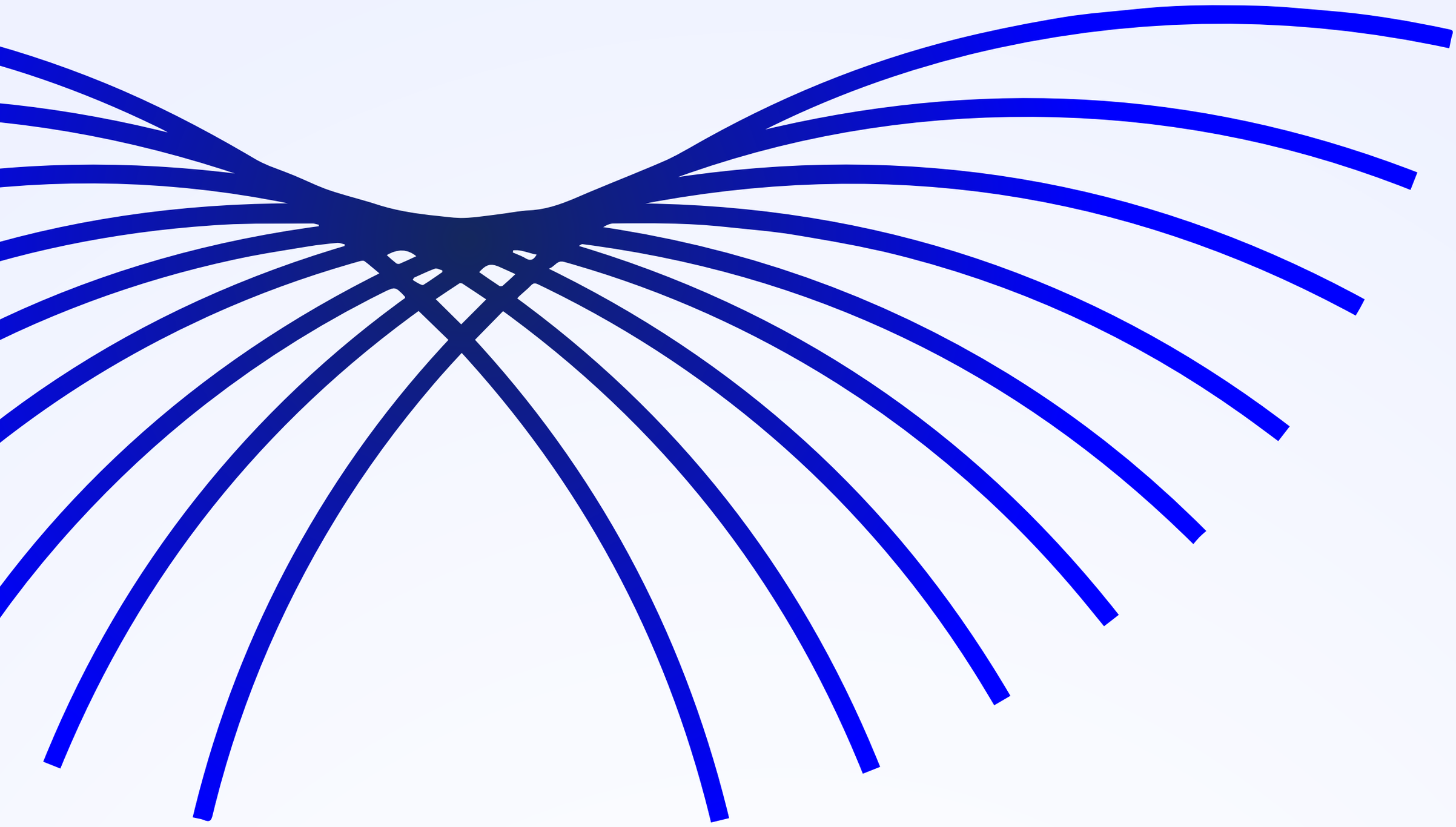
EMPOWERING A FEARLESS INTERNET



WHITEHAWK®

Cyber Risk Radar

For Enterprise Supplier Risk & Compliance Management

Automate your supply chain risk monitoring and mitigation of threats

www.whitehawk.com

Executive Overview

Our economic and political adversaries seek access to information systems most vulnerable, often leveraging discrete intersections to their advantage, gaining and holding root-level access in critical business and government systems.

As a result, there is a risk imperative to have continuous insight across your suppliers' and vendors' cyber and associated business risks to prioritize and address them in real-time, with limited resources. This paper discusses the Cyber Risk Radar process to assess, identify, monitor, prioritize, and mitigate business and cyber risks for organizations and their supply chains.

- The WhiteHawk Cyber Risk Radar provides near real-time continuous monitoring, prioritization, and mitigation support of the cyber risks of an enterprise's teammates, vendors, and suppliers over time.
- The Cyber Risk Radar enables the establishment of a scalable strategy to automating risk identification and accelerating adherence to compliance requirements.
- It is an annual Software as a Service (SaaS) subscription consisting of quarterly services that include Cyber Risk Scorecards, Cyber Risk Portfolio Reports, and online Cyber Analyst consultations.

External Security Assessment

Real time assessments that measure each supply chain company's security performance and vulnerabilities.

Company Scorecard

The scorecard rates each supply chain company's vulnerabilities, active exploits and advance threats to know where to focus their attention and strengthen their security posture.

The Cyber Risk Radar enables companies to efficiently and effectively defend themselves against cyber attacks by

MONITORING, IDENTIFYING, PRIORITZING & MITIGATING

threats caused by third-party vendor networks.

Risk Prioritization

A roadmap that lists risks in order of severity, telling you which vendors in your supply chain need mitigation efforts first.

Continuous Monitoring

Immediate and ongoing monitoring in real time to map and identify risks across the entire supply chain.

WhiteHawk continues to work in each industry sector and implement Cyber Risk Radars to help organizations with their multi-faceted business (Finance, Operations, Governance, Geographic, and IT) and cyber risks. We focus on core areas leveraging cutting edge technology solutions to provide transparency and understanding across a complex and ever-evolving risk environment.

Key Features

How can companies and organizations optimally combine deep tradecraft, all publicly available data, and AI analytics?

Risk programs can now fully leverage all organizational-focused subscriptions (D&B, Gartner, Bloomberg, etc.), world wide web open data sets, AI-driven risk identification, risk tradecraft, and best practice analytics in order to perform thorough risk and compliance risk analysis.

WhiteHawk's Risk and Compliance Services Maximizes Data Discovery and Visualization

1

Portfolio Assessments

Understand an organization's portfolio of all suppliers and vendors.

2

Risk Research and Discovery

Collect, analyze, and correlate openly available data into actionable intelligence.

3

Continuous Risk Monitoring and Alerts

Understand an organization's security performance and be alerted to impactful changes.

4

Focused Analytics

Perform deep dives in the areas that need focus rather than into the entire dataset.

5

Ecosystem Maps

Visualize the enterprise by understanding the supplier and vendor interconnections.

6

Risk Prioritization and Mitigation

Prioritize risk mitigation and business actions based on CMMC levels for impact and performance.

7

One Risk Management Dashboard

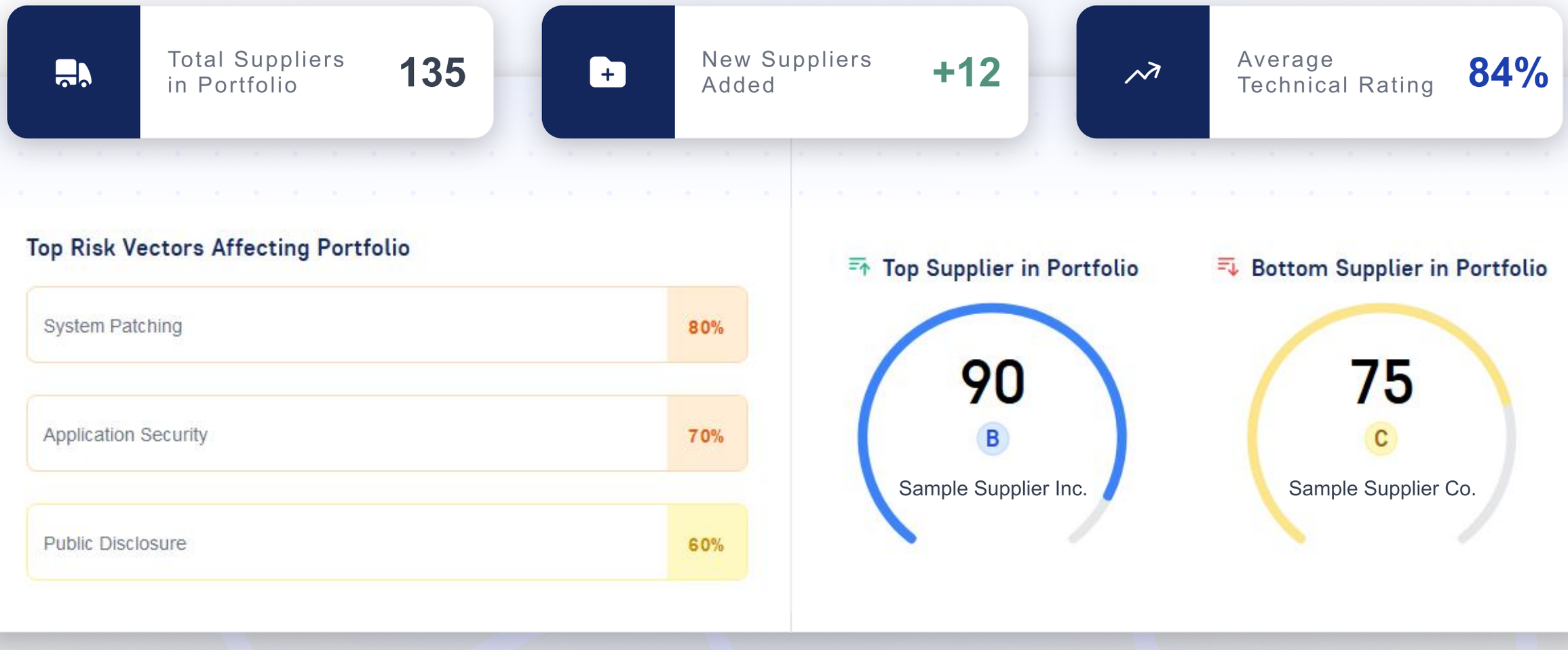
Continuous situational awareness, tracking, mitigation, and management of the Supply Chain Risk Management (SCRM)/Vendor Relationship Management (VRM) program.

Cyber Risk Portfolio Report

The Cyber Risk Portfolio Report provides an aggregated view across multiple suppliers revealing current vulnerability trends and changes over time.

View Executive Level Trend Reports

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



What's included?

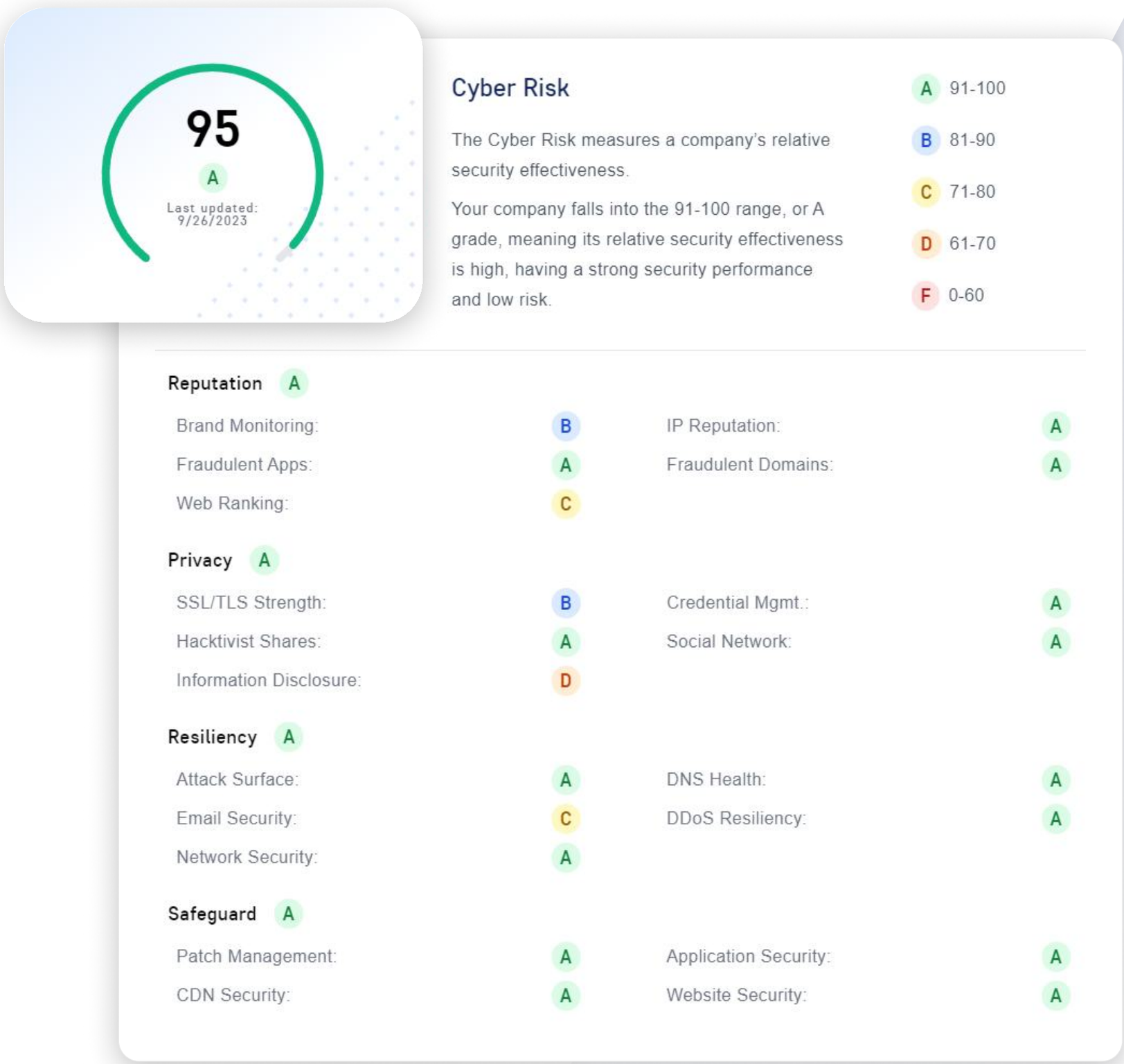
- Analytic summary across the entire supplier portfolio
- Summary of top-findings for prioritization and action
- Report of all suppliers' security rating scores and top risk vectors
- Historical context for risk rating scores for all companies in the portfolio
- Analyst notes that summarizes all of the above

Cyber Risk Scorecard

WhiteHawk's Cyber Risk Scorecard provides businesses and organizations a topline cyber risk report and summary of a organization's effectiveness at addressing the impacts of online crime, fraud and disruption. We start with cyber risk continuous monitoring across 20-30 cyber risk controls. Our cyber global threat trend analytics and deep dives across hundreds of companies provide powerful trend context. This augments the risk indicators, enabling organizations to take smart action to mitigate cyber risks to their revenue, reputation, and operations.

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

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



WhiteHawk Cyber Analysts perform customized analytics in order to:

- Deliver affordable and impactful options to mitigate cyber risks that are 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 datadriven decision making in terms of business risk and budget constraints
- Maintain informed and enable engagement

Achieving CMMC Levels

The WhiteHawk Cyber Risk Radar enables an accelerated path to the Cybersecurity Management Model Certification (CMMC 2.0) levels for companies and organizations of all sizes.

Through WhiteHawk's interactive Supplier Portal—which maps to CMMC 2.0 Levels and offers Risk and Compliance Monitoring along with Virtual Cyber Consults—the Cyber Risk Radar Subscription enables organizations to track their progress and achieve any required CMMC 2.0 Level before seeking certification.

1 FOUNDATIONAL

Essential Practices for Federal Contract Information (FCI) Protection

Establishing Basic Cyber Hygiene

- 17 practices from NIST SP 800-171
- Basic access control implementation
- Limited asset management
- Fundamental physical protection
- Basic incident response planning
- Annual self-assessment required
- Simple password requirements
- Basic security awareness training
- Rudimentary system and data backups
- Minimal media protection measures

2 ADVANCED

Broad Security for Controlled Unclassified Information (CUI) Handling

Elevating Security Measures

- 110 practices from NIST SP 800-171
- Multi-factor authentication
- Regular vulnerability assessments
- Security awareness program
- Controlled maintenance procedures
- Rigorous configuration management
- Third-party assessment required
- Comprehensive access control policies
- Incident response testing and drills
- Monitoring of system security alerts
- Encryption of CUI at rest and transit
- Advanced audit log reviews

3 EXPERT

Sophisticated Defense against Advanced Persistent Threats (APTs)

Mastering Proactive Defense

- 110+ practices beyond NIST SP 800-171
- 24/7 Security Operations Center (SOC)
- Continuous monitoring solutions
- Software bill of materials (SBOM)
- AI-driven threat intelligence
- Advanced data loss prevention (DLP)
- Government-led assessments
- Advanced persistent threat (APT) hunting
- Robust identity and access management
- Zero trust architecture implementation
- Comprehensive supply chain risk management
- Cyber threat emulation exercises

Capabilities Statement

WhiteHawk's mission is to automate and scale Cyber Compliance, Maturity and Resilience for Enterprises, Supply Chains and Critical Infrastructure Sectors, by fully leveraging publicly available data sets and AI risk/threat analytics.

Core Competencies

- **ENTERPRISE SOLUTIONS** Automated Enterprise Cyber Risk SaaS and PaaS Subscriptions
- **SMB SOLUTIONS** Cost effective Cyber Risk Profile, CMMC, Virtual Consult and Scorecard
- **VIRTUAL CONSULTING** CMMC Registered Practitioner & Commercial WhiteHawk Cyber Analysts
- **TECH LEADERSHIP** Vetting of Innovation and Solution Providers
- **PRODUCT LINES** Cyber Risk PaaS, Cyber Risk Program, Cyber Risk Radar, Cyber Risk Scorecard
- **AWS PARTNERSHIP NETWORK** Cyber Risk Scorecards and Services via the AWS Marketplace
- **DUN & BRADSTREET PARTNERSHIP** Dun & Bradstreet Cyber Compliance Powered by WhiteHawk

Key Past Performance

- DOE CIO; ODNI CIO
- DHS CISA
- Federal, State & Local CIO's & CISO's
- Top U.S. Financial Institutions; Top Tier Defense Industrial Base Company
- Global Consulting Groups; Top Tier Global Manufacturers

SMB Clients

- Government Contractors and Suppliers
- Professional Firms (small-to-mid)
- Financial & Insurance Firms Business Clients
- Family Offices

Enterprise Clients

- Federal Contractors and Consulting Firms
- Government Departments and Agencies
- Financial Institutions
- ISPs, MSPs, and MSSPs
- Insurance Groups
- Professional Firms

Influencers

- Sector Professional and Non-Profit Associations
- Client Focused Risk Executives
- Government, Industry, Academia, Cyber, Risk, and Procurement/Supply Chain Executives and Managers
- Risk Professionals: CSO's, CRO's, CISOs
- Sector Social Media: LinkedIn, Facebook

Differentiators

- Online, automated, scalable, and effective cyber risk monitoring and mitigation one-time or continuous service
- Continuous Advancement of SaaS/PaaS Product Lines, with in-house development and data science team
- Continuous access to and integration with Innovative Technologies and Services, via weekly vetting of new solutions
- PaaS and SaaS subscriptions that are globally accessible, impactful and cost-effective solutions, tailorable to organizations and businesses of all sizes
- Virtual Cyber Risk Consults, Automated Assessments and Action Plans, enabling Clients to take smart action immediately
- Make Cyber Resilience Easy and Affordable

The Leadership Team

CHIEF EXECUTIVE OFFICER, PRESIDENT & FOUNDER

Terry Roberts

A global risk analytics, cyber intelligence and national security professional with over 20 years of Executive level experience across government, industry, and academia. Previously the Deputy Director of US Naval Intelligence, TASC VP for Intelligence and Cyber Engineering, and an Executive Director of Carnegie Mellon Software Engineering Institute (established the Emerging Tech Center now the AI Division) with an MSSI w/ AI concentration.

CHIEF OPERATING OFFICER

Soo Kim

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

CHIEF INFORMATION OFFICER

Mike Ferris

With nearly twenty years of experience in IT and cybersecurity,Mike has held pivotal roles at WhiteHawk, including Director of IT Operations & Security, Director of Advisory Services, and Senior Cyber Analyst & Program Manager. Mike began his career in the United States Marine Corps as a Technical Controller, responsible for the installation, maintenance, and repair of complex communication systems, ensuring secure and reliable communication channels transitioning to the private sector in 2010.

CHIEF TECHNOLOGY OFFICER

Michael Good

A Technical Program Manager with over 30 years of experience in cyber operations and technology development for military, government, and commercial cybersecurity solutions. Previous assignments include Raytheon, Vencore, L3 Communications and the US Census Bureau. Before entering private industry, Michael was a US Army Ops Research and Cyber Warfare officer at US Cyber Command, leading cyber operations planning for NSA’s IA Directorate, with an MS in Computer Network Operations.