


INFINITY EXTERNAL RISK MANAGEMENT

Supply Chain Intelligence Module

The Infinity External Risk Management solution’s Supply Chain Intelligence Module comprehensively evaluates the cybersecurity posture of your selected third-party vendors, partners, and suppliers. These cyber risk assessments go beyond typical vulnerability scans to incorporate open, deep and dark web threat intelligence and develop a more robust risk score for each organization. The SCI module then continuously monitors these third-party organizations for major cyber incidents and alerts you in real time if one is suffering an attack or breach.

The Infinity ERM Supply Chain Intelligence module comprises the following capabilities:

Module	Description	Entitlements
Infinity ERM Application fundamentals	Asset Discovery Engine	-
	Alerts Center	Included
	Number of regular users	2
	Number of Threat Hunting users seats	-
	Tenants (a distinct Infinity ERM environment allowing users to visualize intelligence alerts for one company, subsidiary, or brand separately)	1
	Out-of-the-box integrations	1
	Customer Success Manager cadence	Yearly
	Support SLA	Direct Premium
Global Threat Intelligence	Global cyber news and ransomware watch	Included
	Cyberint research threat intelligence reports	-
	Global Intelligence Knowledgebase (Threat Actors, Malware, CVE)	-
	IoC searches and browser extension	Included
Supply Chain Intelligence Module	Automatic detection of used vendors	Included
	Vendor risk monitoring	Included
	Proactive alerts on high identified risks	Included
	Number of monitored vendors technologies	5

Discovery of Digital Suppliers

Through the external attack surface discovery process, Cyberint, a Check Point company, detects the software, services, and technologies running on externally facing assets, which enables the platform to automatically determine which vendors produce those technologies. These vendors and digital suppliers are added into the Supply Chain Intelligence module as suggestions to simplify and accelerate the process of creating a vendor inventory.

Any vendors and 3rd party suppliers not identified through the automated discovery process can be manually added into scope for cyber risk monitoring.

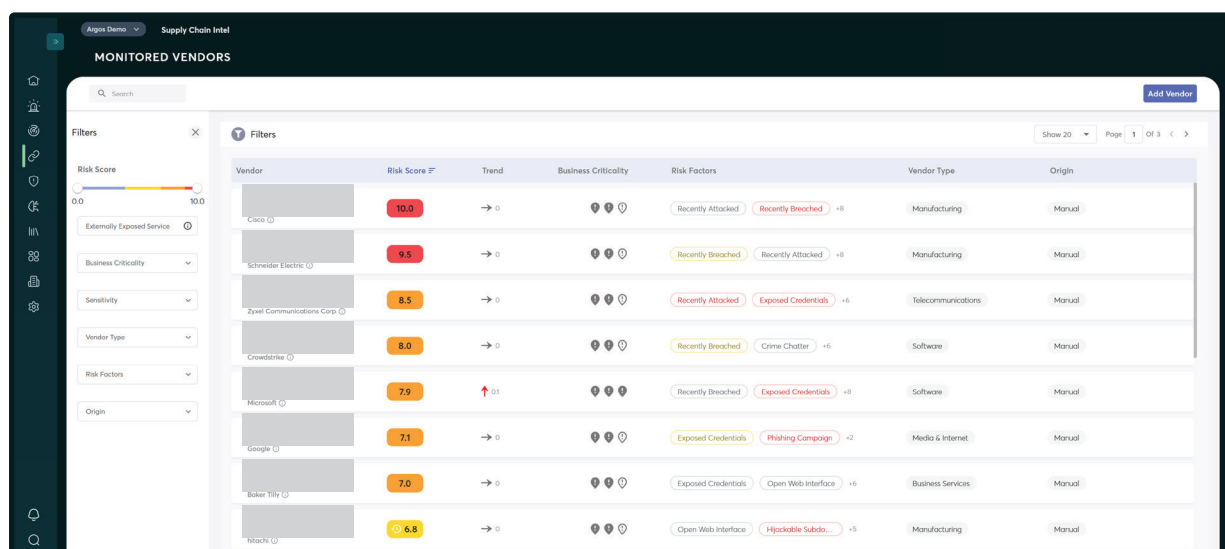


Figure 1 – Infinity ERM Supply Chain Intelligence page

Continuous Monitoring

Cyberint monitors the vendors, partners, and suppliers that have been added into scope for cyber risks along 4 different dimensions: Exposures, Hygiene, Targeted Level, and Breach History.

Exposures

This score indicates the number of external risks and attack vectors that the 3rd party is exposed to, including open ports, malware infections, leaked credentials, and more.

Hygiene

The Hygiene metric estimates the 3rd party's security hygiene and posture, based on the version of software running on externally-facing assets, the presence of CVEs, the versions of protocols like TLS, issues related to SSL certificates, and so on.

Targeted Level

The Targeted Level score uses deep and dark web threat intelligence to check for mentions of the 3rd party's brands, products, domains, and assets in threat actor forums or underground marketplaces. This is a measure of how targeted the 3rd party is by bad actors.

Breach History

The Breach History metric uses historical data, from public media reports to proprietary threat intelligence collected by Cyberint over the past decade. The vendor is assigned a risk score based on their cybersecurity track record.

The Supply Chain Intelligence module's Vendor Monitoring is continuous and ongoing so major security events, such as ransomware attacks and data breaches, are detected in real-time.

Alerting

For 3rd party vendors and suppliers that are in scope, Cyberint issues alerts in real time when major security events are detected. Examples include cyber attacks, ransomware incidents, and data breaches. When a major event like this occurs, Cyberint immediately issues an alert, which can then be shared via API with any integrated platforms, e.g. SIEM, SOAR, or XDR.

Licensing Details

These licensing instructions are related to the Infinity ERM packages: Essentials, Advanced, Complete, Elite.

Licensing Instructions

Supply Chain Intelligence Module

This licensing instructions are related to the Infinity ERM Supply Chain Intelligence Module.

The licensing is based on how many third-party organizations are monitored concurrently as selected using the add-ons.

Monthly licensing is not available.

The following table displays the number of External Assets and Threat Intelligence Assets that come at each pricing interval. Additional External Assets and/or Threat Intelligence Assets can be procured as an add-on, if needed.

ASM assets	200	500	1,000	2,000	5,000	10,000	25,000	50,000	100,000	200,000	350,000
TI assets	30	50	100	150	200	300	400	500	600	800	1,000

Worldwide Headquarters

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters

100 Oracle Parkway, Suite 800, Redwood City, CA 94065 | Tel: 1-800-429-4391

www.checkpoint.com