Cyberint
Impactful Intelligence

CYBERINT ARGOS PLATFORM

ATTACK SURFACE MANAGEMENT DATASHEET

The Cyberint Attack Surface Monitoring 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 exposures, assesses the risk of each one, and assigns risk scores to simplify prioritization, accelerate remediation, and help you improve security posture.

Challenge

It's no secret that corporate digital footprints are growing at a fast pace. There are many contributing factors: cloud migrations, a surge in new domains and websites, more customer-facing applications, vast quantities of data to manage, and more.

Keeping a complete and up-to-date asset inventory is difficult, but it is essential for securing your networks, systems, and data. After all, you cannot protect the assets that you do not know about.

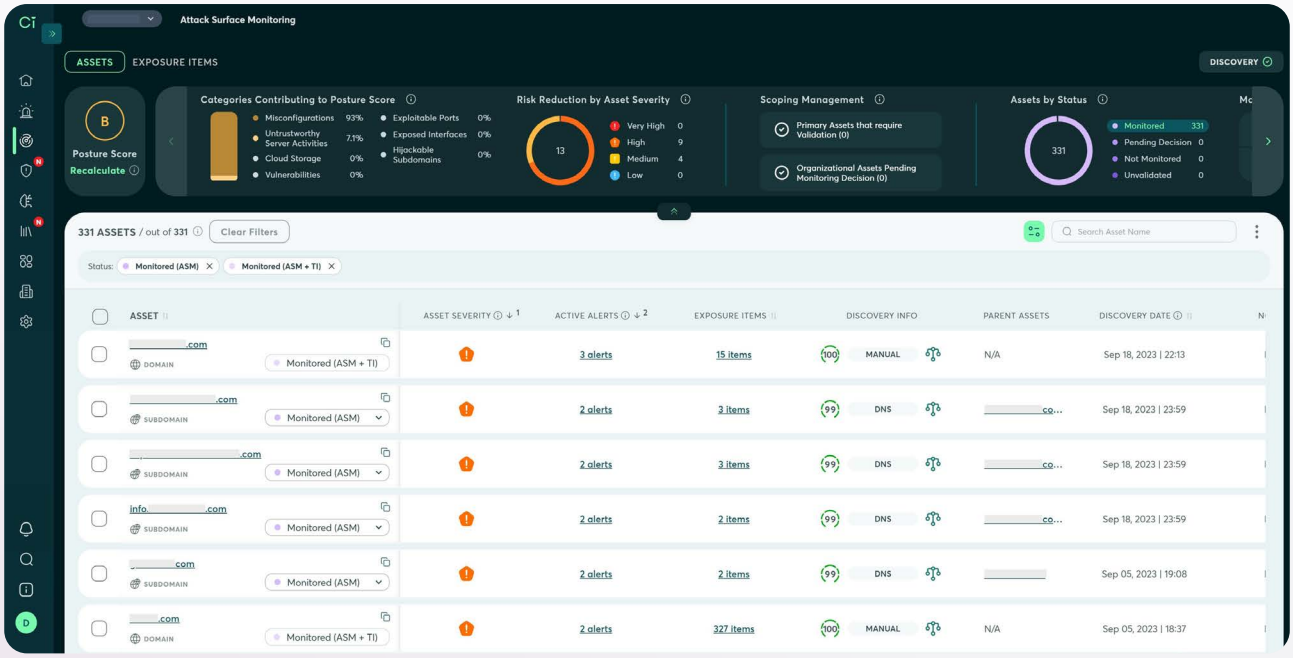
Solution

The Cyberint Attack Surface Management module provides complete visibility on your external IT assets to uncover shadow IT, misconfigurations, high-risk CVEs, and other risks. The discovery process is automated and continuous so new assets are detected and added into scope in real time as your external infrastructure expands and evolves.

Cyberint also maps threat intelligence data to your attack surface, providing high fidelity alerts that enable a proactive security posture. Detect and disrupt threats faster with impactful intelligence tailored to your organization's digital footprint.

Key Benefits:

- Gain a complete understanding of your organization's digital footprint
- Detect risks in your external IT infrastructure, like exposed cloud storage and high-risk CVEs
- Map threat intelligence data to your organization's external attack surface
- Understand your exposures and risks so you can optimize remediation efforts
- Resolve critical issues to reduce risk and keep your organization secure



Continuously Discover Your External Attack Surface

Cyberint continuously maps out your external attack surface to detect, inventory, and validate all of your organization's external digital assets, including the ones you might not know about.

Improve Visibility On Your Attack Surface

Uncover your organization's external attack surface to identify shadow IT, misconfigurations, and other risks.

Keep Up With Your Evolving Footprint

Continuously discover new assets as they are deployed to automatically keep up with your expanding digital footprint.

Save Time With Automatic Scoping

Configure your settings to automatically add new assets into scope and efficiently manage your attack surface.

Identify & Monitor The Technologies In Your Environment

The Cyberint ASM module identifies all technologies, including the version number, running on your Internet-facing assets and creates a comprehensive technology inventory for continuous monitoring.

Develop A Technology Inventory

Know what software and services are running in your external attack surface, and on which domains and IP addresses.

Receive Real-Time Alerts For New CVEs

Receive an alert in real-time when a new CVE is published for a technology running on one of your Internet-facing assets.

Monitor Any Technology For Risks

Manually add software and services to the Technology inventory to monitor them receive CVE alerts.

Detect Exposures & Understand Your Cyber Risks

Cyberint provides visibility on exposures, such as open ports, exposed interfaces, outdated protocols, and more. While not all exposures are a risk, Cyberint identifies and alerts you to the real risks.

Gain Visibility On Your Exposures

View all your organization's exposures that are visible to attackers, so you can add new controls where needed.

Assess Risk & Prioritize Issues

Use Cyberint's risk scores to prioritize issues, streamline remediation, and improve security posture.

Map Intelligence To Your Assets

Cyberint uses your asset inventory as the basis for deep and dark web monitoring and impactful threat intelligence alerts.

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

Evans Duvall, Cyber Security Engineer, Terex

Read more in the customer case study.

"We realized that Cyberint was much more than an EASM solution, it delivered much value with highly relevant intelligence from the deep and dark web."

Benjamin Bachmann, Head of Group Information Security, Ströer

Read more in the customer case study.

"Once we identified the need to address the risk of fraudulent websites and social profiles, I quickly realized we needed to handle this in a scalable manner. Our solution is to use Cyberint to help us automatically detect and takedown these threats."

Ken Lee, IT Risk and Governance Manager at Webull Technologies

Read more in the customer case study.

Recognition As An Industry Leader From Trusted Analysts

Gartner FROST & SULLIVAN G2 IDC

Discover Cyberint with a personalized demo

About Cyberint

Cyberint, the Impactful Intelligence company, reduces risk by helping organizations detect and mitigate external cyber threats before they have an adverse impact. The Cyberint Argos platform's patented technology 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 Cyberint 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