Cyberint

Impactful Intelligence

CYBERINT ARGOS PLATFORM

# SUPPLY CHAIN INTELLIGENCE DATASHEET

Reduce risk generated by third-party technologies and vendors through continuous vendor detection, monitoring and cyber risk assessment. Go beyond basic external security scans with extensive deep and dark web intelligence that provides a comprehensive evaluation of an organization's cyber risk. Stay secure with targeted alerts that notify you when a trusted third-party organization falls victim to an attack.

## Challenge

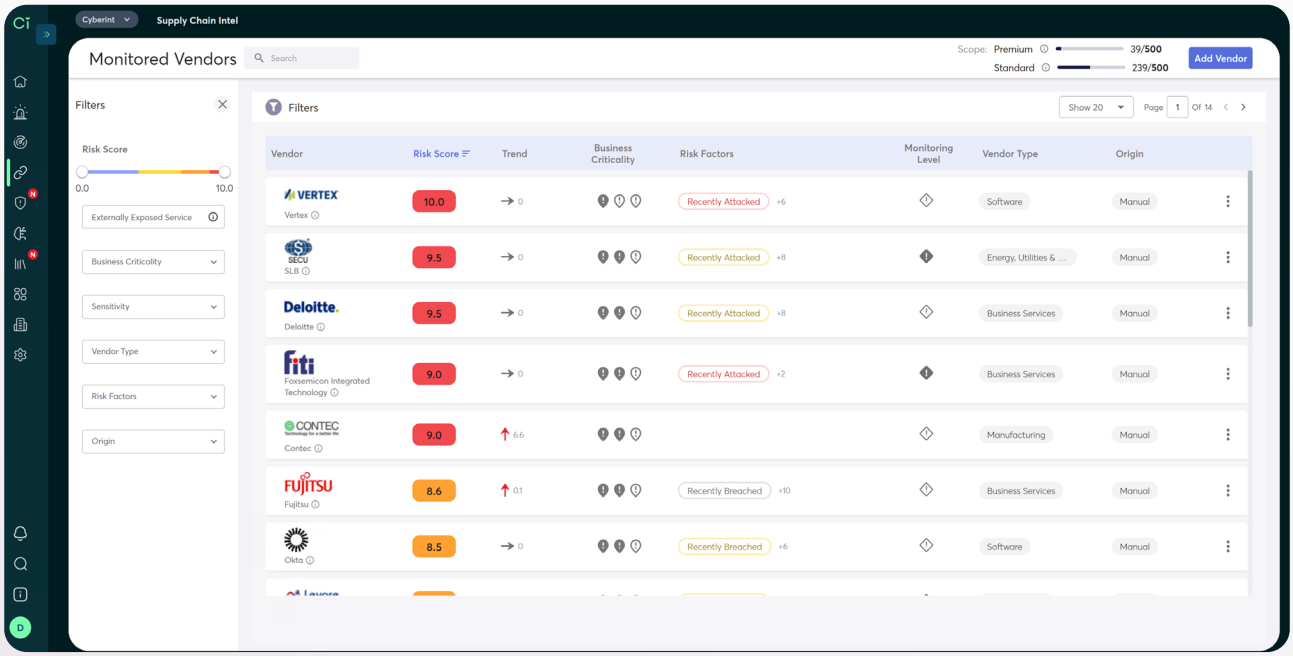
Many teams throughout an enterprise can choose to use a new SaaS app or work with a new vendor. Security leaders don't always get to approve these decisions, but they are ultimately responsible for the cyber risks that these third-party relationships introduce. Legacy techniques for managing third-party risk typically rely on periodic assessments so they lack continuous visibility and fail to detect new risks in real-time, such as 3rd party data breaches.

## Solution

Cyberint's Supply Chain Intelligence module automatically discovers the 3rd party technologies and vendors in your digital supply chain, continuously monitors these third-parties, and assigns risk scores that leverage Cyberint's extensive open, deep and dark web intelligence. The module issues targeted alerts in real-time about the threats that may negatively affect your organization.

## Key Benefits:

- Identify the 3rd party technologies running on your external assets as well as the vendors that produce them
- Create an up-to-date inventory of all the vendors, partners, and providers in your digital supply chain
- Continuously monitor third-party technologies and organizations for relevant risks
- Gain real-time deep and dark web intelligence on trusted third-party organizations
- Receive alerts when a major security incident occurs at one of the organizations in your vendor watchlist



## Gain Visibility On Your Digital Supply Chain

Cyberint's discovery engine fingerprints the technologies running on your Internet-facing digital assets, identifies the vendors that produce those technologies, and suggests those vendors for monitoring.

### Inventory Third-Party Technologies

Create a complete, up-to-date inventory of the third-party technologies you use with automated discovery techniques.

### Understand Your Vendors & Suppliers

Gain visibility on all the third-party vendors and suppliers that your organization relies on.

### Customize The 3rd Parties You Monitor

Customize the list of third parties you monitor by adding organizations not scoped in through automated discovery.

## Continuously Monitor & Comprehensively Assess 3rd Party Risk

Cyberint continuously assesses the risk of the vendors and suppliers that you choose to monitor, taking into account security hygiene, exposures, deep and dark web threats, and breach history.

### Security Posture Evaluation

Use comprehensive external attack surface evaluations to understand the security posture of your vendors.

### Deep & Dark Web Intelligence

Assess third-party deep and dark web risks, such as malware infections, exposed credentials, and data leaks.

### Targeting Level & Breach History

Understand how highly targeted a 3rd party organization is by threat actors as well as that organization's cyber track record.

## Receive Real-Time Alerts About Relevant Risks

Cyberint provides real-time alerts when one of your monitored third-parties experiences a major drop in cyber risk score, falls victim to a cyber attack, or suffers a major data breach.

### Complete Security Awareness

Know when a trusted third-party experiences a security incident, such as a ransomware attack or data breach.

### Informed Risk Management

Understand 3rd party risks so you can accurately report to stakeholders and make informed risk management decisions.

### Pull Alerts Into Your SOC

Bring alerts regarding supply chain risks into existing workflows via integrations with SIEM, XDR, and SOAR platforms.

> “Because we’re a small team, the Cyberint analysts are like an extension of us, which really helps from a risk management standpoint.”
>
> Evans Duvall, Cyber Security Engineer, Terex
>
> Read more in the customer case study.

> “We realized that Cyberint was much more than an EASM solution, it delivered much value with highly relevant intelligence from the deep and dark web.”
>
> Benjamin Bachmann, Head of Group Information Security, Ströer
>
> Read more in the customer case study.

> “Once we identified the need to address the risk of fraudulent websites and social profiles, I quickly realized we needed to handle this in a scalable manner. Our solution is to use Cyberint to help us automatically detect and takedown these threats.”
>
> Ken Lee, IT Risk and Governance Manager at Webull Technologies
>
> Read more in the customer case study.

## Recognition As An Industry Leader From Trusted Analysts

Gartner FROST & SULLIVAN IDC

Discover Cyberint with a personalized demo

## About Cyberint

Cyberint, the Impactful Intelligence company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Cyberint Argos platform’s patented technology provides superior visibility through continuous discovery of the evolving attack surface, combined with the automated collection and analysis of vast quantities of intelligence from across the open, deep and dark web. A team of global military-grade cybersecurity experts work alongside customers to rapidly detect, investigate, and disrupt relevant threats – before they have the chance to develop into major incidents. Global customers, including Fortune 500 leaders across all major market verticals, rely on Cyberint to protect themselves from an array of external risks, including vulnerabilities, misconfigurations, phishing, impersonation attacks, malware infections, exposed credentials, data leaks, fraud, and 3rd party risks.

**For more information visit:** https://cyberint.com