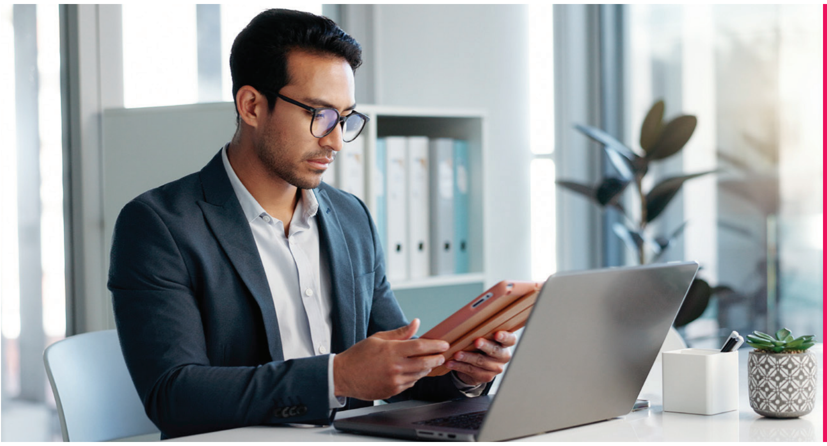
CHECK POINT™

Infinity



INFINITY EXTERNAL RISK MANAGEMENT

Attack Surface Management Module

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.

> "To protect ourselves, we must first know what to protect."

The Infinity ERM Attack Surface Management module comprises the following capabilities:

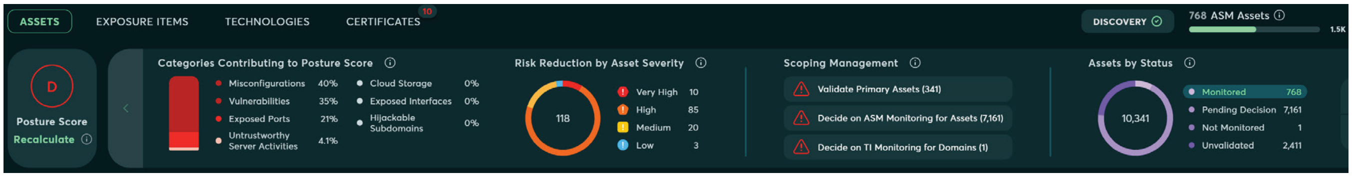
Module	Description	Entitlements
Infinity ERM Application fundamentals	Asset Discovery Engine	Included
	Alerts Center	Included
	Number of regular users	2
	Number of Threat Hunting users	-
	Tenants (a distinct Infinity ERM environment allowing users to visualize intelligence alerts for one company, subsidiary, or brand separately)	1
	Out-of-the-box integrations	1
	Customer Success Manager cadence	Yearly
	Support SLA	Direct Premium
Attack Surface Management Module	Vulnerabilities and exposure detection	Included
	Exposure items scan frequency	Daily
	Technologies detection & watchlist	Included
	Risk Posture Monitoring	Included
	Managed assets review & scoping (Cyberint Analyst)	-
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

ASM Discovery

The ASM discovery module identifies the entire organization's digital footprint, including additional domains, subdomains, IPs and cloud assets. These discovered assets are being utilized not only to identify vulnerabilities and exposure risk but also used as defined assets in the Threat Intelligence and Digital Risk protection module to identify additional areas requiring intelligence coverage. The Discovery module automates the process of asset discovery and provides up to date asset information while supporting continuous identification of the changing organization's landscape.

In order to discover the organization's assets, Infinity ERM uses various discovery mechanisms including: WHOIS data, DNS data, Cloud search, Certificates analysis and more.

The discovery engine will highlight additional discovered assets, the discovery reason, and its related confidence. Assets with high discovery confidence will be automatically put into coverage that yield risk identification. Assets that have lower confidence will require the user perspective to make the coverage decision.



Exposure Items & Vulnerabilities Scanning

For all monitored assets, the ASM module scans for the organization's digital presence for exposure items. The ASM dashboard displays all assets and issues in granular operational views.

The exposure items Infinity ERM looks for include but are not limited to the following:

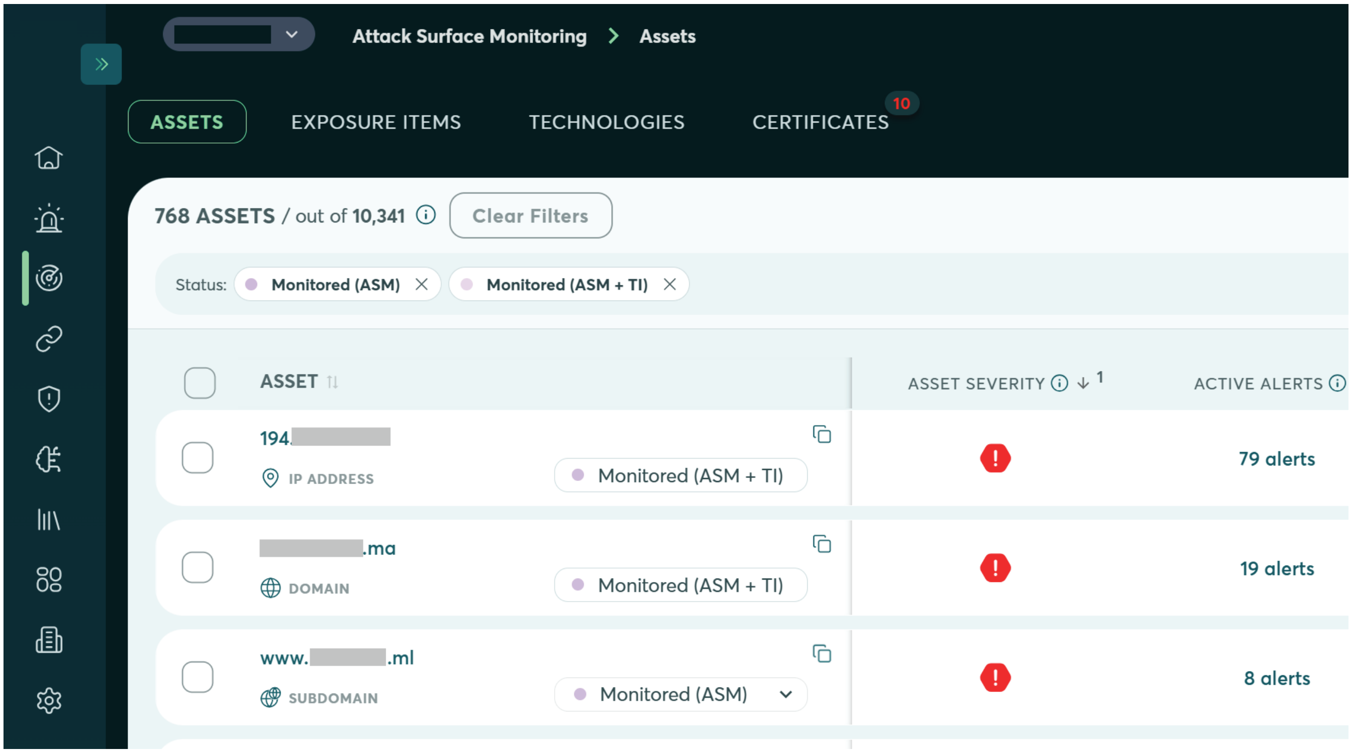
- Subdomain hijacking
- Misconfigured Cloud Assets
- Missing DNS and SPF records
- Potentially Exploitable Open Ports
- Open Web Interfaces
- Phishing and brand abuse
- Certificate Issues (CAA, SSL, etc.)
- Vulnerable technologies

Identified exposure items will undergo additional enrichment and contextualization. Exposure items with associated risk will generate alerts with the relevant content and recommendations for remediation actions.

Posture Risk Score

Based on the number of assets with identified risks, the environment's average remediation time, and the organization's size, Infinity ERM continuously calculates a risk score which is benchmarked against the organization itself and against organizations with a similar nature. The score is provided both in scale of 0-100 as well as A to F based on industry best practices.

The posture risk score is calculated for the entire organization as well as per asset, suggesting which assets contribute most significantly to organization's level of cyber risk and thus should be dealt with first.



[redacted] Attack Surface Monitoring > Assets

ASSETS | EXPOSURE ITEMS | TECHNOLOGIES | CERTIFICATES 10

768 ASSETS / out of 10,341 ⓘ Clear Filters

Status: ● Monitored (ASM) × ● Monitored (ASM + TI) ×

□	ASSET		ASSET SEVERITY ⓘ ↓ 1	ACTIVE ALERTS ⓘ
□	194.[redacted] IP ADDRESS	● Monitored (ASM + TI)	!	79 alerts
□	[redacted].ma DOMAIN	● Monitored (ASM + TI)	!	19 alerts
□	www.[redacted].ml SUBDOMAIN	● Monitored (ASM)	!	8 alerts

Figure 2 – Attack Surface Monitoring risk scoring, summary of leading risk categories and highest risk asset

Licensing Details

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

	Licensing Instructions
Attack Surface Management Module	This licensing instructions are related to the Infinity ERM Attack Surface Management module.
	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.
	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