aws marketplace

IONIX

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

IONIX

IONIX Recap

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

IONIX ASM – Widest Coverage, Sharpest Focus

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

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.

IONIX Benefits:

Discover more – get full attack surface coverage

- Discover up to 50% more assets, even digital-supply chain assets
- Minimize false positives
- Map changes continuously

Assess further – focus only on what's important to fix and avoid noisy alerts

- Evaluate both assets and connections
- Scan with the context of 13 asset categories

Prioritize smarter – Not an inventory of assets, a connected map of exploitability

- Go beyond severity scores
- Integrated threat intelligence
- Analyze exploitability and blast radius

Remediate faster – MTTR of days, not months

- Improve efficiency by clustering issues
- Simple-language action items to send to SOC and IT teams
- Streamline workflows with built-in integrations to SIEM, SOAR…

Protect automatically – take control of exploitable assets before hackers do

- Apply Active Protection on critically vulnerable assets, preventing attacks before they

happen

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- “The most valuable feature of IONIX is the effortless setup.”

Rick Beltran

Director of Cybersecurity at a recruiting/HR firm with 1,001-5,000 employees

- “We're constantly surprised by how good IONIX is at detecting timely vulnerabilities.”

Verified user

AVP, Cyber Security at a insurance company with 10,001+ employees

- “The portal is an excellent resource, offering valuable insights in a clear and actionable format. It provides a wealth of information, presented in a way that's easy to understand and use. This aligns perfectly with our key focus when working with IONIX: ensuring the data they deliver is highly actionable.”

Verified user

Director - IT Security Services at a insurance company with 10,001+ employees

"IONIX enables us to manage all our assets from one platform. We can see all the assets, login pages, web services, etc., from one place. It automatically scans everything so we can find new information about our organization. We don't need to add each asset or interface manually."

Kfir Ernst

IT Administrator/Engineer at a financial services firm with 1,001-5,000 employees

"My favorite is the dark web association that it does. It basically takes things that are unknown to you and then also runs those URLs through the dark web to see if there are potentially leaked credentials unknown to you. It links both of those together and gives you that on a report. You can identify potentially compromised credentials that were previously unknown to you, and you can do something about them. It is a cool feature."

Verified user

IT Security Engineer at a media company with 1,001-5,000 employees

"The integration was easy."

Verified user

IT Security Officer at a retailer with 10,001+ employees

What users had to say about valuable features:

“We're constantly surprised by how good IONIX is at detecting timely vulnerabilities. If things were to happen today, I would likely get a report tomorrow. IONIX is staying on the cutting edge to help us detect emerging threats on our attack surface..”

Verified user
AVP, Cyber Security at a insurance company with 10,001+ employees

Read full review

“The integration was easy. During the POV they used our IP ranges and ran a scan that barely required any adjustments.

I also like that in addition to the vulnerabilities, they also provide possible solutions..”

Verified user
IT Security Officer at a retailer with 10,001+ employees

Read full review

“IONIX helps us prioritize our primary assets. Its action items are written in simple language, making it easy for our IT team to remove them.

We've integrated IONIX with Splunk with the help of IONIX support, and they were able to do the integration quickly. Their automated vulnerability resolution feature works nicely, but I haven't used it often. The solution has few false positives—maybe one or two per year. .”

Kfir Ernst

IT Administrator/Engineer at a financial services firm with 1,001-5,000 employees

Read full review

Other Solutions Considered

"I evaluated CrowdStrike for a month and did not get the information the IONIX provided within the first five minutes. CrowdStrike requires a long time to set up and collect information.."

Rick Beltran
Director of Cybersecurity at a recruiting/HR firm with 1,001-5,000 employees

Read full review

"We looked at most of them. We went for IONIX because of the most and the best findings prioritized by risk. We found the dark web capability where it can also scrape the dark web incredibly nice.."

Verified user
IT Security Engineer at a media company with 1,001-5,000 employees

Read full review

"I favor IONIX over our previous solution because it offers significantly deeper visibility into findings and also covers a much larger portion of our network. Furthermore, I find IONIX generally user-friendly. It's great to have a dedicated account manager who responds promptly to our inquiries.."

Verified user
IT Security Officer at a retailer with 10,001+ employees

Read full review

"We are using Rapid7 InsightVM, Rapid7 Insights, and Rapid7 InsightAppSec. However, the Rapid7 suite is not able to discover all the assets that IONIX identified. We will not be renewing the contract with Rapid7 because IONIX is much better.

I haven't gotten complete asset visibility with other tools like I have with IONIX. For example, even after eight months of using Rapid7, not all our assets are publicly identified. Similarly, CrowdStrike only shows maybe half of them. With IONIX, however, all our assets were readily apparent.."

Rick Beltran

Director of Cybersecurity at a recruiting/HR firm with 1,001-5,000 employees

Read full review

“I have previously used CyCognito. With CyCognito's recognition of network addresses, we get a tremendous amount of false positives. The difficulty is that I get an overwhelming amount of detection, which we find out does not belong to my organization. That created a lot of conflict between the different teams because it became confusing, and people chased the wrong owners to remediate things that didn't exist in the organization.

The complexity of modern-day environments makes it very difficult for vendors like CyCognito and IONIX to accurately detect and recognize which network resources are owned by clients like me. I think that's the big thing there, and the rest are somewhat similar.

There's seemingly very good marketing about the effectiveness of many other vendors. Once organizations like mine go and test out and use different vendors, the results are very, very clear. We get to know which vendor is going to be able to distinguish those really, really, really confusing details and make it accurate..”

Verified user

AVP, Cyber Security at a insurance company with 10,001+ employees

Read full review

ROI

Real user quotes about their ROI:

"We have seen a return on investment in terms of identifying risks that we need to work on immediately. It has definitely helped us take care of some of the risks in a prioritized way.."

Verified user
IT Security Engineer at a media company with 1,001-5,000 employees

Read full review

"In terms of return on investment, we've significantly improved what we were aiming for. This includes a minimal setup time, minimal training time, and the elimination of effort needed to convince stakeholders to use IONIX. Its simplicity means they can take action immediately. We can then rescan and instantly assess our risk score. This rapid risk evaluation is important to us.."

Rick Beltran
Director of Cybersecurity at a recruiting/HR firm with 1,001-5,000 employees

Read full review

Use Case

“We are using IONIX to scan our public network ranges for vulnerabilities as part of our external technology service management.

We implemented IONIX after our previous supplier discontinued their services..”

Verified user
IT Security Officer at a retailer with 10,001+ employees

Read full review

“It is an attack surface management tool. We use it to detect unknown assets actively exposed to the Internet.

We wanted to look for threats that were exposed to the Internet that we did not know about. We were looking for those unknown things out there on the Internet. We were trying to make sure that we knew what our attack surface looked like from an outside point of view. We were looking for a platform to identify that..”

Verified user
IT Security Engineer at a media company with 1,001-5,000 employees

Read full review

"IONIX enhances our understanding of our attack surface by revealing both known and unknown aspects of our systems. This insight helps us anticipate the various tactics attackers might use to penetrate our network. With IONIX, we can evaluate the risks associated with vulnerabilities in our internal systems.

Moreover, the recent addition of a threat sensor feature enables us to prioritize these risks more effectively.."

Verified user

Director - IT Security Services at a insurance company with 10,001+ employees

Read full review

"We use IONIX to gain visibility into our external attack surface. This allows us to see our organization from an attacker's perspective, identifying potential vulnerabilities. By exporting reports, we can effectively communicate these risks to key stakeholders, enabling them to take proactive measures to mitigate them.

The most important thing was to identify all our public-facing systems. In other words, any systems that the public could access. Once I had that list, my priority was to ensure their security. That meant making sure they were free from vulnerabilities. Next, I wanted to have actionable intelligence on any vulnerabilities we found. This way, I could send it directly to the system owners, who could then take immediate action to fix the problems. The IONIX platform has been instrumental in achieving this. On the very first day, I got access, we were able to identify and address two critical vulnerabilities within just five minutes! Additionally, we discovered a public-facing system that we weren't previously aware of. Overall, it's been a very impressive tool.."

Rick Beltran

Director of Cybersecurity at a recruiting/HR firm with 1,001-5,000 employees

Read full review

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

"The initial setup was a breeze. It only took five minutes to complete. All I had to do was click a link and follow the prompts. Within five minutes, I was online and able to explore the IONIX platform. I even exported a CSV report and forwarded it to our infrastructure team. They were then able to address two critical vulnerabilities – all within that same five-minute window! After over 20 years in this industry, it's truly exciting to use a system that requires zero configuration on my end.."

Rick Beltran

Director of Cybersecurity at a recruiting/HR firm with 1,001-5,000 employees

Read full review

“The solution's initial deployment depends on the organization's understanding of the environment. For us, the initial deployment was reasonable. I would not say it's easy, but it requires a certain amount of understanding. For example, we need to know our IP address spaces. IONIX will provide a list of assets like IP addresses and check if they belong to us. If we're not able to identify them, or if we're not even able to know our organization's structure, then it would be very difficult.

It comes back to whether the people working with IONIX understand their environment. If they do not understand the environment, it would be very difficult. It's not a technical thing but more of an organizational thing. For example, when IONIX asks us if a company is one of our subsidiaries, we immediately know that it is, and in some cases, it isn't. That's the level of work effort that is required.

It depends on the organization operating it and who is actually in the driver's seat working on it. If we put the most junior person who's new to the organization, that would have become very hectic. Luckily, we initially put some very senior people into it, and we were able to work very quickly. Some investment of time and effort are required..”

Verified user

Read full review

AVP, Cyber Security at a insurance company with 10,001+ employees

Customer Service and Support

“I rate IONIX support nine out of 10. I'm satisfied with their service. They have resolved every ticket I've opened and given me all the answers. If we need additional assistance, they will contact their developers and product team to help us understand something. .”

Kfir Ernst

IT Administrator/Engineer at a financial services firm with 1,001-5,000 employees

Read full review

“Our bi-weekly meetings with their technical support are a great way to discuss and address desired platform improvements. Their dedication to client success is truly impressive, making them a valuable resource..”

Verified user

Director - IT Security Services at a insurance company with 10,001+ employees

Read full review

"Technical support is not something we reach out to because we work in a partnership methodology, where we have regular standing meetings with IONIX's support team. We already have standing meetings at regular intervals, and we review not just issues we have but also the reporting that they provide. This helps us ensure that we fully understand all the reporting and monitor the situation or the attack surface as a result. The technical support benefits us only because we invest time into it.."

Verified user

AVP, Cyber Security at a insurance company with 10,001+ employees

Read full review

"The technical support team impressed me with their ability to identify a common thread. We have three websites that essentially serve the same purpose. The team recognized that a single action taken across all three sites would minimize the risk. In other words, their assistance wasn't limited to just one website; they identified a vulnerability that spanned all our assets. That's what makes them truly amazing. Their response time is almost instantaneous.."

Rick Beltran

Director of Cybersecurity at a recruiting/HR firm with 1,001-5,000 employees

Read full review

"They are slow and not the best. If we want to get more information on a particular finding, it is not ideal at times. It seems like they do not have the expertise on the line to get some of the more pointed answers. Also, from the speed, it feels like a weekly cadence as opposed to a daily cadence.

I would rate their support a five out of ten. They are responsive, and they finally get to the answers, but they are not the fastest and the most detailed. Their support needs improvement.."

Verified user

IT Security Engineer at a media company with 1,001-5,000 employees

Read full review

Other Advice

“It's not just whether it recognizes the vulnerability we care about but where those vulnerabilities occur. If it is not mine, I cannot take action. Reporting it to me makes no sense, and it would only waste my time and cause a lot of confusion. I would say reducing false positives is a big deal.

Overall, I rate the solution a nine out of ten..”

Verified user
AVP, Cyber Security at a insurance company with 10,001+ employees

Read full review

“I would rate IONIX nine out of ten.

No maintenance is required from our end.

The key to effectively prioritizing risks lies in understanding the data IONIX provides. This data needs to be actionable, meaning it should tell you what issues to address first. By thoroughly grasping the information, you'll be able to make informed decisions about which risks your team should focus on resolving..”

Verified user
Director - IT Security Services at a insurance company with 10,001+ employees

Read full review

“I would rate IONIX ten out of ten.

I was on the implementation team for the IONIX deployment. I am also an admin and user of IONIX.

The only aspect of IONIX that I consider to be maintenance involves taking action to rescan the system whenever a vulnerability is identified.

For anyone considering IONIX, I recommend adopting a security-focused mindset. This tool empowers you with clear instructions to address potential vulnerabilities that hackers might exploit..”

Rick Beltran
Director of Cybersecurity at a recruiting/HR firm with 1,001-5,000 employees

Read full review

“To those evaluating IONIX, I would advise to definitely understand what their risk tolerance is and make sure they are seeing the value in a tool like this upfront before purchasing. They should make sure that they are seeing the things that they would expect to see out of a tool like this, especially if they are coming from nothing at all.

IONIX's action items are written in simple language so that IT personnel can fix them, rather than needing security experts to do so, but they are a little bit lengthy in some cases. You can get to the resolution without the help of the security team. However, you would need to summarize some of that before giving it to someone who does not know anything about it. It is very lengthy. The descriptions are very verbose.

For communicating to our organization’s executives, we are just using severities. It does help at a high level, but the executives do not go into the platform.

I would recommend IONIX to others. I would rate it an eight out of ten..”

Verified user
IT Security Engineer at a media company with 1,001-5,000 employees

Read full review

“I would rate IONIX a nine out of ten.

IONIX can provide automated integration into our SOC tools but we can't take advantage of this because our infrastructure is on-premises and they mainly connect to cloud services.

We currently have some processes in place that are proving difficult to manage effectively. One challenge is the high volume of project work, which often delays the prioritization of identified vulnerabilities. However, we are actively working on improving our system to prioritize these vulnerabilities and reduce our mean time

to remediation.

We have eight people that use IONIX all from the same team.

The only maintenance required is keeping track of the domains being scanned. We can add new domains to the list of scanned objects when needed.

I recommend IONIX to others, but it depends on the customer's specific needs. A proof of concept is advisable..”

Verified user
IT Security Officer at a retailer with 10,001+ employees

Read full review

Top Industries

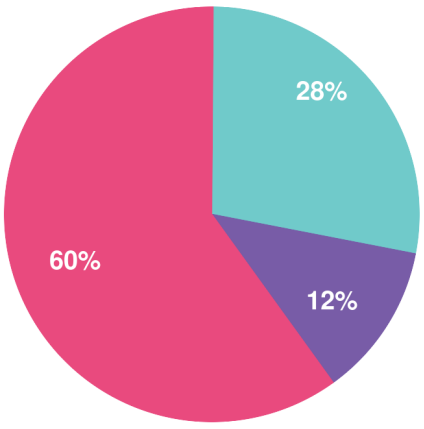
by visitors reading reviews

Financial Services Firm	12%
Insurance Company	11%
Manufacturing Company	9%
University	8%

Company Size

by reviewers

by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944