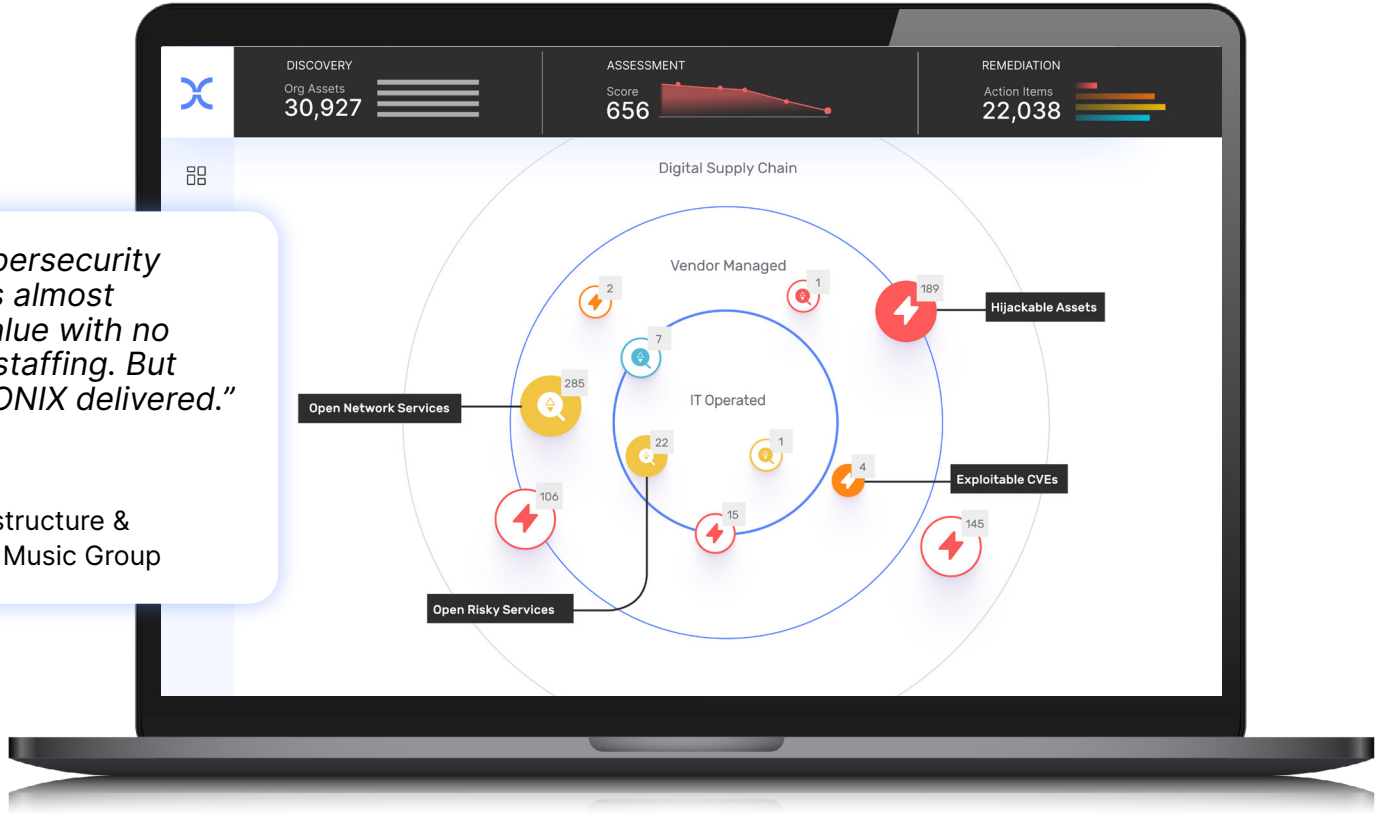
IONIX

DATASHEET

IONIX ATTACK SURFACE MANAGEMENT

EXPOSE THREATS ACROSS YOUR REAL ATTACK SURFACE



"It's rare to find a cybersecurity solution that delivers almost immediate time to value with no impact on technical staffing. But that's exactly what IONIX delivered."

John Remo
SVP Global Cloud / Infrastructure & Cybersecurity at Warner Music Group

MORE THAN 20% OF YOUR ATTACK SURFACE RISK SITS IN THE DIGITAL SUPPLY CHAIN

IONIX Attack Surface Management delivers laser-focus into your most important exploitable attack surface risks - including deep into the digital supply chain.

SEE YOUR ATTACK SURFACE LIKE AN ATTACKER WOULD, FROM THE OUTSIDE-IN

Your organization's attack surface risk exposure goes beyond assets that you own. That's because a threat actor set on penetrating your organization doesn't care whether they're attacking your internet-facing asset directly or exploiting a vulnerability from a third-party digital service that provides a toehold into your environment. Only IONIX monitors every internet-facing asset and connection, delivers laser-focus into the most critical risks to your business, and provides recommendations to rapidly remediate exploitable threats and reduce attack surface risk.

IONIX BENEFITS

- Discover more – get full attack surface coverage
- Assess further – understand what's important to fix and avoid noisy alerts
- Automatically validate – non-intrusive testing for critical exposures
- Prioritize smarter – not an inventory of assets, a connected map of exploitability
- Remediate faster – MTTR of days, not months

"After working with IONIX for over a year, we are confident that its ASM platform gives us the critical visibility we need to solve the difficult challenge of managing the risks and vulnerabilities in our entire digital supply chain."

René Rindermann
CISO, E.ON

USE CASES

Continuous attack surface management
Automatically adapt coverage to changes and monitor risks.

Digital supply chain security
Protect your organization from digital supply chain threats.

Attack surface reduction
Reduce critical risks systematically and decommission unused, neglected assets.

M&A risk management
Manage cyber risk throughout the acquisition process, from evaluation to integration.

Subsidiary risk control
Centralize oversight and localize attack surface management with automated attribution.

Cloud operation security
Gain visibility and manage risk exposure across public cloud platforms.

Vulnerability management
Augment your existing program with automated attack surface discovery, assessment, and prioritization.

Attack Surface Validation
Automated testing to validate exposures and determine the exploitability of zero-day threats

HOW IONIX WORKS

ATTACK SURFACE DISCOVERY | RISK ASSESSMENT | EXPOSURE VALIDATION | RISK PRIORITIZATION | ACCELERATED REMEDIATION

ATTACK SURFACE DISCOVERY

Discover your real attack surface and its digital supply chain

IONIX's multi-layered discovery engine creates a comprehensive inventory of your organization from the attacker's point of view – including the 20% of your exploitable attack surface from your digital supply chain:

- **Global event tracking** - monitor global PKI and domain registration
- **FQDN and IP discovery** - Machine learning driven discovery of all domains, subdomains, and IPs
- **Reverse indexing** - domains, IP blocks, and cloud platforms
- **Reduced False Positives** - "Discovery Evidence" findings use ML to accurately attribute each asset

IONIX represents your attack surface using a dynamic, graph-based ML model – with nodes and dependencies that are continuously updated and an ever-evolving set of potential kill chains evaluated.

RISK ASSESSMENT

Identify risks in context, at scale

IONIX runs an in-depth evaluation of each asset according to 13 asset categories including Cloud, PKI, Web, DNS – automated at scale across your entire environment. Using patented Connective Intelligence, IONIX's risk assessment extends recursively from your own assets to your digital supply chain. By evaluating assets and connections, IONIX identifies risky connection vulnerabilities – external risks due to connected DNS chains, 3rd party web services, and external dependencies – that impact your security posture. Plus, IONIX Risk Scores aggregate security issues and risks into high-level attack surface benchmarks across multiple categories - providing actionable ways to improve your security program.

EXPOSURE VALIDATION

Automate exploit simulation

IONIX conducts active, non-intrusive security tests that simulate external attacks, across your entire attack surface. Without disrupting operations, IONIX Exposure Validation tests for thousands of risks and continually expands coverage in response to emerging threats including, exploitable vulnerabilities, critical misconfigurations, data exposures and more. The IONIX approach identifies critical exposures, ensuring that resource-strapped security teams can focus on the most significant risks to their business and get buy-in from IT stakeholders to accelerate remediation.

HOW IONIX WORKS

ATTACK SURFACE DISCOVERY | RISK ASSESSMENT | EXPOSURE VALIDATION | RISK PRIORITIZATION | ACCELERATED REMEDIATION

RISK PRIORITIZATION

Focus on the risks that matter most

Security teams need to consider the unique business context of an asset at risk. IONIX prioritization framework combines risk severity, exploitability, blast radius, and threat intelligence to help security team stay laser-focused on the risks that matter most to their organization. IONIX dynamically prioritizes threats based on asset importance across four dimensions: sensitive data access, business context, brand reputation, and dependencies' operational impact.

IONIX's risk-based prioritization draws on severity (CVSS & EPSS) as well as attack vectors like misconfigurations and other critical security issues such as dangling DNS records, exposed storage, cross-site scripting risks, weak/no password.

ACCELERATED REMEDIATION

Prevent attacks before they happen

IONIX's smart workflows align remediation tasks with the way that security operations work – so you spend less time routing tickets and more time resolving critical risks. Security issues are clustered into concise action items reducing noise and providing immediate clarity on what needs to be done. Action items are automatically attributed to the right business entity or subsidiary – and assigned to the relevant personnel – for faster time to resolution.

IONIX integrates with security information and event management (SIEM) systems, SOAR, security operations center (SOC) software, and ticketing systems – accelerating remediation with streamlined workflows across teams.

GET STARTED TODAY

Contact our team to get a free scan.

Get a free scan | Learn more at ionix.io

DATASHEET IONIX

© 2024 IONIX. All rights reserved. IONIX is a trademark of IONIX.
Information subject to change without notice. MAR2024