Cyberint
A Check Point Company

How To Win Deals With Infinity External Risk Management (Cyberint)

For Channel Partners and Value-Added Resellers (VARs)

SOLUTION OVERVIEW

Cyberint, now a Check Point company, provides Impactful Intelligence solutions focused on the customer's digital estate – domains, IP addresses, websites, applications, social media channels, digital supply chain, and digital use of brand names and logos. The solution goes beyond the network perimeter to identify relevant threats 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.

The Infinity ERM platform focuses on protecting organizations beyond their perimeter and it includes several key modules:

1. **Attack Surface Management -** The 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.

2. **Brand Protection -** The Brand Protection module 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.

3. **Deep and Dark Web Monitoring -** The 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 a wealth of threat intelligence, the module analyzes the data and correlates it with the customer's digital assets to detect relevant threats and risks.

4. **Supply Chain Intelligence -** The Supply Chain Intelligence module evaluates the cybersecurity posture of 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 comprehensive risk score. Third-parties are continuously monitored for major incidents and alerts are issued in real time if one is suffering an attack.

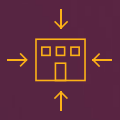
WHO IS THE INFINITY ERM SOLUTION FOR?

Infinity ERM is an ideal solution for Value Added Resellers (VARs) who want to offer a market leading product to their accounts while benefiting from large margins and business growth opportunities.

The ERM solution is most valuable for organizations that have a significant digital footprint, particularly those with 1,000 employees or more. Organizations of this scale often face an elevated risk from external threats due to their extensive digital exposure. Infinity ERM's capabilities provide comprehensive visibility across external attack surfaces, allowing companies to identify and address vulnerabilities before they're exploited. With Infinity ERM, companies can strengthen their resilience against a wide array of external threats, safeguarding their reputation and operational continuity.

INFINITY ERM ADVANTAGES

Infinity External Risk Management, Check Point's proprietary external cyber risk management solution, tailors impactful intelligence to the customer's attack surface and also provides the option to add supporting services from highly experienced threat intelligence analysts. Infinity ERM offers a fresh approach to address the following challenges:



Determine which relevant threats should be considered in order to design an effective cybersecurity defense architecture.

Illustrate the updated cyber risk status to the board and management, as well as an action plan.

Acquire predictive intelligence to identify intent, techniques, and tools to mitigate targeted threats before they materialize.

Continuously monitor digital risk exposures that can be exploited by cybercriminals.

Detect breaches as they propagate outside the organization's perimeter.

Gain visibility into attacks targeting your brand and customers that are constantly evolving outside of your network.

IDEAL CUSTOMER PROFILE -ICP

The ideal customer profile is:

SIZE	INDUSTRY	THREAT INTELLIGENCE MATURITY
1,000 to 100,000	FSI, healthcare, retail, technology, software, manufacturing	Have a SOC, CISO, or Cyber Security team

PAIN/INTEREST	TIMING	EXISTING CHECK POINT CUSTOMER
leaked credentials, impersonation, vulnerabilities, dark web monitoring	Replace current CTI/ASM vendor (Recorded Future, Intsights (Rapid7), Digital Shadows (Reliaquest), ZeroFox, RiskIQ, SOC Radar)	can be an advantage due to integration benefits leading to automated remediation

PERSONAS WE TARGET AND WORK WITH

CISO (Chief Information Security Officer)

The senior executive responsible for overseeing the organization's entire security operation. The CISO makes strategic decisions about cybersecurity initiatives and ensures alignment with the organization's risk management goals.

SOC Manager (Security Operations Center Manager)

The leader of cybersecurity incident handling within the organization, often reporting directly to the CISO. The SOC Manager coordinates incident response efforts and manages a range of cybersecurity tools, such as SIEM, SOAR, incident response platforms, and malware analysis solutions. The SOC Manager is often our primary champion throughout the engagement process and represents a key target persona.

Threat Intelligence (TI) Manager

Oversees the collection and analysis of cybersecurity threat intelligence, both specific to the organization and relevant to its region, competitors, and industry. The TI Manager, who may report to the SOC Manager, CISO, or Red Team, requires access to detailed intelligence insights to assess and respond to emerging threats effectively. In Tier 1 organizations, we often see a stronger presence and influence from the TI Manager, sometimes even surpassing that of the SOC Manager. In these cases, it's recommended to initially target both the TI and SOC Managers and then assess who is more likely to become the primary champion.

Cybersecurity\SOC Analyst

Responsible for responding to cybersecurity incidents within the SOC, the Analyst typically reports to the SOC Manager. For Tier 3 and Tier 4 organizations, the Analyst may report directly to the CISO and serve as a key technical advisor, especially when evaluating new security solutions.

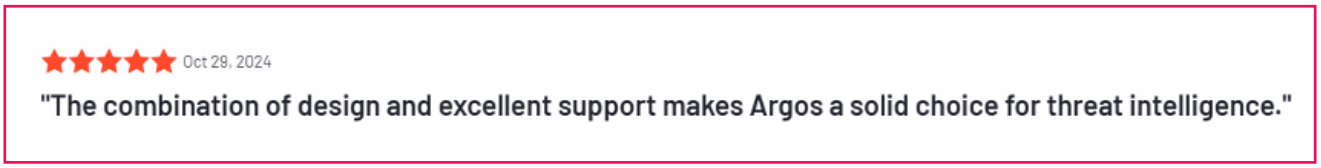
RECOGNITION AS AN INDUSTRY LEADER

By Industry Analysts

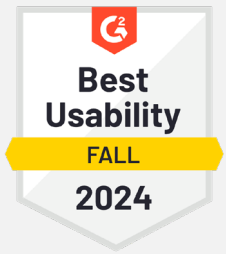
"In today's threat landscape, organizations face a multitude of challenges, including limited resources, visibility, and scalability. Cyberint recognized these unmet needs early on and capitalized on new growth opportunities to consolidate CTI, DRP, and EASM solutions into a unified framework and provide organizations with a holistic security posture."

https://e.cyberint.com/hubfs/Frost%20and%20Sullivan%20-%20Company%20of%20the%20Year%20-%20EERM%20-

By Our Customers



https://www.g2.com/products/argos-threat-intelligence-platform/reviews



Because we're a small team, the Check Point analysts are like an extension of us, which really helps from a risk management standpoint.

Evans Duvall, Cyber Security Engineer, Terex

THE OPPORTUNITY

- High demand – The ERM market is growing fast, and customers are looking for a solution to provide meaningful insights regarding their external facing threats.

- Trusted advisor – you can position yourself as a trusted advisor by shading light on threats that the customers were not aware of and how to mitigate them – big differentiator.

- External Health check – Check Point offers a free of charge POV in which we monitor the customer external threats based on their domain/sub domains/IP's and present an impactful summary of the insights. ERM POV's have more than 80% success rate!

- Revenue and Margin – ERM presents an amazing opportunity to increase your footprint within your client install base with an average of 6-digit ARR

- Upsell/cross sell – ERM deals tend to grow over time with more than 100% NDR and various upsell opportunities via the different modules and the ability to increase the capacity.

- Competitive replacement- ERM is leading Threat Intelligence platform in the market. When facing competitive situations, ERM can present great value and superior capabilities against the current solution the customer has.

- Check Point support – Check Point offers partner with advanced enablement and sales tools to support partners on their ERM journey (online certification, Workshops, Demo tools.)

- Sales models- ERM can be positioned via a Reseller or MSSP sales model.

CONTACT US

ISRAEL

Tel: +972-37-286-777
17 Ha-Mefalsim St Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
3rd Floor, Great Titchfield House,
14-18 Great Titchfield Street,
London, W1W 8BD

USA - TX

Tel: +1-646-568-7813
7250 Dallas Parkway STE 400
Plano, TX 75024-4931

SINGAPORE

Tel: +65-3163-5760
Level 42, Suntec Tower 3,
8 Temasek Boulevard. Singapore 038988

USA - MA

Tel: +1-646-568-7813
22 Boston Wharf Road
Boston, MA 02210

JAPAN

Tel: +81-3-3242-5601
27F, Tokyo Sankei Building, 1-7-2 Otemachi,
Chiyoda-ku, Tokyo 100-0004

ABOUT CYBERINT

Cyberint, now a Check Point company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Check Point External Risk Management solution 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 Check Point External Risk Management 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 / checkpoint.com/erm