IONIX

DATASHEET

IONIX ASM FOR MSSPs

AT A GLANCE

IONIX Attack Surface Management is the Ideal ASM Platform for MSSPs

See the whole digital ecosystem from the outside, in.

Provides the widest ASM coverage while keeping noise-levels low.

Inspect your clients' posture from the attacker's perspective.

Purpose built for MSSPs

- Enhances security and supports revenue growth with your existing customer base
- Manages customer security your way with your toolset
- Lightweight and flexible pay-as-you-grow business model
- Offer a pre-sales scan to help prospects understand the value and allow you to price accurately

Global CISOs depend on IONIX's machine learning-powered discovery engine, contextual risk assessment and prioritization, for their remediation workflows, managing their complex and ever-changing attack surface.

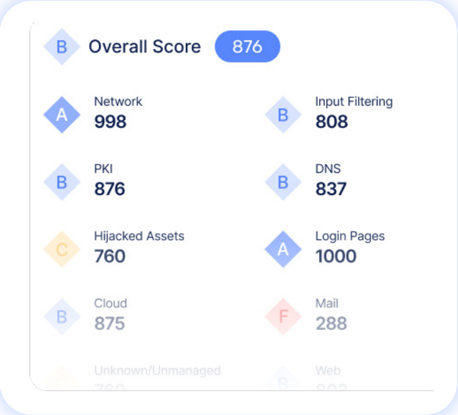
Infosys Lexmark WARNER MUSIC GROUP

The Telegraph e·on GCE GRAND CANYON EDUCATION

IONIX - BUILT FOR MSSPS

IONIX ASM was purpose-built for MSSPs. Native multi-tenancy means that you can manage each customer as well as you manage all your customers. And IONIX ASM doesn't just enhance security across all your customers, it enhances revenues, too. From presales to upsell – IONIX grows your business as you grow confidence in customer security.

- Simple pre-sales hunting
  Pre-sales scan shows prospects what they can't see in their own real attack surface, and deep into their digital supply chain dependencies.
- Executive summary reports for decision makers
  Clearly demonstrate value with reports describing a weighted Risk Score and key remediation recommendations across multiple security audit and assessment categories.
- Not one size fits all
  Custom-tailored service offerings fit each customer perfectly .
- Integrated API access
  API and portal access for each onboarded customer lets you consume IONIX data in your system of choice, in a single pane of glass.



B Overall Score 876

A Network 998

B Input Filtering 808

B PKI 876

B DNS 837

C Hijacked Assets 760

A Login Pages 1000

B Cloud 875

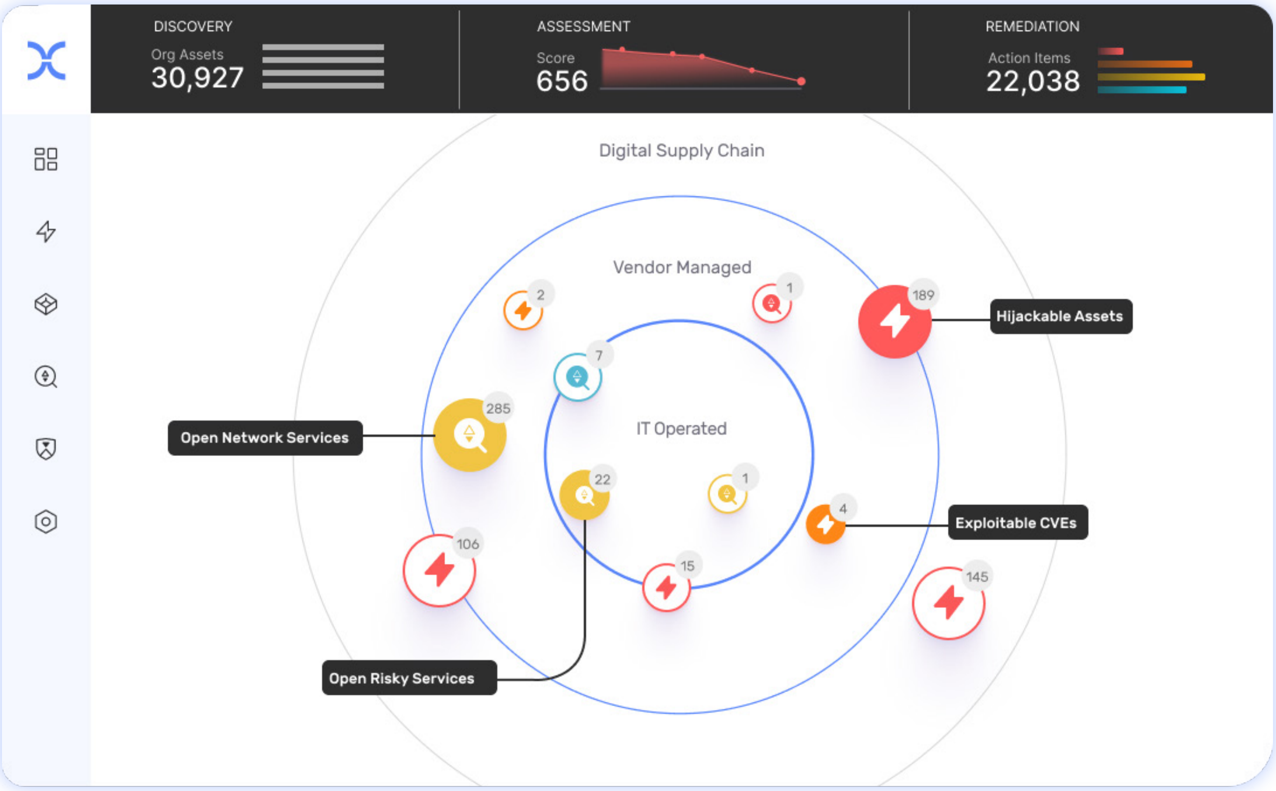
F Mail 288

Unknown/Unmanaged

Web

ASM DEFINED - WHAT IS ATTACK SURFACE MANAGEMENT?

Attack surface management (ASM) is the continuous discovery, analysis, remediation and monitoring of cybersecurity vulnerabilities and misconfigurations that make up an organization's potential attack surface.



DISCOVERY
Org Assets 30,927

ASSESSMENT
Score 656

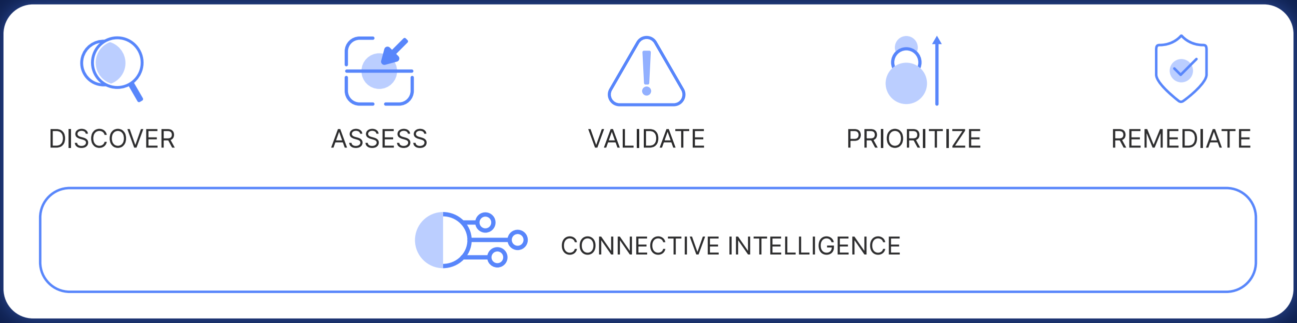
REMEDIATION
Action Items 22,038

IONIX Threat Exposure Radar exposes critical risks so you can effectively reduce risk and improve your security posture.

IONIX ASM – WIDEST COVERAGE, SHARPEST FOCUS

IONIX is a leader in Attack Surface Management, focused on the discovery of every internet-facing asset the ways those assets are connected to an organization's supply chain, shedding light on the most important risks to your business, and providing simple-to-follow recommendations to rapidly remediate exploitable threats and reduce attack surface risk.

THE PLATFORM IS BUILT ON FIVE PILLARS OF MODERN ASM AND OUR PROPRIETARY "CONNECTIVE INTELLIGENCE"



ATTACK SURFACE DISCOVERY

IONIX discovers customer assets, connected business partners and subsidiaries including third-, fourth- and fifth-party digital supply chain assets.

CYBER RISK ASSESSMENT

The platform automatically conducts assessment of the organization's entire attack surface across 13 categories. Every asset is tested for vulnerabilities, misconfigurations, and security posture issues.

SECURITY VALIDATION – POTENTIAL EXPLOITABILITY

IONIX's simulations use non-intrusive methods to validate security issues using our stealthy operation techniques.

PRIORITIZATION

IONIX prioritization framework provides risk severity, exploitability, asset importance, and threat intelligence to help security teams stay laser-focused on the risks that matter most.

REMEDIATION

The platform clusters multiple findings together into clear recommendation actions, automatically attributed to the right subsidiary or functional owner, leveraging integrated workflows with SIEM, SOAR and ticketing systems. Plus, our innovative Active Protection is capable of identifying supply chain related misconfigurations and automatically neutralizes these sorts of threats.

CONNECTIVE INTELLIGENCE

IONIX is built on a graph data model, comprised of assets and connections. 'Connective Intelligence' refers to proprietary patented techniques that transform this data model into meaningful outcomes, for example, identifying digital supply chain-related vulnerabilities or misconfigurations to expose attack paths that may lead back to organizational assets.

THE RIGHT FIT ACROSS ALL CUSTOMER TEAMS

IONIX ASM delivers immediate visibility and value for:

- Red and Blue Teams – Greater visibility for all security researchers into organizational attack surface, for better offense and defense exercises.
- SOC Teams– enabling better and faster mitigation of emerging threats originating from organizational or managed assets.
- Vulnerability Management Teams – Streamline scanning to find unknown assets, both owned and hosted and consolidate effective patching and updating based on risk priorities.
- Risk Assessment and TPRM Teams - Easy visibility into digital supply chain and organizational dependencies.
- Infosec Analysis Teams - Immediate visibility into risk-based assessments and searches for “needle in the haystack” tied to attack surface (such as potential impact of a newly released Zero day vulnerability).

> *“While other ASM solutions provided remediation instructions for classical vulnerabilities and best-practice issues, IONIX went further and prevented abuse of sophisticated supply-chain vulnerabilities that the other solutions did not detect.”*
>
> CISO, Global 1000 retailer

IONIX: YOUR ASM DIFFERENTIATOR

IONIX ASM is a strategic market differentiator that grows with you and your customers. Key differentiators include:

GREATER VISIBILITY INTO WHAT’S IMPORTANT:

Offer customers the market’s deepest discovery, including the digital supply chain, with assessment and prioritization capabilities to focus customers on what’s urgent and important to fix.

VISIBILITY INTO THE ATTACKER'S PERSPECTIVE:

By understanding and managing the external attack surface, organizations can proactively address vulnerabilities and misconfigurations before they are exploited by threat actors.

FAST TIME TO VALUE:

Non-intrusive scanning continuously discovers and expose risks across organizations’ internet facing assets and their digital supply chains. Your customers have nothing to install or configure. See results starting from a proof-of-concept.

ALIGNS WITH DIGITAL TRANSFORMATION:

As your customers increasingly adopt cloud services, online platforms, and digital interfaces for their operations, the external attack surface becomes even more critical.

GET STARTED TODAY

Contact us at sales@ionix.io to learn more.
Head to ionix.io to understand more about the IONIX platform.