



INFINITY EXTERNAL RISK MANAGEMENT

## Essential Package

Infinity External Risk Management (ERM) is a unified solution that continuously detects and mitigates a broad range of external cyber threats. By combining deep and dark web monitoring, external attack surface management, brand protection, and supply chain intelligence into a single solution, Infinity ERM quickly identifies and mitigates cyber risks before they develop into costly security incidents.

The focus is on protecting your organization's digital estate – domains, IP addresses, websites, applications, social media channels, digital supply chain, and digital use of trademarks such as brand names and logos. The solution goes far beyond the networks' perimeters to identify relevant threats to your assets and mitigate them before they materialize.

As an agentless SaaS solution that continuously and proactively reduces cyber risk, Infinity ERM is deployed immediately without the need for new infrastructure or installation of new agents and begins providing value immediately.

Infinity ERM is dedicated to providing Impactful Intelligence, meaning the intelligence delivered is:

- **True:** a "true positive" threat that has been validated and poses a real risk.
- **Relevant:** the risk affects one or more of the customer's assets.
- **Actionable:** it is possible to mitigate the risk with certain actions.
- **Cost-effective:** the cost of remediation is lower than the cost of the risk.

Impactful intelligence enables organizations to efficiently manage external cyber threats with a minimal input of time. Ultimately, Infinity ERM is committed to providing value and ensuring a low total cost of ownership for customers.

The Infinity ERM Essential Package comprises following modules and capabilities.

Module	Subscription Topic	Essential
<b>Infinity ERM Application fundamentals</b>	Asset Discovery Engine	Included
	Alerts Center	Included
	Number of regular users	1
	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
<b>Attack Surface Management Module</b>	Vulnerabilities and exposure detection	Included
	Exposure items scan frequency	Weekly
	Technologies detection & watchlist	Included
	Risk Posture Monitoring	Included
	Managed assets review & scoping (Cyberint Analyst)	-
<b>Brand Protection Module</b>	Typosquatting & phishing & brand abuse sites detection	Included
	Social Media and mobile app impersonation for brand and VIPs	-
	Phishing beacons instances (# of subdomains) <ul style="list-style-type: none"> <li>• For phishing detection - Login interfaces recommended</li> <li>• A subdomain could be the root site (domain.com) or specific subdomain (sub.domain.com)</li> </ul>	-
	Manual Threat Hunting for impersonation (Cyberint Analyst)	-
<b>Deep and Dark Web Monitoring Module</b>	Credentials & Account Takeover monitoring & alerting	Included
	Open, deep and darkweb sources collection & search engine	-
	Data leakage & fraud detection using pre-supported use cases (for credit cards, emails, source code and more)	-
	Custom Threat Hunting rules	-
	Targeted intelligence manual threat hunting for data leakage, fraud and attackware (Cyberint Analyst)	-
<b>Global Threat Intelligence</b>	Global cyber news and ransomware watch	Included
	Cyberint research threat intelligence reports	Included
	Global Intelligence Knowledgebase (Threat Actors, Malware, CVE)	-
	IoC searches and browser extension	Included
<b>Remediation &amp; Investigations</b>	Remediation Credit Points ("Coins") for takedowns* and investigations	20

\*Subject to signing Check Point's letter of authorization (LOA)

## External Attack Surface Management

The Infinity ERM Attack Surface Management Module continuously discovers your organization's digital footprint, creating a complete asset inventory and providing visibility on your Internet-facing digital assets. The ASM module then identifies security vulnerabilities and exposures, assesses the risk of each one, and assigns risk scores to simplify prioritization and accelerate remediation.

## Brand Protection

Infinity ERM continuously monitors the web for illegal use of trademarked brand names and logos, as well as malicious impersonation of executives. This includes detection of lookalike domains, phishing sites, malicious applications on official or unofficial app stores, and more. It also includes fraudulent social media profiles that impersonate brands, products, or members of the executive leadership team.

## Deep & Dark Web Monitoring

The Infinity ERM Deep & Dark Web Monitoring module gathers intelligence from thousands of sources, including cybercriminal communities, threat actor forums, hidden chat groups, underground marketplaces, TOR onion sites, and more. After collecting massive quantities of threat intelligence, the module analyzes the data and correlates them with the customer's digital assets to detect relevant threats and risks.

## Global Threat Intelligence Knowledgebase

The Infinity ERM Threat Intelligence Knowledgebase provides a library of data on threat groups, malware, and documented CVEs. Customers can filter their threat landscape by industry and region, drill down on the attacks they are most likely to face, and access relevant data—such as common tactics, techniques, and procedures (TTPs) and indicators of compromise (IoCs)—enabling more proactive cyber defenses.

## Cyberint Coins for Takedowns & Investigations

Cyberint Coins can be used to initiate takedowns of illegal content, dark web investigations, custom threat reports, and more. Takedowns can be completed for malicious use of trademarked brand names and logos, fraudulent social media profiles, publication of proprietary data, and more. Investigations can be conducted on specific threat actors or groups, malware families, attack campaigns, and other relevant risks.

## Licensing Details

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

### Licensing Instructions

#### Essentials Package

The main licensing dimension is the number of external facing assets. These assets includes: Domains, Subdomains, IP, Cloud Assets. The approximate number can be detected using an external scan through the ERM platform or through information provided by the customer. It is possible to monitor only part of the external attack surface, meaning only a selected subset of the customer's external assets, but this is not recommended. Once the External Assets dimension is established, a predefined number of Threat Intelligence Assets (Brands, Keywords, VIPs, Login Interfaces and more) is automatically included. If desired, additional External Assets or additional Threat Intelligence Assets can be procured as an add-on to the license entitlements.

Users: Regular Users are granted access to most Infinity ERM modules. Threat Hunting Users receive access to additional modules: Forensic Canvas, Threat Knowledgebase (TTPs and IOCs of threat actors and malware), and the Threat Intel Data Lake. Threat Hunting Users are licensed separately.

Essentials and Advanced packages include the platform without managed services. Complete and Elite packages include manage services on top with different service levels and SLAs. Managed service packages are less flexible for discounts due to the labor costs.

All packages include remediation credit points ("Coins") which can be used for takedowns, darkweb credential purchases and analyst investigations on demand (4-8 coins per takedown, 8 coins per investigation hour, 6 coins for darkweb credential removal).

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.

<b>ASM assets</b>	200	500	1,000	2,000	5,000	10,000	25,000	50,000	100,000	200,000	350,000
<b>TI assets</b>	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](http://www.checkpoint.com)