staff help build a tailored cyber maturity plan customized to meet your business or mission objectives.

For more information, visit www.whitehawk.com.

WhiteHawk CEC Inc.
Terry Roberts - Founder, President, & CEO
consultingservices@whitehawk.com



WHITEHAWK®

Cyber Risk **Platform** as a Service

WhiteHawk CEC Inc.

www.whitehawk.com

