

MAY 2020



# **WhiteHawk**

## **Online Cybersecurity Exchange**

2020 Annual General Meeting

## SAFE HARBOUR STATEMENT

This information is given in summary form & does not purport to be complete. Information in this presentation, including financial information, should not be considered as a financial projection, advice or a recommendation to any particular or potential investors in relation to subscribing for securities in WhiteHawk. Before acting on any information you should consider the appropriateness of the information having regard to these matters, any relevant offer document & in particular, you should seek independent financial advice. All securities involve risks, which include (among others) the risk of adverse or unanticipated market, financial or political developments and, in international transactions, currency risk. This presentation may contain forward looking statements including statements regarding our intent, belief or current expectations with respect to our businesses & operations, market conditions, revenues, market penetration, & results of operations. Readers are cautioned not to place undue reliance on these forward looking statements. WhiteHawk does not undertake any obligation to publicly release the result of any revisions to these forward looking statements to reflect events or circumstances after the date hereof to reflect the occurrence of unanticipated events. While due care has been used in the preparation of forward looking information, actual results may vary in a materially positive or negative manner. Forecasts & hypothetical examples are subject to uncertainty & contingencies outside WhiteHawk's control. Unless otherwise specified all information is stated as at 20 May 2020

# WhiteHawk

*Founded 2015: First online SMB Cybersecurity Exchange*

- New Website July/August 2020
- Corporate Snapshot (ASX:WHK)
- Overview: Financial Highlights & Outlook
- Key Contracts
- Revenue by Year
- 2020 Outlook
- Enterprise Product Lines & Revenue Streams
  - Cyber Risk Radar
  - CMMC
  - Cyber Risk Program
- SME Product Lines & Revenue Streams
  - Cyber Risk Scorecard & Online Customer Journey
  - Sontiq/WhiteHawk Business Suite
- The Team

[Marketplace](#)[News & Insights](#)[About Us](#)[Client Portal](#)[FREE CONSULTATION](#)

# Empowering a Fearless Internet

Easily identify your cyber risks and get connected to products that match your needs

ENTERPRISE LEVEL SOLUTIONS



SMB FOCUSED SOLUTIONS



FREE 20 MINUTE CONSULTATION



# About WhiteHawk

*Founded 2015: First online SMB Cybersecurity Exchange*

## Business Model & Focus:

- Drive global risk transparency, in order to make smart business & mission decisions
- Leverage AI & Open Data
- Be Product/Vendor Agnostic
- Continuously vet innovation; 1-2 Companies a week
- Partner with Best of Breed Commercial Technologies & SaaS/API Based Analytic Platforms & Services
- Drive our online Cybersecurity Exchange to identify, prioritize & mitigate cyber risks at scale across companies & organizations

*Be the customer advocate always – providing products & services based on their needs & budget*

# Corporate Snapshot



ASX Ticker  
**WHK**



Shares on issue  
**159 m**



Last share price  
**\$0.061**



Undiluted Market cap  
**A\$9.7 m**



Net Cash  
**~ A\$2.3 m**  
as of 31 March 2020  
Including receivables



Listing Date  
**24 Jan 2018**

## Top 5 Shareholders

## % Shares Outstanding

Vivien Enterprises Pte Ltd	4.82%
Mr Darren Carter	3.87%
Terry Roberts	3.79%
Mr Amilcar Albino Moreno	3.49%
Vantage House Limited	3.45%

**Top 5 Shareholders** 19.42%

**Top 20 Shareholders** 37.47%

**Directors & Associates** 5.02%

All figures are as of 19/05/2020 unless otherwise noted

## Overview: Financial Highlights

Contracted revenue for calendar year 2020 currently at US\$1.5m (~AU\$2.4m)

- Strong pipeline of opportunities across currently operating revenue streams

Current cash balance as of 31/03/20 is US\$1.5m (~A\$2.4m) which includes a debt limit of A\$400k

- Primary use is to fund operations while driving online & advisory sales & expanding pipeline.
- Potential A\$1.5m ESA Facility available to finance growth

Sales channels & marketing strategy driving increased online sales

- Each Cyber Risk Radar sale (US\$250K to US\$1M) drives online sales & advisory contracts
- Sontiq/EZShield Partnership to service Financial Institution & Managed SaaS Service Provider business clients (5,000 to 140,000 SME's with each contract - US\$3.2M to US\$21.6M)

# U.S. Federal Government CIO Contract Update:

**Contract with U.S. Federal Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) under Prime, Guidehouse (formerly PWC Federal):**

- WhiteHawk is a sub-contractor on a contract won by the prime contractor. The contract is for 7 years (1 year with 6 option years)
- WhiteHawk's development project is scoped to be between USD\$300K to USD\$600K in 2020 & 2021.
- Cybersecurity online marketplace has been scoped, architected & mapped to customer initial requirements for phase 1 completion in 2020 & phase 2 in 2021.

Meritalk link [CISA Selected as QSMO for Cybersecurity.](#)

[Marketplace](#)[News & Insights](#)[About Us](#)[Contact](#)[Client Portal](#)[FREE CONSULTATION](#)

Search



Browse by Vendor...

Clear All Filters &gt;

## Browse Categories

[Access Control](#)[Antimalware](#)[Application Security](#)[Backup](#)[Compliance Reporting](#)[Data Leak Prevention](#)[Denial of Service Mitigation](#)[Email Filter](#)[Encrypted Communication](#)[Encrypted Storage](#)[Forensics](#)[See All 36 Categories >](#)

## Price Range

## Marketplace

One stop shop for cyber risk products and solutions

## 382 Products

Get connected to products that match your cybersecurity needs.

SORT BY:

Alphabetical (Asc...



Security Awareness Training

\$\$\$



Security Awareness Training

\$\$\$



Security Awareness Training

\$\$\$

# Defense Industrial Base Contract & CMMC

- Current contract builds upon the lessons learned from two smaller contracts, for a total of over USD\$700K, incorporating a flexible Tiered approach to Cybersecurity Maturity Model Certification (CMMC) commencing in 2020

## Positioning for Growth

- Provided initial impact of COVID-19 analytics to some key suppliers
- Conducting live demonstrations of Cyber Risk Radar platform to U.S. Federal Government Supply Chain Cyber Risk Leads
- Provided response to April 2020 CMMC Advisory Board Continuous Monitoring RFP
- Nextgov: Defense Contractor Certification Body Says Maintenance of Companies' Cybersecurity Posture is Within its Role

# Cyber Risk Program contract with major U.S. Manufacturer via Global Consulting Partner

- Cyber Risk Program is tailored & delivered to the Chief Information Officer (CIO), Executive Team, Chief Executive Officer (CEO), & Board of Directors (BoD)
- This independent risk assessment subscription for 8 Business Groups includes: Cyber Risk Continuous Monitoring & Prioritization; Quarterly Executive Level Scorecards & Reporting; & Bi-Annual Risk Validation by Real-Time Red Team Assessment.

## Progress for the Quarter

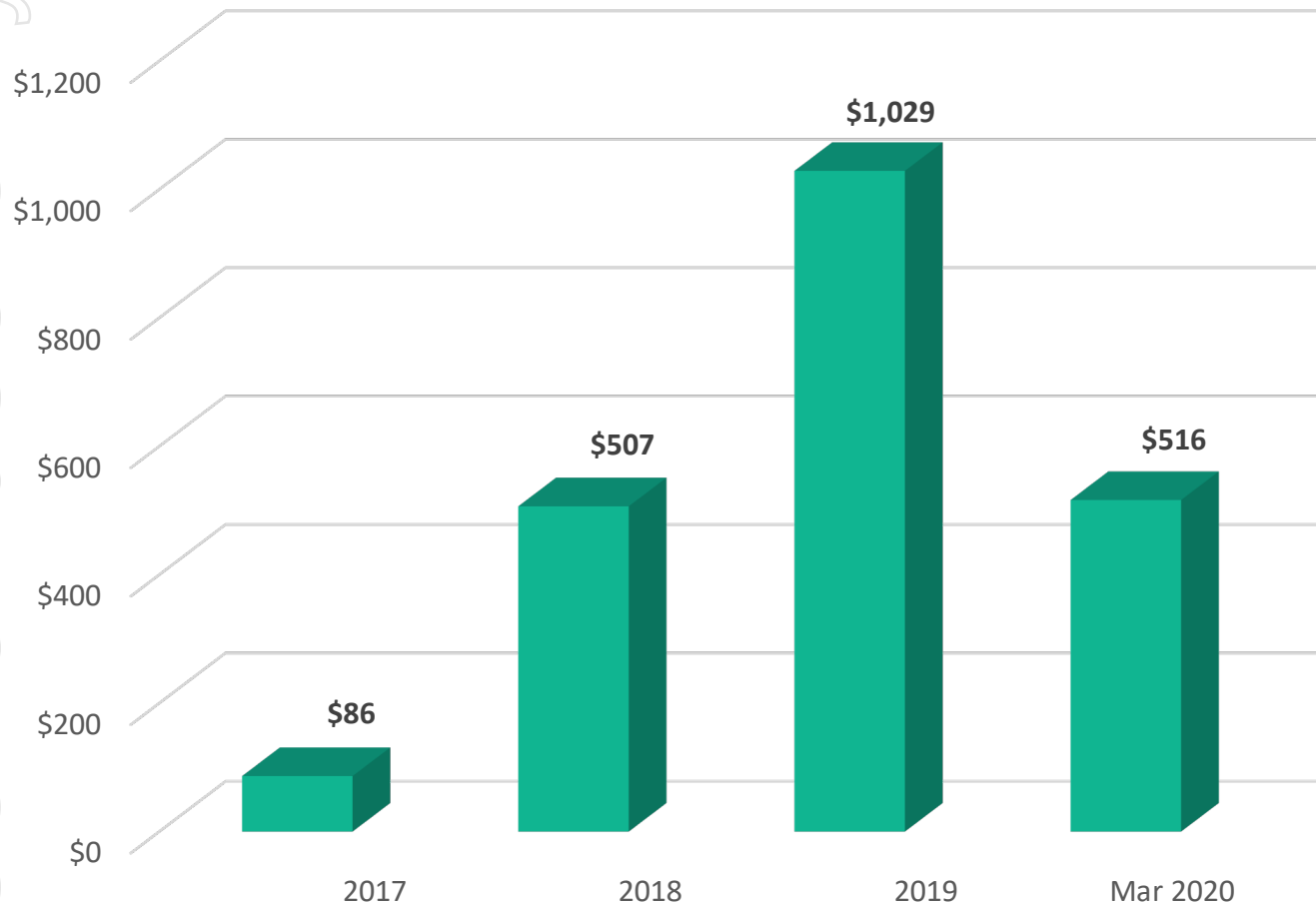
- Completed Cyber Risk Monitoring & Scorecards for 3 Business Groups
- Initial scoping & Cyber Risk Monitoring for additional 5 Business Groups
- Planning & coordination for real-time red team initial assessment in 2<sup>nd</sup> QTR 2020.

## U.S. Government Cyber Risk Radar Contract:

- Contract is the result of a Proof of Value that was implemented early in 2019 across 10 vendors for the same US Federal Government agency.
- WhiteHawk demonstrated through automation & subject matter expertise, the status & health of suppliers; using global publicly available data sources, AI analytics, & custom Cyber Analytics to assess & report on top risk indicators & vectors, areas that may require prioritized attention.
- This **annual SaaS** contract, will see WhiteHawk generate base revenues of US\$580,000 over the first year of the contract, with 4 additional option years, worth a further US\$600,000 (each additional year subject to the client exercising each of those options).
- WhiteHawk Cyber Risk Scorecards will be provided quarterly, for 150 to 300 vendors to this US Federal Government Chief Information Security Officer, via an integrated risk management dashboard.

# Overview: Revenue by Year in \$US Thousands

*Growing Revenues*



## 2020 Outlook

Taking into account the impact of the Global Pandemic on the dramatic growth of cybercrime & fraud on our current & potential customers, WhiteHawk is doubling down on the more economically resilient Sectors of the U.S. Federal Government & the U.S. Defense Industrial Base for the rest of 2020:

- 1) Continued sale of Cyber Risk Radars across the supply chains of U.S. Department of Defense Military Services & Agencies.
- 2) New Federal Contractor Cybersecurity Regulatory policies (in particular the Cybersecurity Maturity Model Certification – CMMC), focusing on our WhiteHawk online Company Customer Cyber Risk Journey, as an efficient path for Federal & Defense Industrial Base (DIB) Contractors to achieve CMMC in 2020 & beyond.
- 3) Recently responded to quick turn CMMC Advisory Board (AB) Continuous Monitoring RFP, to phase in over the next 4 years across the 330,000 DIB contractors.
- 4) Position our Cyber Risk Program as an enabler for DIB Prime (large) Companies to achieve CMMC level 5 in 2020 & beyond.
- 5) Focus on integrated Service with the Sontiq/EZShield Business Suite SaaS service as an effective means for SME's to mitigate the cyber risks during the Pandemic.

*Achieving an average of 30%-40% gross margin aggregate across all products lines*

# COVID Related Business Scams on the Rise

*Mobilizing Your Cyber Risk Strategy*

## Hackers Target Companies with Coronavirus Scams

<https://www.wsj.com/articles/hackers-target-companies-with-fake-coronavirus-warnings-11583267812>

## FTC Reports COVID-19 stimulus payment scams

<https://www.consumer.ftc.gov/blog/2020/04/coronavirus-stimulus-payment-scams-what-you-need-know>

## Digital Fraudsters Increase Attacks Against Multiple Industries during Pandemic

<https://www.globenewswire.com/news-release/2020/05/13/2032727/0/en/Digital-Fraudsters-Increase-Attacks-Against-Multiple-Industries-During-Pandemic-Use-COVID-19-Scams-to-Target-Younger-Generations.html>



**79.1 million** identity crime victims – that is **2 every second!**<sup>1</sup>



**\$16.8 billion** stolen<sup>1</sup>



**3 of 5** consumers have been part of a breach; **1 of 5** is a victim of fraud/ID theft<sup>1</sup>



**58%** of consumers have checked their credit scores in the last 12 months<sup>2</sup>

1. Javelin Strategy & Research, 2018 2. INFCC

# ENTERPRISE PRODUCT LINES/REVENUE STREAMS

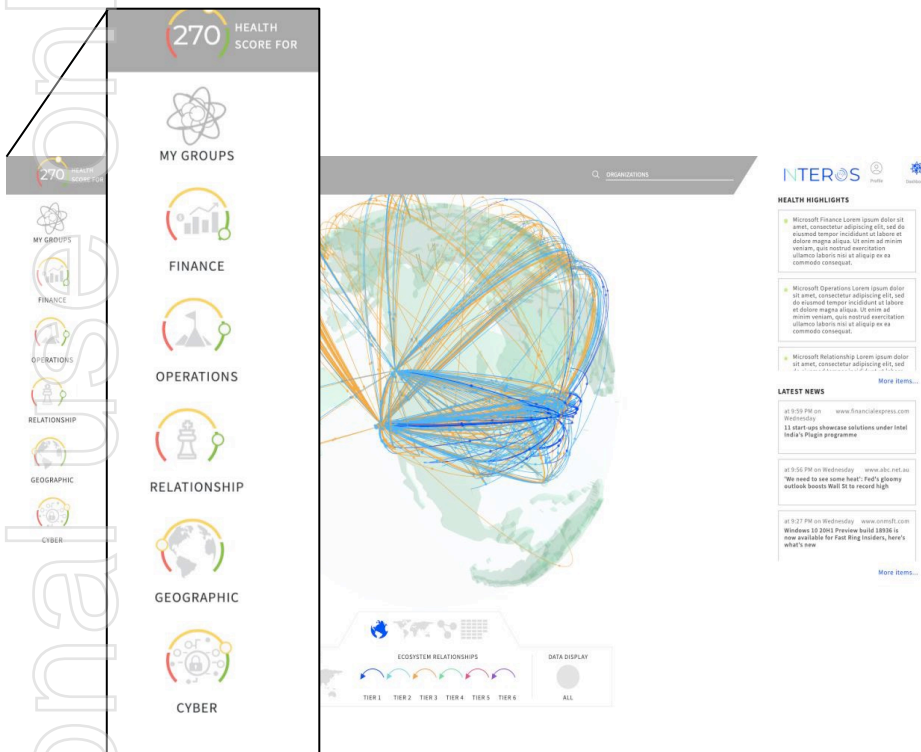
*Affordable & immediately impactful solutions for businesses of all sizes*

- **Cyber Risk Radar – Across Suppliers/Vendors**
  - *Annual SaaS Subscription*
  - *Priced by Vendor & Features - \$1,000 to \$3,000 per vendor*
  - *Average contract 100 to 1,000 vendors*
  - *Federal Government & Industry Sales Channels*
  - **[WhiteHawk Cyber Risk Radar Demo Video](#)**
- **Cyber Risk Program – For Mid to Large Companies**
  - *Annual SaaS Subscription*
  - *Priced by Number of Business Groups & Features - \$10,000 to \$100,000 per Business Group*
  - *State Government & Industry Sales Channels*
  - **[WhiteHawk Cyber Risk Program Demo Video](#)**

# Cyber Risk Radar:

## Supplier Risk Discovery, Alerting, Prioritization & Mitigation

### Business Risks

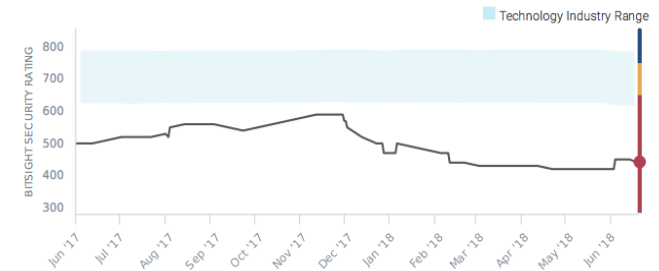
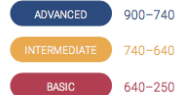


### Cyber Risk Rating

BitSight Security Rating

## 430

Our ratings measure a company's relative security effectiveness.



The Security Rating for Saperix, Inc. has varied from **410** to **580** over the past 12 months. The blue band represents the range of ratings for all companies within the Technology industry. Outliers are excluded. Sudden drops in ratings can be due to publicly disclosed breaches, an increase in observed events, file sharing activities, or poorly configured diligence records.

### Cyber Risk Mitigation

#### Solution 1

##### Basic Bundle

The Basic bundle provides the essential 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

[Buy Now](#)  
[Review the Bundle](#)

#### Solution 2

##### 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

[Buy Now](#)  
[Review the Bundle](#)

#### Solution 3

##### Advanced Bundle

The Advanced 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.

[Buy Now](#)  
[Review the Bundle](#)

## WhiteHawk Customer Journey Online Demo

The WhiteHawk Essential, Balanced, & Premier bundles are focused on providing a **customized, complete, & affordable** cyber mitigation package for each customer.

# Cyber Risk Radar: Levels & Features

*Sized & Customized to Fit Your Mission Objectives*

Features	Basic	Balanced	Advanced
One-time Cyber Risk Scorecard Report	✓	✓	✓
Cyber Analyst Consultation with each Supplier	✓	✓	✓
WhiteHawk Platform Access	✓	✓	✓
Cyber Risk Portfolio Report		✓	✓
Cyber Risk Continuous Monitoring of each Supplier		✓	✓
Cyber Risk Supplier Relationships		✓	✓
Project Management		✓	✓
Cyber Risk Rating Dashboard Access		✓	✓
Quarterly Cyber Risk Scorecard & Portfolio Updates		✓	✓
Business Risk Snapshot			✓
Business Risk Dashboard Access			✓
Security Instrumentation Platform			✓
Vendor Risk Management Dashboard			✓

*Additional Cyber & Business Risk Capabilities & Services Available to Support Organization's Objectives*

## Prime Defense Contractor CMMC Objectives

- Start to demonstrate that a consistent Cybersecurity Maturity Model Certification (CMMC) Program is being put in place across Suppliers/Vendors/Team-Mates
- Align current VRM/SCRM cyber risk reviews & processes to the CMMC framework – minimizing duplication & maximizing automation
- In support of all new proposals & current contracts, conduct initial Cyber Risk Assessments & maintain Cyber Risk Scorecard documentation that provide a path to the appropriate CMMC level for each Supplier/Vendor
- Provide all SMB Suppliers/Vendors with a complimentary cyber risk mitigation service that maps to CMMC controls
- Within 3 years, put in place a comprehensive, repeatable CMMC program across all – efficiently & cost effectively

*Be leveraged as a differentiator on all proposals & contract renewals*

# Fast Track Meeting DoD's CMMC Requirements

- Monitor suppliers' key risk indicators
- Mitigate suppliers' verified vulnerabilities
- Ensure compliance with appropriate CMMC level requirements

## TIER 3 SUPPLIERS

### One-time Cyber Risk Scorecard — Snapshot

Suppliers that have consistently presented high/advanced security rating scores. Provides an annual "physical." Recommended for vetting of all new suppliers, vendors & services teammates.

## TIER 2 SUPPLIERS

### Continuous Cyber Risk Monitoring

### 4X Cyber Risk Scorecard — In-Depth

Suppliers that have presented Intermediate security ratings, thereby ensuring continuous monitoring and improvement of their security posture, primarily for Professional Service teammates.

## TIER 1 SUPPLIERS

### Continuous Business Risk Monitoring

### Continuous Cyber Risk Monitoring

### 4X Cyber Risk Scorecard — In-Depth

Critical, Strategic, and Important Suppliers. Include Suppliers of HW/SW/Professional Services & providers that have basic security ratings and/or low business risk health scores; thereby enabling continuous improvement of their risk and security posture.

\* Requires Internal SOC/NOC Integration

## LEVEL 1 BASIC CYBER HYGIENE

### 17 Practices

- Equivalent to FAR 48 CFR 52.204-21

## LEVEL 2 INTERMEDIATE CYBER HYGIENE

### 72 Practices

- Comply with the FAR
- Select subset of 48 practices from NIST SP 800-171 r1
- Additional 7 practices to support intermediate cyber hygiene

## LEVEL 3 GOOD CYBER HYGIENE

### 130 Practices

- Comply with the FAR
- All practices from NIST SP 800-171 r1
- Additional 20 practices to support good cyber hygiene

## LEVEL 4 PROACTIVE

### 156 Practices

- Comply with the FAR
- All practices from NIST SP 800-171 r1
- Select subset of 11 practices from Draft NIST SP 800-171B
- Additional 15 practices to demonstrate a proactive cybersecurity program

## LEVEL 5 ADVANCED / PROGRESSIVE

### 171 Practices

- Comply with the FAR
- All practices from NIST SP 800-171 r1
- Select subset of 4 practices from Draft NIST SP 800-171B
- Additional 11 practices to demonstrate an advanced cybersecurity program

## CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) LEVELS

# Cyber Risk Radar Objectives



- Leveraging commercial AI, open data sets, integrated SaaS & online platforms - automate end to end supply chain risk insights & mitigation
- Mapping to NIST SP 800.171/800-53, ISO 27001/27032, AIA NAS9933 & CIS controls, in compliance with DFARS 252.204-7012 & JAN20 DoD CMMC.
- Providing actionable, sourced, prioritized & mitigated risks in an integrated dashboard
- Delivering scalable cyber risk scorecards, action plans & near real time risk mitigation
- Showcase across DOD, IC, & DHS

*Mature discussions underway with USCC CISO, NSA DoDCAR, DIA SCRM-Tech, DHS CISA/.govCAR, DON NIA*

# Vendor Risk Management Playbook

Manage the complete VRM life cycle with CyberOne Security Platform



Your Company

[Search](#)

Home **Vendors** Engagements Contacts Assessment Templates Assessments Assessment Targets Assessment Answers Findings Risk Metrics Metric Results Vendor Document Request Plans

Create New...



All

[Clone](#) | [Create New View](#)

Recent Items

- [Box Inc](#)
- [WHK-00000022](#)
- [Blue Assistance SpA](#)
- [WHK-00000025](#)
- [Canon Italia Group](#)
- [Sheraton Systems Limited](#)
- [Salesforce.com](#)
- [Nvidia Corp](#)
- [Forrest Allen-Zurch](#)
- [ABC Transparency GmbH](#)

Recycle Bin

[New Vendor](#) [Change Owner](#) [Delete Selected](#)

	Action	Vendor Name ↑	Status	Risk Rating	BitSight Security Risk Score	Whitehawk Security Rating	Interos Business Risk ...	Compliance Status
<input type="checkbox"/>	<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">ABC Transparency G...</a>	New	Not Rated	780	780	0	No
<input type="checkbox"/>	<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Blue Assistance SpA</a>	New	Not Rated	760	760	0	No
<input type="checkbox"/>	<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Box Inc</a>	New	Not Rated	750	750	252	No
<input type="checkbox"/>	<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Canon Italia Group</a>	New	Not Rated	690	680	0	No
<input type="checkbox"/>	<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Dell Technologies</a>	New	Not Rated		0	240	No
<input type="checkbox"/>	<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Metis Solutions, S.L.</a>	New	Not Rated	770	780	0	No
<input type="checkbox"/>	<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">MetricStream</a>	New	Not Rated	650	630	0	No
<input type="checkbox"/>	<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Nvidia Corp</a>	New	Not Rated		0	280	No
<input type="checkbox"/>	<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Oracle Corporation</a>	New	Not Rated		0	220	No
<input type="checkbox"/>	<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Salesforce.com</a>	New	Not Rated		0	240	No
<input type="checkbox"/>	<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Sheraton Systems Limit...</a>	New	Not Rated	760	760	0	No
<input type="checkbox"/>	<a href="#">Edit</a>   <a href="#">Del</a>	<a href="#">Splunk</a>	New	Not Rated	640	630	0	No

# WhiteHawk Cyber Risk Program

*Enabling mid & large enterprises to efficiently & effectively defend themselves against cyberattacks by continuously monitoring, prioritizing, validating & mitigating cyber risks via continuous monitoring of your network, the www & dark net activity, with executive level reporting & prioritized action plans*

## Outside-In Cyber Risk View & Findings



Continuous Cyber Risk Monitoring & Prioritization



Executive Cyber Risk Scorecards & Reporting



Real-Time Red Team Cyber Risk Validation



Dark Net Risk Validation & Assessment

*Validate Cyber Risks Continuously*

# Cyber Risk Portfolio Report

*Across Business Groups, a Region or Sector of Clients*

## View Executive Level Risk Trend Reporting:

- Gather & analyze cyber risk data & analytic outputs for each entity in the portfolio
- Perform data collection, assessment, & analytics using externally available open data

## Cyber Risk Portfolio Reporting contains:

- Analytic summary across the entire portfolio
- Overview of key findings for prioritization & action
- Individual Scorecard of each Business Unit or Vendor: security rating scores & top risk vectors
- Historical context for Risk Rating scores for all companies or organizations in the portfolio
- Analyst Notes that summarize all the above to an executive & practitioner audience



# SME PRODUCT LINES/REVENUE STREAMS

## Sontiq/WhiteHawk Business Suite

- Annual SaaS Subscription
- Priced by Business Model & number of employees covered (Embed, Wholesale, Retail)
- Pricing from \$100 to \$1,100
- Sales Channels via MSSP's & Banks as a security service for SME Clients
- [Sontiq/WH Business Suite Demo Video](#)

## Cyber Risk Scorecard

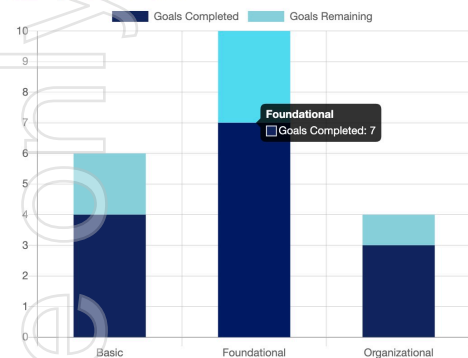
- Quarterly or Annual SaaS Subscription
- Pricing based on volume from \$500 to \$2,500, 50%+ margins
- Sales Channels as a feature of all Product Lines or via the Cybersecurity Exchange Customer Journey
- [WhiteHawk Cyber Risk Scorecard](#)

*10% to 20% Margins on All Cybersecurity Products & Services Sold via the WhiteHawk Marketplace*

# Cyber Risk Questionnaire & Maturity Model

AI-based WhiteHawk proprietary Decision Engine that provides tailored Product & Services Options through a Non-Invasive Cyber Risk Readiness Questionnaire

Maturity Level Assessment

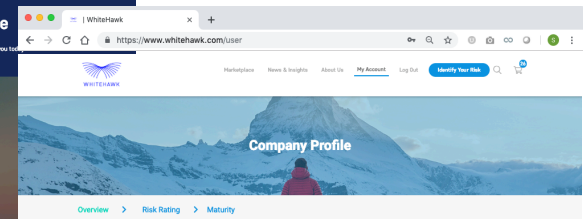
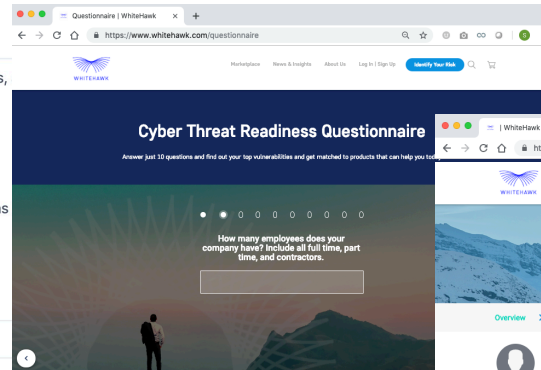


Basic Foundational Organizational

- ☒ Limitation and Control of Network Ports, Protocols, Controlled Access Based on the Need to Know
- ☒ Account Monitoring and Control
- ☒ Data Protection
- ☒ Malware Defenses
- ☒ Email and Web Browser Protections
- ☒ Secure Configuration for Network Devices, such as Routers and Switches
- ☒ Boundary Defense
- ☒ Wireless Access Control
- ☒ Data Recovery Capabilities

Todo Item

Add Cancel



WhiteHawk  
Industry 4.0 • Employees 13 • Locations 31  
Interaction Managed By A Third-Party Provider, Website, Email, Mobile, Face-to-Face

Based on the answers provided, your focus should be on protecting your company's computers and users during a wide range of transactions involving many different customers and suppliers. Your business may attract sophisticated groups of attackers, Advanced Persistent Threats or "APT", who are willing to invest a lot of time and effort in the hopes of a single large payout. The payout does not have to be financial: cyber criminals may also be targeting your intellectual property. In addition, attackers may see you as a useful stepping stone in attacking your business partners.

Your company tends toward light, informal internal rules. Because of this, you should make sure that you have appropriate plans in place to deal with cybersecurity breaches. It is important to know and understand your risks in order to take appropriate steps to mitigate them. You should set up employee training and controls on your corporate network to ensure employees are equipped with the knowledge to identify and report potential scams. In addition, developing an incident response plan will help your company respond and recover if and when it is attacked and will help to protect your reputation.

Our evaluation indicates that your current overall cybersecurity posture is poor. Your company needs to take immediate steps to close the most urgent gaps in your cybersecurity.

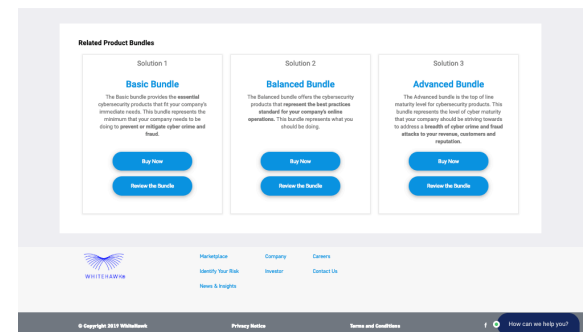
This profile is based on the email amount of business specific data you have provided through the questionnaire, and on broad statistics for your industry. Please contact WhiteHawk to get a more accurate, personalized evaluation.



Answer 10 non-intrusive, non-technical questions to access:

- Company risk profile
- Tailored sets of risk mitigation solutions
- Risk comparison to similar companies
- A virtual conversation with a WhiteHawk Cyber Analyst
- Interactive cyber maturity model

[View our online Customer Demo](#)



# WhiteHawk Reporting & Deliverables

## 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 Address		
Sample Company Technology Corp.		www.Sample Company.com		513		
Security Rating			Risk Vector Performance			
Ratings measure a company's relative security effectiveness.			Risk Vector grades show how well the company is managing each risk vector.			
690	Advanced:	900 – 740	Compromised Systems:	B	Systems Patching:	C
	Intermediate:	740 – 640	Communications Encryption:	D	Application Security:	C
	Basic:	640 – 250	User Behavior:	A	Email Security:	B
					Public Disclosure:	A
Prioritized Areas of Focus						
WhiteHawk Cyber Analyst recommendations for top-3 Focus Areas the company should consider						
Recommended Focus Area 1:		Communications Encryption				
Recommended Focus Area 2:		Systems Patching				
Recommended Focus Area 3:		Application Security				
Solution Options						
Solution options that address primary business risks identified in the Cyber Risk Scorecard						
Basic Bundle		Balanced Bundle		Advanced Bundle		
– Symantec: Endpoint Protection – KnowBe4: 1 Year - Security Awareness Training		– Micro Focus Software Inc.: ZENworks Patch Management – StorageCraft: ShadowProtect IT Edition V5.x Subscription - 1 Year – Symantec: Desktop Email Encryption		– Micro Focus Software Inc.: Log and Event Management – Check Point: Threat Prevention Security Suite – Trend Micro: TippingPoint – D3 Security: D3 SOAR		

# Sontiq/EZShield Business Suite | Main Dashboard

[Sontiq Small Business Suite Demo Video](#)



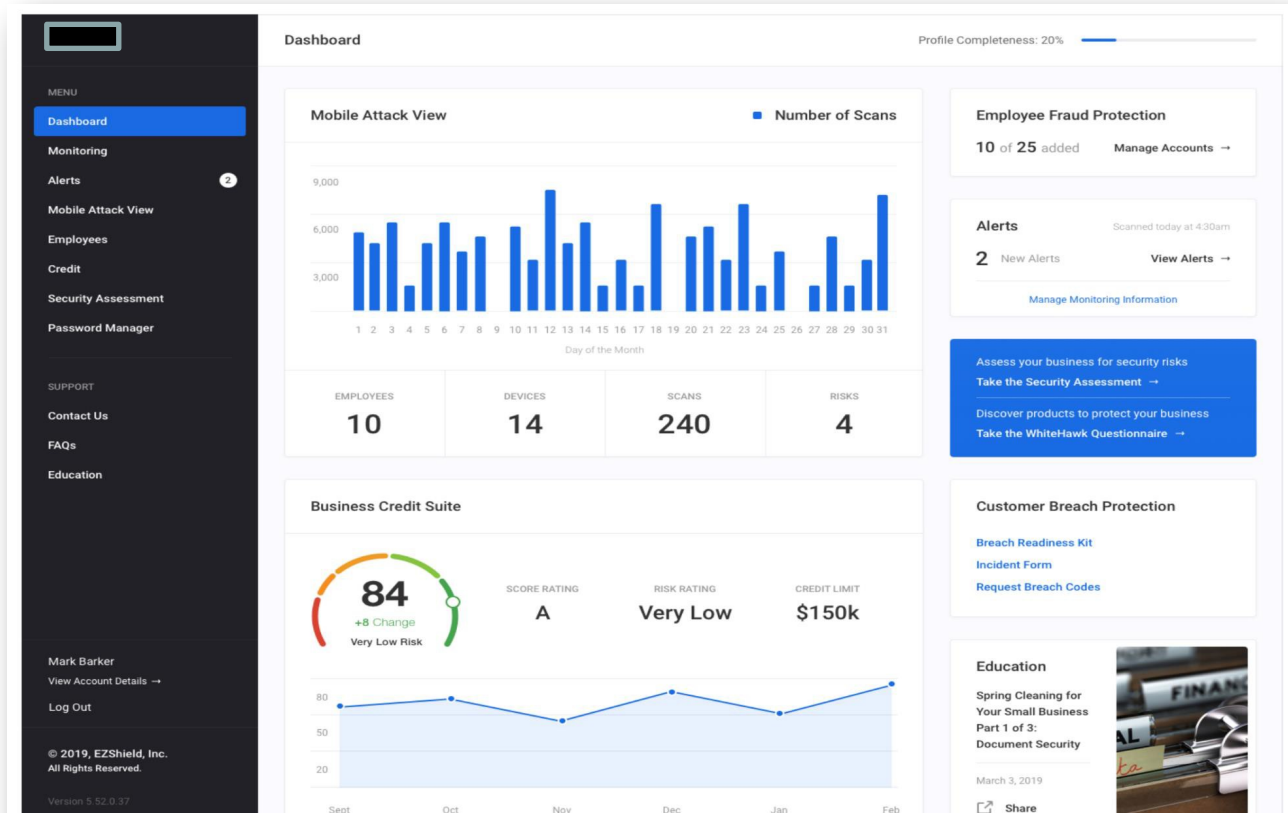
SECURE



MONITOR



RESTORE



# Business Suite Features:

*Starting at \$480 for an Annual Subscription*

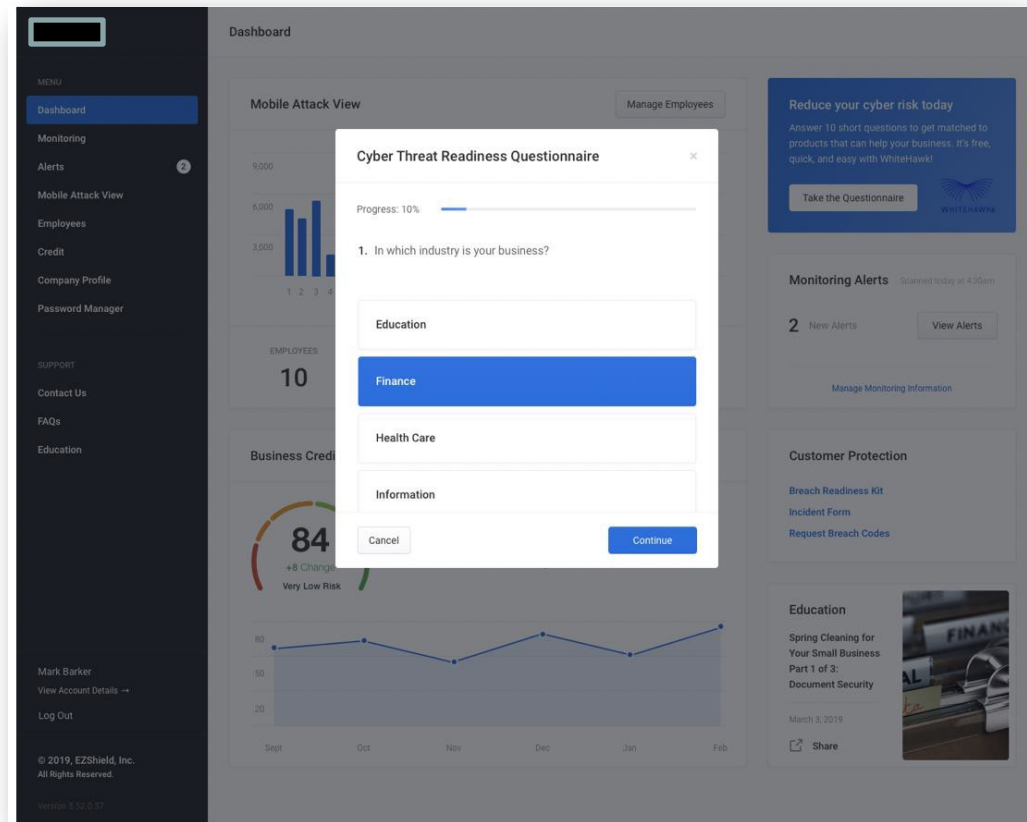
Business Protection	Secure	Plus	Premium
Business Restoration	✓	✓	✓
Business Dark Web Monitoring	✓	✓	✓
Business Credit Monitoring	✓	✓	✓
Mobile Attack View	✓	✓	✓
Continuous Security Risk Monitoring	✓	✓	✓
Annual WhiteHawk Cyber Risk Scorecard	✓	✓	✓
Employee Protection			
Fully Managed Restoration	✓	✓	✓
Dark Web Monitoring	✓	✓	✓
\$25K Insurance	✓		
\$1M Insurance		✓	✓
Mobile Attack Control	✓	✓	✓
1 Bureau Credit Monitoring		✓	✓
1 Bureau Score			✓
Financial Account Monitoring			✓

# Business Suite | The WhiteHawk Cyber Risk Questionnaire

Exclusive to EZShield's Business Suite is a Cyber Risk Profile, powered by WhiteHawk

**WhiteHawk's Cyber Risk Profile empowers SMB's to:**

- Pinpoint & understand risks
- Develop a customized cybersecurity action plan
- Identify the tools required to safeguard the business

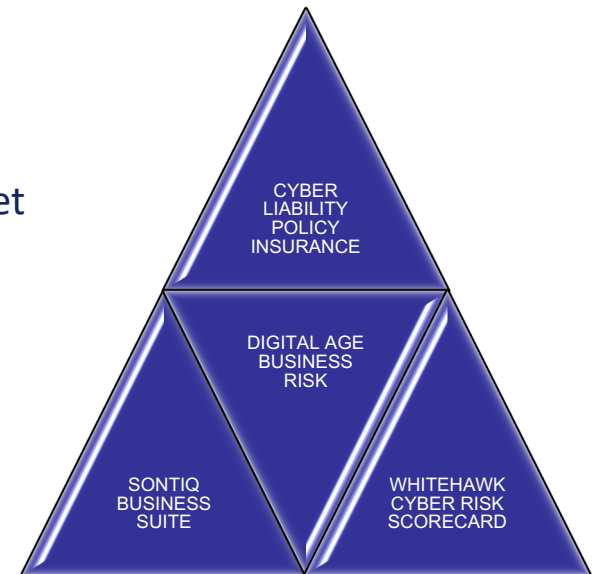


# Business Client Digital Age Resilience: Path to Discounted Cyber Liability Insurance

- 1) Complete the WhiteHawk virtual cyber risk consult
- 2) Receive your Cyber Risk Scorecard
- 3) Become eligible for discounted comprehensive Cyber Liability Insurance
- 4) Provide Cyber Risk Scorecard to Insurance Partner and get your tailored quote

Via Clarke & Sampson

Clarke and Sampson Cyber Liability Quote Request



# Sontiq Sphere: Dynamic Loading of Clients

## Sontiq Sphere Partner options:

- ✓ Up-load tens of thousands of clients within weeks seamlessly
- ✓ Access clients in large quantities through a simple upload template

A screenshot of the Sontiq Sphere Client Management interface. The background shows a 'Client Manage' section with a 'Filter by Group' dropdown set to 'All (2)', a 'Results: 1 Clients' summary, and a table with one client named 'Amazon'. Overlaid on this is a modal window titled 'Upload Client'. The modal contains three steps: 1. 'Download and Complete the Client Upload Template' with a download icon and a link for more information. 2. 'Select Organization (Required)' with a dropdown showing 'Solarwinds Pilot Msp1' and a 'Package Code(s): 3 found' status with an 'Expand Package Code List' button. Below this is an 'MSP Code: 26-3798676\_MSP1'. 3. 'Upload Your File' with a file input field and a 'Choose File' button. At the bottom of the modal are 'Cancel' and 'Submit' buttons.

# The Team

**Terry Roberts, CEO, President & Founder**

Cyber Executive across government, academia & industry. Previously Deputy Director of US Naval Intelligence, TASC VP for Intelligence & Cyber, an Executive Director of Carnegie Mellon Software Engineering Institute. Currently US National Security Cyber Thought Leader, Board Member & Chair Emeritus, Intelligence & National Security Alliance Cyber Council. US Fed Top 50 Women & MSSI in Strategic & Artificial Intelligence.

<https://www.linkedin.com/in/terry-roberts-193493143/>

**Soo Kim, Chief Product Officer**

Previously the cybersecurity, technology strategy expert at Accenture Federal Services, Hewlett Packard Federal & VP at TASC. Experience in technical & business leadership, tactical execution, business operation, & solutions delivery. Bachelor's degree in mathematics from Virginia Tech, a Certified Enterprise Architect & Scrum Master.

<https://www.linkedin.com/in/soo-kim-23655786/>

**Kevin Goodale, CFO**

CFO at Impressions Marketing Group Inc. from 2005 – 2016.

Career Commercial Financial & Contracting Manager with over 20 years at the CFO level, using degrees in accounting & management information science to reduce risk & increase profits.

<https://www.linkedin.com/in/kevin-goodale-6ba4383b/>

# The Board

## **Terry Roberts, Executive Chair**



## **Louise McElvogue, Non-Executive Director**

Currently company director & advisor with strategy, commercial, & digital expertise in North America, Europe, & Asia Pacific.

Global Experience of media, digital transformation, & start-ups.

Governance & strategic experience.

Expert in media, journalism, & marketing.



## **Tiffany O. Jones, Non-Executive Director**

Previously SVP at Imperva, CEO Of Distill Networks, VP of Global Strategic Partnerships & Alliance Operations at FireEye and SVP of Client Solutions & Chief Revenue Officer for iSIGHT & Mandiant.

Former Deputy Chief of Staff at the White House Office of Cyber Security & Critical Infrastructure Protection. Decorated US Coast Guard Officer.



## **Phil George, Non-Executive Director**

Specialist in Information Security & Risk Management

Currently operates Nurv Cloud, a cloud telecom company, specializing in high quality, secure voice solutions.

Launched Uber Perth in Australia in 2014 as Operations Manager

Former Non-Executive Director of Department 13 International Limited (ASX:D13)

## WhiteHawk Cybersecurity Exchange

- Stop being overwhelmed by cybercrime, fraud, & disruption
- Have clarity of understanding & insight
- Take constructive & measured action
- Prevent, detect, or respond effectively to cyber disruption or attack focused on your company, people or partners

[Contact Us](#)