

Cyberint

Beyond Digital Risk Protection

BEYOND DIGITAL RISK PROTECTION

Digital Risk Protection (DRP) is a proactive defensive strategy used by organizations to counter threats, improve efficiency, avoid unnecessary costs, and recover lost revenue. This provides security leaders and security teams with the ability to identify and address any existing cyber risk exposures before they turn into a breach.

Cyberint with its unique approach to moving Beyond Digital Risk Protection offers its Argos Edge™ platform to provide a DRP solution fully integrated with an external Attack Surface Monitoring (ASM) capability, both seamlessly infused with autonomous and targeted Threat Intelligence to help address the following challenges:

- **Determine which relevant threats** should be considered in order to design an effective cybersecurity defense program
- **Illustrate the up to date cyber risk status** to the board and management with a clear action plan
- **Acquire predictive intelligence** to identify intent, techniques, and tools to mitigate targeted threats before they materialize
- **Continuously monitor digital risk exposure** that can be exploited by cybercriminals
- **Detect breaches as they propagate** outside the organization perimeter
- **Gain visibility into attacks** targeting your brand and customers that are constantly evolving outside of your network
- **Autonomous and continuous discovery** of an organization's evolving digital footprint – automatically updating and optimizing the Threat Intelligence coverage

BUSINESS CHALLENGES ADDRESSED BY CYBERINT:



Digital Footprint Monitoring



Phishing Attacks



Data Leakage



Ransomware & Attackware



Fraud



Account Takeover



Deep & Dark Web Monitoring



3rd Party Cyber Risk

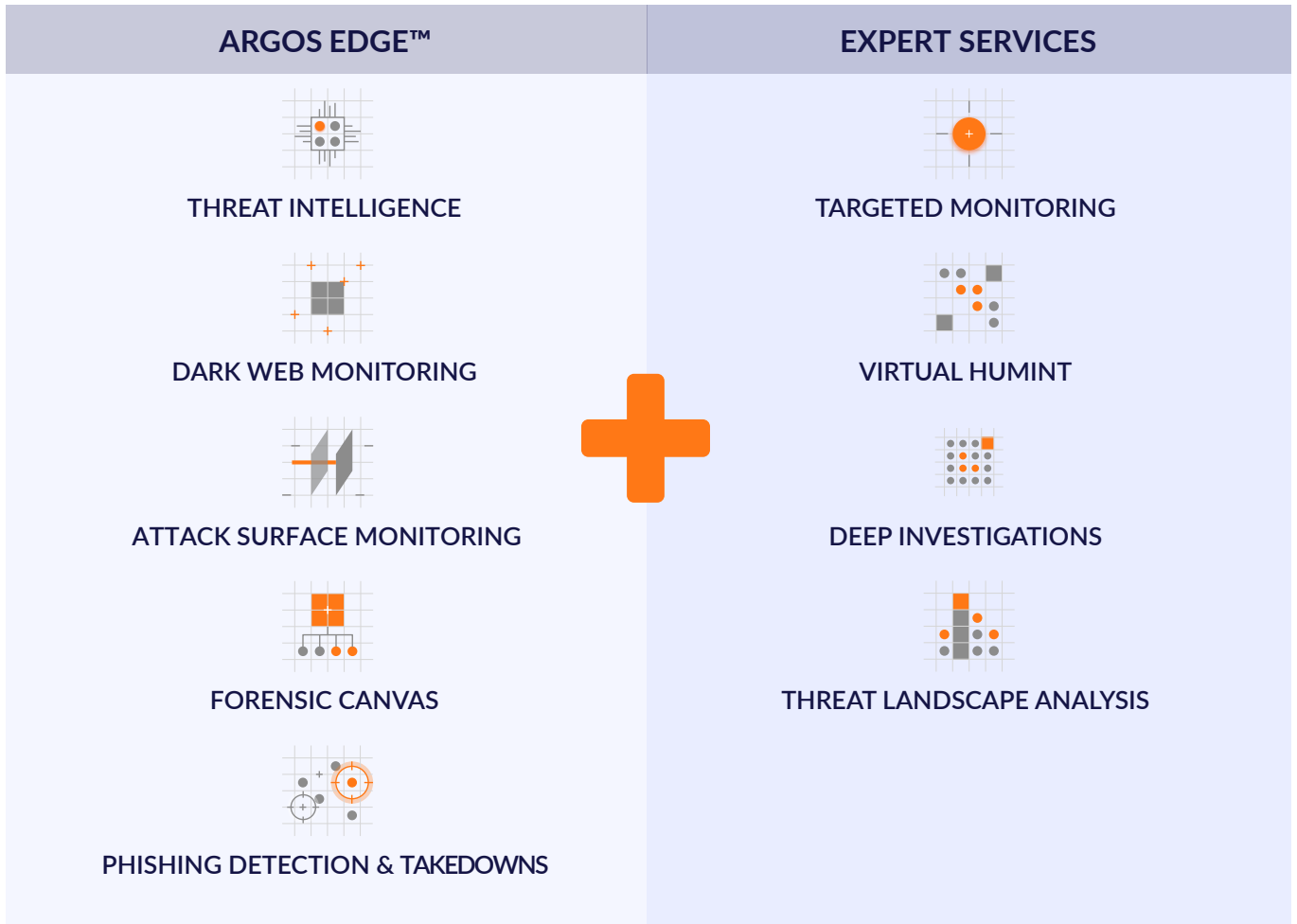


Social Media Monitoring

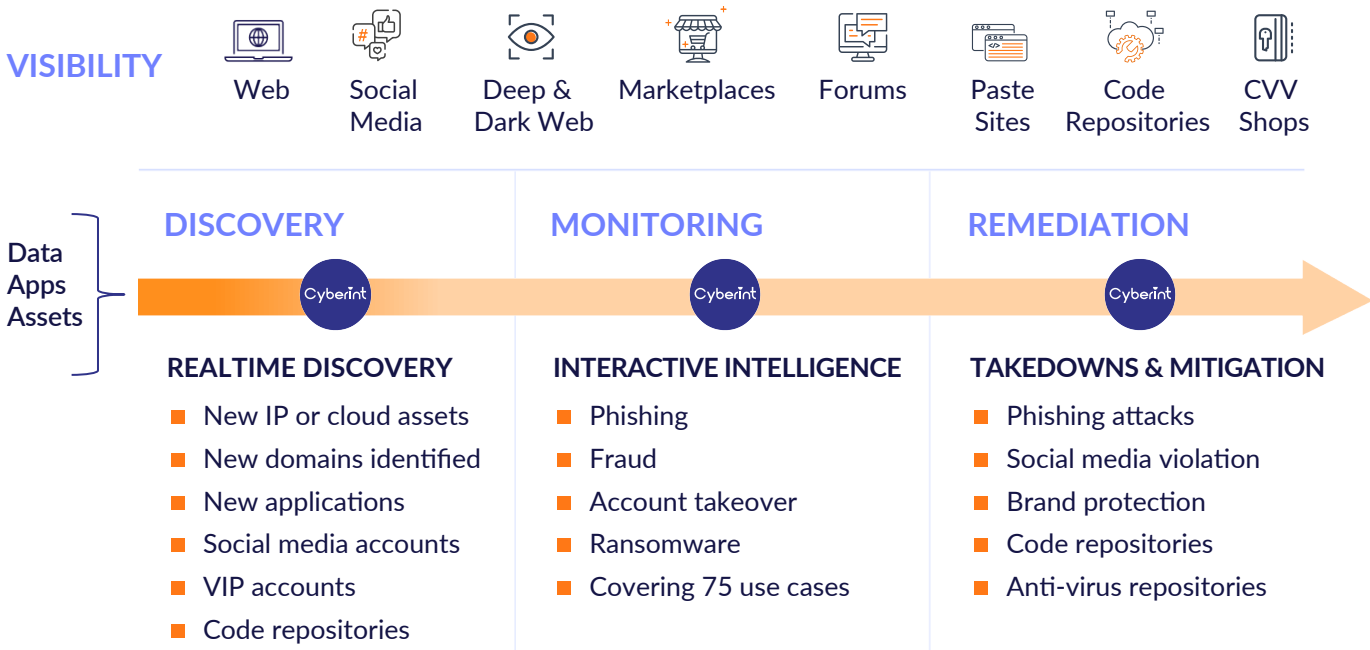


Brand Protection

CYBERINT OFFERING

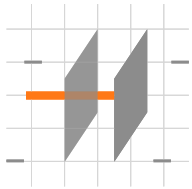


COMPLETE LIFE CYCLE OF PROTECTION FROM THE OUTSIDE:



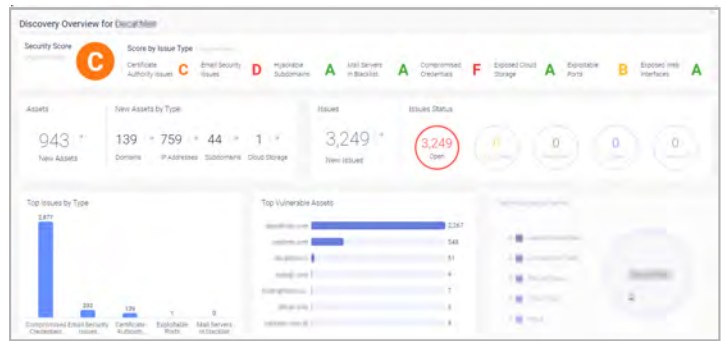
ARGOS EDGE™ DIGITAL RISK PROTECTION PLATFORM

Argos Edge™ is a multi-tenant, SaaS platform that uniquely integrates a Digital Risk Protection Solution along with Attack Surface Monitoring capability, infused with realtime Threat Intelligence to help protect an organization from external cyber threats beyond the perimeter with multiple modules:

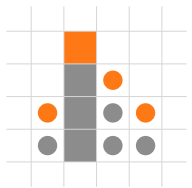


ATTACK SURFACE MONITORING

Argos Edge™ Attack Surface Monitoring identifies the organization's digital footprint and monitors assets beyond the perimeter on an ongoing basis, ensuring visibility into said assets with severity-based prioritization of issues to address, highlighting related threats, vulnerabilities, and weaknesses.



Argos Edge™ Digital Risk Protection Platform, Attack Surface Monitoring



THREAT INTELLIGENCE COLLECTION AND ANALYSIS

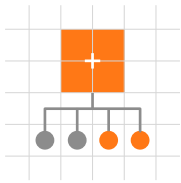
Cyberint's real-time monitoring of thousands of threat sources in the open, deep, and dark web leads to the collection of millions of intelligence items per day to Argos Edge™'s internal data lake.

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, credential stuffing, data leakage fraudulent activity and others. Using Cyberint's proprietary machine learning algorithm, this raw intelligence is prioritized according to potential risk and impact, allowing smart and cost-effective analysis.

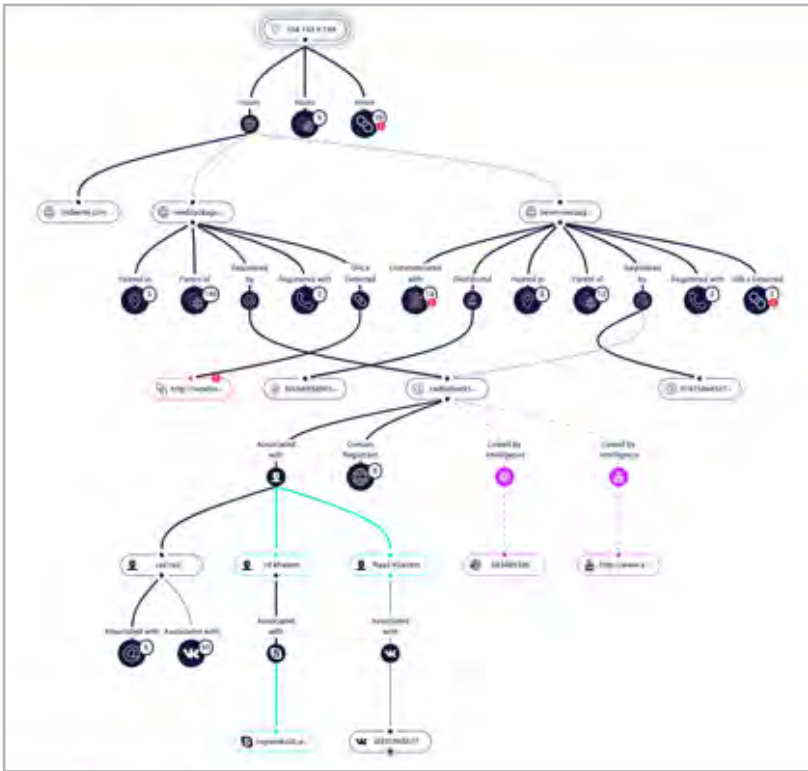


Argos Edge™ Digital Risk Protection Platform

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.



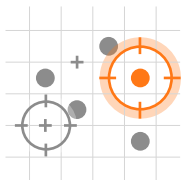
FORENSIC CANVAS



Argos Edge™ Digital Risk Protection Platform, Forensic Canvas

Cyberint's Forensic Canvas Module allows identification and profiling of threat actors as well as a deep investigation of tools, tactics, procedures (TTP's) they employ.

The Forensic Canvas is utilized to enrich the context of specific or multiple IOCs, integrating multiple services into a unified investigation platform to support various types of connections, including Argos Edge™ Threat Intelligence, WHOIS services, passive DNS, social discovery, malicious code detection, etc.



PROACTIVE PHISHING DETECTION TECHNOLOGY & TAKEDOWNS

Phishing persists as a major risk for digital organizations, resulting in account takeover, leading to customer churn, and negative impact to brand reputation. Answering this challenge, Cyberint developed the Phishing Beacon, a proprietary module allowing real-time visibility of newly created phishing sites cloned from organization's website content, an effective technique utilized by threat actors. Cyberint's rapid detection enables us to take down phishing sites on behalf of the organization to quickly eliminate the risk.

WHAT'S IN IT FOR YOU

- **REDUCE SHADOW IT SECURITY RISK**
- **GAIN VISIBILITY INTO YOUR ATTACK SURFACE**
- **SHORTEN THREAT DWELL TIME**
- **EXTEND YOUR TEAM'S CAPABILITIES**
- **REDUCE CYBERSECURITY TCO**
- **MITIGATE 75 BUSINESS RISKS**

EXPERT SERVICES

Bespoke cyber intelligence services that fit your needs

THREAT INTELLIGENCE TEAM AUGMENTATION

Cyberint offers a managed Digital Risk Protection program providing access to our Argos Edge™ platform and a team of cyber threat analysts, augmenting any CTI program to a higher level of quality and performance.

Partnership with Cyberint’s analyst team includes day-to-day interaction with a dedicated analyst who becomes a member of your in-house team. Analysts are assigned based on their knowledge of industries and their intimate understanding of business needs.

All raw intelligence items brought to light by Argos Edge™ are diligently verified, contextualized, and attributed to real risks by utilizing tremendous amounts of data collected from the open, deep, and dark web.

Our team of analysts is multilingual thus allowing an understanding of the threat actors in their respective language. In addition, the analyst’s mastery of cybercriminal “lingo” and culture allows you to identify, verify, and mitigate those threats that will most likely come to fruition as attacks.

Cyberint provides a valuable human element when it comes to research, investigation, and threat intelligence operations. The Virtual HUMINT capabilities, i.e. live interaction with threat actors, enables deeper contextualization which is required for effective mitigation.

CYBERINT RESEARCH

Cyberint’s Cyber Research Team explores the frontier of the cyber threat landscape to maintain strategic visibility of trending threats. The Cyber Research Team analyzes vast amounts of data to create strategic threat intelligence reports, enabling decision makers to identify meaningful trends, and gain a broader and deeper perspective of the digital risks targeting their organization. The report includes periodic analysis of current sector risks, notable threat actors, TTP analysis, and more.

SAMPLE CYBERINT REPORTS



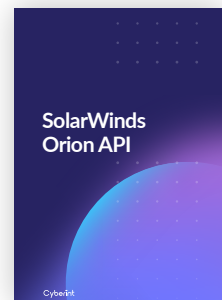
US Threat Landscape Report
Threat Landscape Report

[DOWNLOAD](#)



REvil - Steal, Encrypt & Auction
Research Report

[DOWNLOAD](#)



SolarWinds Orion API
Research Report

[DOWNLOAD](#)

BENEFITS OF PARTNERING WITH CYBERINT



THREAT DETECTION

Detect threats with predictive intelligence



IDENTIFY SEVERITY

Identify the severity of threats and understand 'the big picture'



VIRTUAL HUMINT CAPABILITIES

communicate directly with threat actors, attribute their activity to specific campaigns and gain more context and intelligence



IDENTIFY FRAUD OPERATIONS

Identify and provide actionable intelligence on how to respond and mitigate



REAL-TIME PHISHING DETECTION

Real-time phishing website detection and takedown operations



VIP THREAT INVESTIGATIONS

Monitor online presence of your executives to prevent the threat actors from obtaining personal information for malicious use



MAP AND MONITOR

Map and monitor the digital presence of the organization, including credential leaks, digital vulnerabilities & sensitive documents leakage



HOLISTIC PROTECTION

Fully integrated ASM and DRP to provide autonomous and continuous discovery of an organization's evolving digital footprint.



4.8



The only sample vendor mentioned by Gartner for both EASM and DRPS in the r Hype Cycle reports, July 2021

FROM OUR CUSTOMERS



With Cyberint, our team is able to act efficiently on alerts. We are confident the information we receive is validated and enriched to paint a clear picture of our attack surface, a vital aspect of our threat intelligence program. The launch of the new Argos™ platform has allowed us to get visibility and act upon the digital threats faced outside the perimeter to our digital assets. We've also managed to heighten visibility to our executive team

Thomas Neumann
Group CTO



For me, Cyberint isn't just another third-party vendor, but an extension of my team. Together we are working to help enable the future of a digital and cashless economy not only in the Philippines but around the world.

Mark Frogoso
CISO at GCash



CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

368 9th Ave, Suite 09-123
New York, NY 10001
Tel: +1-646-568-7813

ISRAEL

17 Ha-Mefalsim St.
4951447 Petah Tikva
Tel: +972-3-7286-777

UNITED KINGDOM

14 Grays Inn Rd., Holborn
WC1X 8HN, London
Tel: +44-203-514-1515

SINGAPORE

135 Cecil St. #10-01 MYP
PLAZA 069536
Tel: +65-3163-5760

FRANCE

67 Avenue de Wagram
75008 Paris
Tel: +33 1 77 50 58 91