CHECK POINT™

Infinity

INFINITY EXTERNAL RISK MANAGEMENT

Deep and Dark Web Monitoring Module

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.

The Infinity ERM Deep and Dark Web Monitoring module comprises the following capabilities:

Module	Description	Entitlements
Infinity ERM Application fundamentals	Asset Discovery Engine	Included
	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
Deep and Dark Web Monitoring Module	Credentials & Account Takeover monitoring & alerting	Included
	Open, deep and darkweb sources collection & search engine	Included
	Data leakage & fraud detection using pre-supported use cases (for credit cards, emails, source code and more)	Included
	Custom Threat Hunting rules	10
	Targeted intelligence manual threat hunting for data leakage, fraud and attackware (Cyberint Analyst)	-

Module	Description	Entitlements
Global Threat Intelligence	Global cyber news and ransomware watch	Included
	Cyberint research threat intelligence reports	Included
	Global Intelligence Knowledgebase (Threat Actors, Malware, CVE)	Preview
	IoC searches and browser extension	Included

Automated Intelligence Collection & Analysis

Cyberint, a Check Point company, conducts real-time monitoring of thousands of threat sources in the open, deep, and dark web, enabling the collection and addition of millions of intelligence indicators per day to the Infinity ERM internal data lake.

Raw intelligence items are automatically correlated with the organization's assets (IPs, domains, brands, executives, etc.) and are categorized according to a specific use case:

- Phishing
- Malware campaigns and other attackware
- Data (documents, source code, credentials) leakage
- Brand Abuse
- VIP protection
- Fraudulent activity
- others

Using proprietary machine learning algorithms, this raw intelligence is prioritized according to potential risk and impact, allowing rapid, smart and cost-effective analysis.

Automatic and semi-automatic analysis engines generate actionable intelligence alerts which are then disseminated to security teams with in-depth analysis, enriched context, threat actor profiling and more, allowing the organization to take effective action.

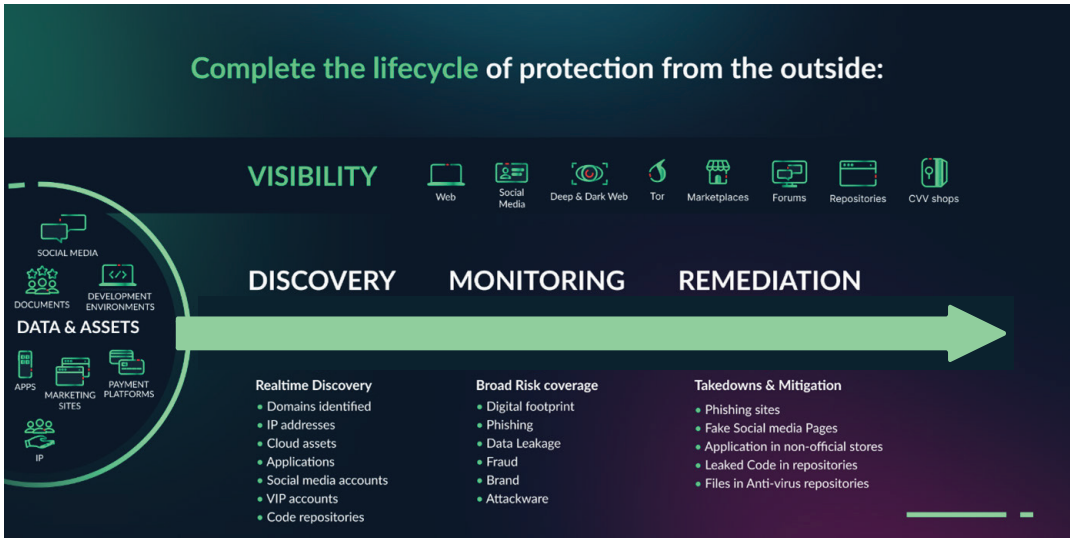

Figure 1 - Infinity ERM Threat Intelligence Data Flow

Contextualized Threat Intelligence

Infinity ERM provides context for all intelligence alerts with the following steps:

- Collect relevant threat intelligence items from an ever-growing list of open, deep & dark web sources.
- Execute complex analysis, including the application of machine learning and natural language processing algorithms to determine raw data relevancy and significance to each customer.
- Present relevant and analyzed data via the Infinity ERM web interface and/or share the data with customers' external systems via out-of-the-box integrations and/or a web services API in real time.
- Highlight for each intelligence item, when applicable, the relevant context concerning threat actors, tools, and techniques.

Infinity ERM is being used both by Cyberint's in-house analysts as well as customers to gain insights of threats and collaboration, allowing us to effectively become an extension of your organization's security team.

Infinity ERM Unique Threat Intelligence Differentiators

1. Infinity ERM provides real-time, targeted Threat Intelligence, collected from thousands of sources, as well as operational threat intelligence collected from numerous feeds to augment that data. The collected intelligence is then enriched with additional context and relevant information in the form of insights on the threat actors, tactics, techniques and procedures, as well as IoCs associated with the flagged indicator.
2. The targeted intelligence capabilities built into Infinity ERM rely on an array of advanced crawlers and proxies, which enable data collection from thousands of relevant sources (open web, dark web, social networks, forums, marketplaces, etc.) while maintaining anonymity.
3. These crawlers can automatically handle and bypass human authentication/trust mechanisms such as CAPTCHA. For special access forums and dark web sites, Cyberint's team of analysts and researchers create and manage avatars to gain access.
4. Cyberint is constantly evolving its list of unique sources and intel feeds supported by the system. These sources are scanned by Infinity ERM automated crawlers for the purpose of harvesting customer-specific information. Examples of Infinity ERM platform's current list of sources include Social Media feeds, online cyber-dedicated sources (XSS, breached, Exploit, hackforums, etc.), paste sites (such as pastebin.com, pastie.org, etc.) and an updated list of dark net marketplaces, chat rooms and forums, which are known locations for cyber criminals, across different industries.

5. This list of sources is updated continuously by cybersecurity experts and includes regionally relevant local sources per customers' needs (e.g. we cover unique Chinese sources, Russian marketplaces, and other specific sources). In addition, Cyberint constantly adds more feeds (free and commercial) to its aggregation engine to provide a holistic view of the customer's threat landscape, using all intelligence methodologies available.

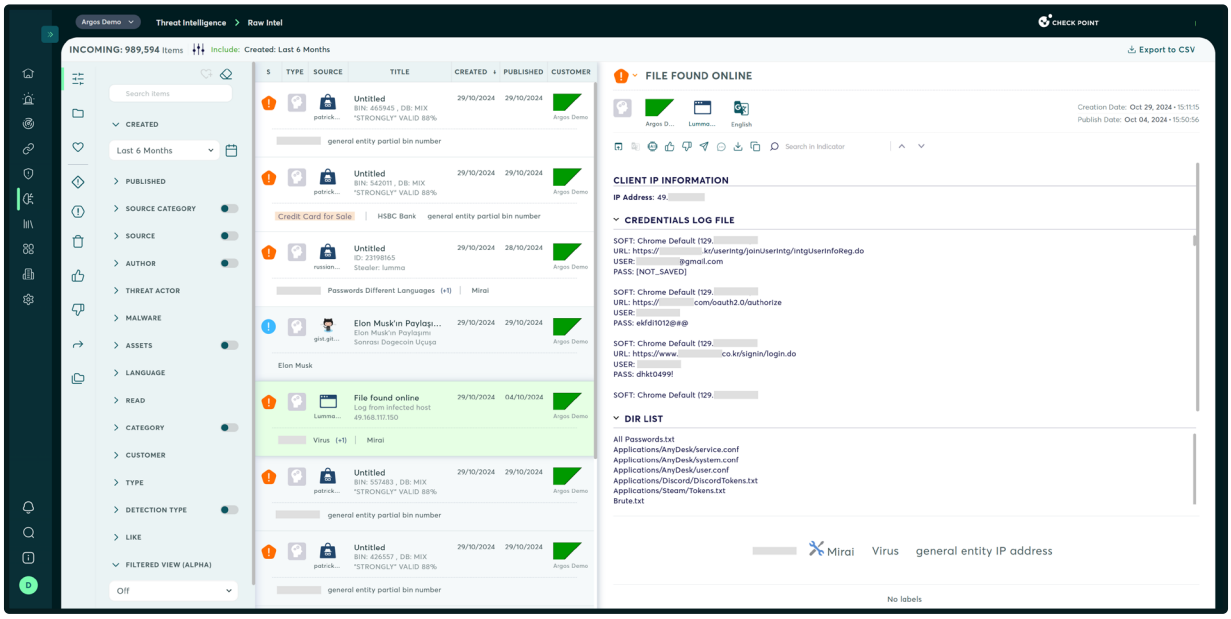

Figure 2 - Infinity ERM Threat Intelligence feed

Threat Hunting

Threat Intelligence Events collected within this module are prefiltered to display only raw intelligence which is relevant to the organization. This allows focused hunting and identification of threats that are related to the organization. Prefiltering is done through configuring the Infinity ERM solution with assets that belong to the organization, such as domains, keyword terms, brand names, VIP names, and so on. Once configured, Infinity ERM begins hunting through all sources for relevant intelligence items, flagging only relevant events within the targeted threat events view.

Licensing Details

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

	Licensing Instructions
Dark Web Monitoring Module	This licensing instructions are related to Dark Web Protection Module
	The main licensing dimension is the number of Threat Intelligence Assets. Assets are: Brand, Domain, Social Medial Account, Keyword, VIP name, and more. The assets are correlated with the data aggregated through continuous intelligence collection across the open, deep, and dark web to identify threats, data leakage, fraud and more.
	Select the number of assets needed based on the customer's needs. Additional assets can be procured as add-on.
	The standalone Dark Web Monitoring module doesn't include managed services. If required, the Complete and Elite packages include managed services.
	Monthly licensing is not available.

The following table displays the number of External Assets and Threat Intelligence Assets that come at eachpricinginterval. 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