IONIX

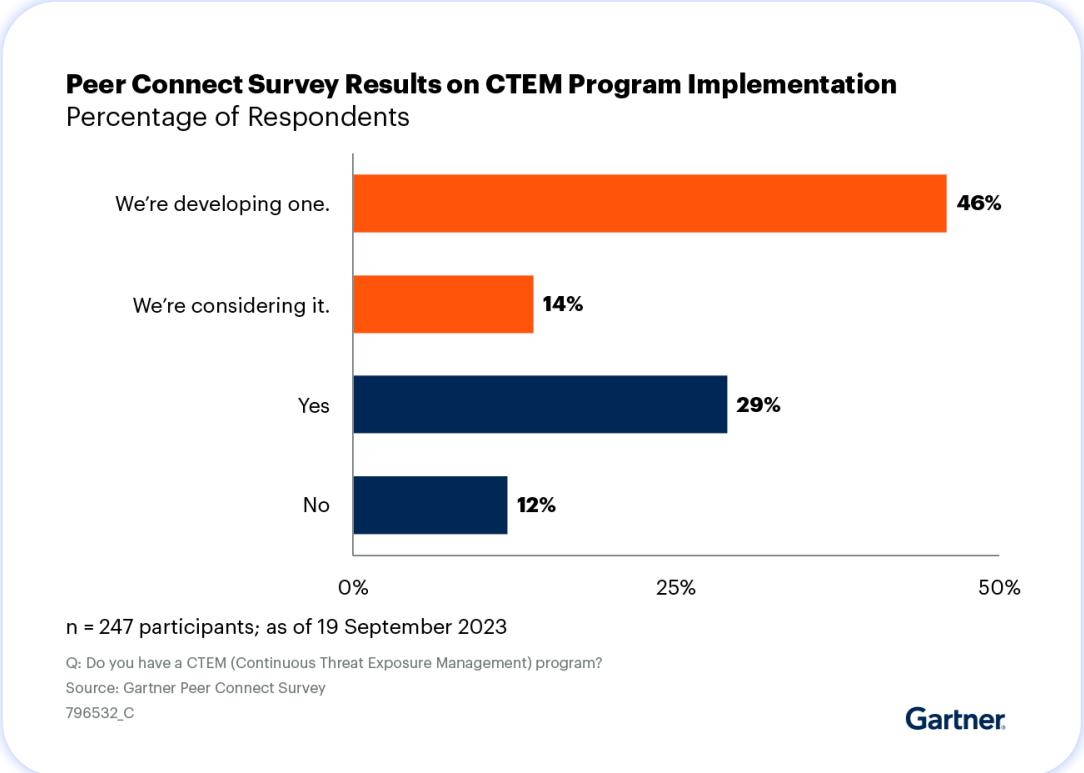
WHITEPAPER

ADDRESSING CONTINUOUS THREAT EXPOSURE MANAGEMENT (CTEM) WITH IONIX

A Proactive Approach to Exposure Management using Context-based Prioritization and Exploit Validation to Mitigate Risk

This white paper provides insights into how industry experts and analysts view taking a more comprehensive, proactive approach to managing cybersecurity exposures. We explain how a new framework known at CTEM – Continuous Threat Exposure Management – can address the need for better security. We also cover how IONIX customers are shifting from a reactive to a proactive approach by continuously identifying, evaluating, and mitigating potential threats.

Is your company considering a CTEM approach? From the Gartner survey data below, it seems many are considering a shift to proactive exposure management. This white paper will help you to understand how to approach CTEM in ways that your team can implement effectively.



THE ATTACK SURFACE GAP

In today's digital landscape, organizations face a growing array of sophisticated cyber threats. The attack surface is expanding, becoming harder to manage, with ESG research indicating a 5.5% monthly fluctuation. Security teams, tools, and processes are also increasing in complexity, creating coverage gaps. How do successful companies manage their attack surface exposure and gain control over tools and processes?

There are several key reasons for the gap:

1. **EXPANDED ATTACK SURFACE**
New technologies like cloud computing and IoT, along with trends like digital transformation, have significantly increased organizations' attack surfaces.

2. **RAPIDLY CHANGING THREATS**
New vulnerabilities, attack methods, and zero-day exploits are frequently emerging, which introduce new types of risks, making it increasingly challenging to defend against cyber threats.

3. **LACK OF CONTEXTUAL AWARENESS**
Traditional tools focus on discovering vulnerabilities but lack overall risk context and business impact, preventing security teams from prioritizing activities based on actual risks.

4. **MORE SOPHISTICATED ATTACKS**
Cyber attackers are adopting new tools and technologies, enabling them to carry out sophisticated attacks that exploit organizational blind spots, causing significant damage.

5. **INSIDE-OUT VIEW**
Cybersecurity tools are focused on protecting the assets that are owned and managed by the organization. With the proliferation of cloud and vendor-managed applications, companies find that in fact, a large percentage of their attack surface consists of internet-facing assets that they don't own or manage themselves.

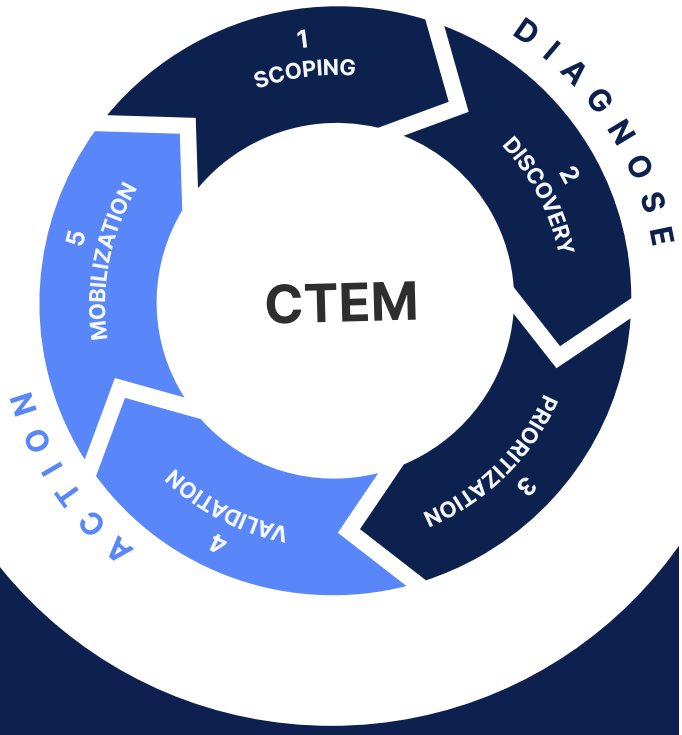
Traditional tools focus on discovering vulnerabilities but lack overall risk context and business impact, preventing security teams from prioritizing activities based on actual risks.

A New Approach is Needed.

As the challenges listed above grow, organizations find that they are taking a reactive tactical approach to managing their risk exposure. They need instead to align teams, tools and processes to a framework that helps prioritize and mitigate risks in a much more comprehensive way.

WHAT IS CTEM?

To help organizations systematically identify, prioritize, and address security exposures, thereby improving their overall security posture, Gartner introduced the Continuous Threat Exposure Management (CTEM) framework. Unlike typical Gartner categories that are defined by software tools in a given practice area, CTEM is a framework and encompasses many disparate cyber tools and processes. Ideally, a CTEM program enables the shift from reactive measures to a proactive, ongoing process of identifying and mitigating potential security exposures. This comprehensive framework encompasses five key stages: scoping, discovery, prioritization, validation, and mobilization.



1. SCOPING

Defines the boundaries of an organization's attack surface. It represents a comprehensive view of digital assets, including traditional infrastructure and cloud resources. It reflects the organization's critical business operations and risk landscape, providing the context for ongoing threat exposure management.

2. DISCOVERY

Identifies and catalogs assets within the defined scope, building comprehensive risk profiles which incorporate potential vulnerabilities, exposures, and security posture. This provides a foundation for risk-based decision-making in subsequent stages.

3. PRIORITIZATION

Prioritizing exposures based on urgency, severity, existing controls, and overall risk to the organization, this approach focuses on high-value assets and critical business systems, providing a clear rationale for prioritization decisions.

4. VALIDATION

Confirms that attackers can exploit exposures and assesses the system's response to such attacks. This validation involves automated simulations along with manual assessments. It allows for understanding the actual risk and verifying the effectiveness and feasibility of suggested remediations.

5. MOBILIZATION

Ensures that security teams effectively operationalize the findings from previous stages by defining communication standards and establishing documented cross-team approval workflows, which include approval, implementation processes, and mitigation deployments.

ASM IS A GOOD STARTING POINT FOR CTEM

So, if we want to begin a CTEM Program, where do we begin?

Attack Surface Management tools have exploded in usage and popularity over the last five years. Most companies that have implemented ASM, or often EASM (tools that focus on external assets) as part of their cyber tooling are using it to ensure that their internet-facing assets have been scanned and inventoried. However, in recent years ASM has evolved considerably, and now represents an ideal place to begin a CTEM program. The following are the features of mature ASM programs:

NARROWER SCOPE WITH SIGNIFICANT IMPACT

EASM focuses on the external-facing assets of an organization. This provides a relatively narrow scope, making it more manageable for organizations to start their CTEM journey. Despite its narrower focus, managing the external attack surface is crucial as it's the primary entry point for many cyber threats.

VISIBILITY INTO THE ATTACKER'S PERSPECTIVE

EASM provides insights into how an attacker views the organization from the outside. 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

EASM tools operate from the outside, in a non-intrusive way. They continuously discover and expose risks across organizations internet facing assets and their digital supply chains. By proactively reducing their external attack surface, security teams can quickly demonstrate the value of the CTEM program to stakeholders. This can help in securing buy-in for further expansion and investment in the program.

FOUNDATIONAL FOR FURTHER EXPANSION

EASM helps organizations break security silos by providing a holistic view across their hybrid on-premises and cross-cloud IT environments. Starting with EASM allows organizations to establish foundational processes, workflows, and collaboration mechanisms. Once these are in place, it becomes easier to expand the CTEM program to include other areas.

ALIGNS WITH DIGITAL TRANSFORMATION

As organizations increasingly adopt cloud services, online platforms, and digital interfaces for their operations, the external attack surface becomes even more critical. EASM aligns with the digital transformation trends, ensuring that as organizations evolve, they have the security controls needed to continuously evolve their security posture.

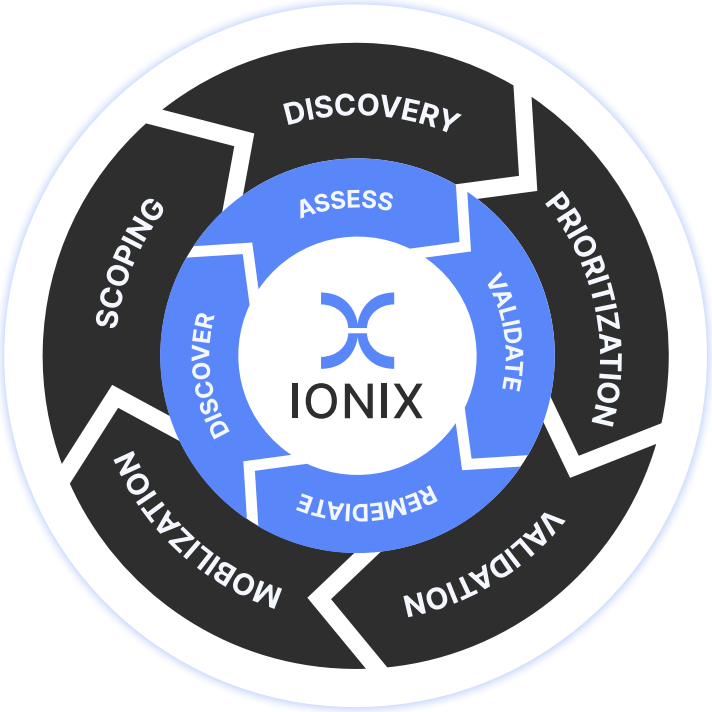
By adopting EASM as the first use case for CTEM, companies can break security silos and gain a holistic view of their attack surface from the attackers' point of view. This is a practical starting point that delivers immediate value while setting the stage for a more comprehensive CTEM strategy.

ADDRESSING CTEM WITH IONIX

IONIX ASM helps companies understand the business context of exposures - ensuring a more thorough and proactive defense strategy, ultimately enhancing overall cybersecurity posture and safeguarding critical assets.

Consider the illustration below to understand how IONIX views both ASM and CTEM on a 'proactive security continuum'. Five years ago, ASM was used only for asset visibility, creating asset inventories and assessing potential risk. As the market consolidated, some held onto their antiquated views of ASM. Today, we see that asset discovery and assessment are just the first step to a proactive security program which includes prioritization of findings, validation of exploits and of course remediation.

> ***"The realization that the number of discovered assets and vulnerabilities is not success itself, accurate scoping based on business risk and potential impact is far more valuable."***
> (Gartner)



1 SCOPING

To effectively identify the business impact during the scoping stage, it's crucial to focus on the widest coverage possible. IONIX creates a wider scope than other approaches by including organizational assets (both cloud and on-prem), vendor-managed assets, third party assets like SaaS services, and even assets connected to those third parties which we refer to as the 'digital supply chain'. By focusing on a much wider scope, IONIX ensures a comprehensive and business- aligned understanding of the attack surface.

2 DISCOVERY

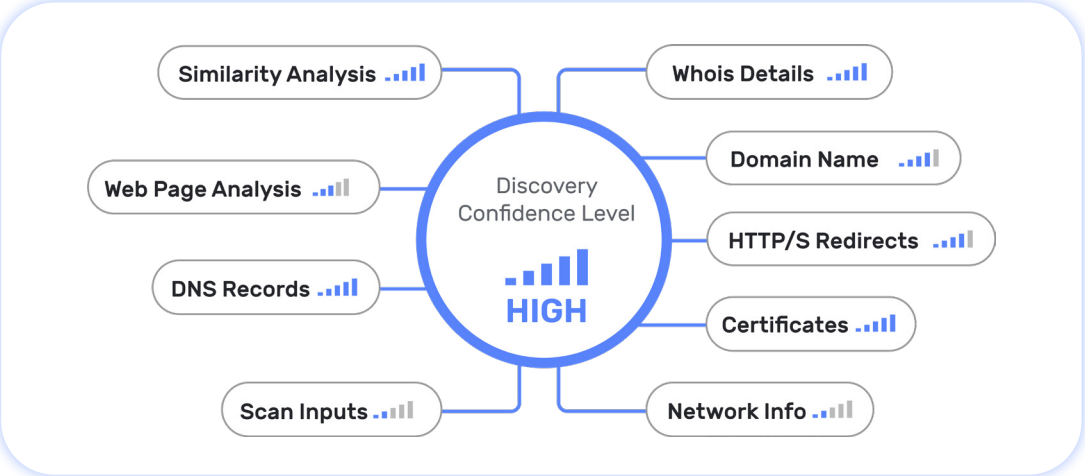
IONIX's multi-layered discovery engine uses connective intelligence and machine learning algorithms across nine distinct discovery methods, enabling it to uncover up to 50% more organizational assets compared to traditional approaches.
It involves the identifying and cataloging of all assets including digital assets, cloud resources, on-premises infrastructure, IoT devices, third-party connections and more.

The platform's advanced attribution techniques minimize false positives, ensuring accurate asset identification. This continuous, adaptive process adjusts to an organization's evolving digital footprint, constantly enhancing discovery capabilities by building on previous findings and incorporating new data.

One of the key capabilities of IONIX Discovery is its Discovery Evidence, which provides clear and understandable visibility into the complex evidence collection and attribution process. Discovery Evidence details the specific pieces of information collected for each asset and their contribution to determining whether the asset belongs to the organization. Evidence is presented in relation to the keywords used during the scoping stage (such as company names, brands, or legal entities) and is compared across the various discovery methods employed by the platform.

IONIX also bridges security gaps, enabling visibility and insights provides systematic discovery of AWS, Azure, and GCP environments, identifying not just the assets but the intricate web of interconnections that could potentially be exploited. This approach transcends the limitations of Posture Management tools like CSPM by incorporating a broader view that includes unintentional internet exposures anddigital supply chain vulnerabilities.

By adopting EASM as the first use case for CTEM, companies can break security silos and gain a holistic view of their attack surface from the attackers' perspective.



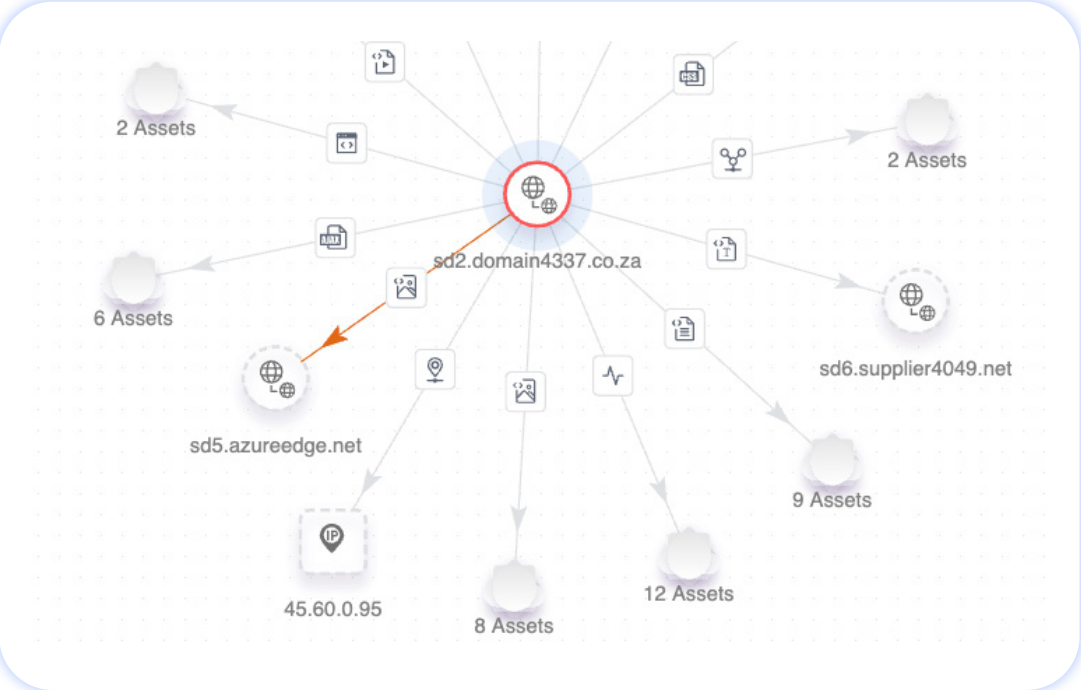
IONIX's comprehensive approach allows organizations to maintain an up-to-date, accurate inventory of their attack surface, understand the reasoning behind asset attributions, and make informed decisions about their cybersecurity posture. By providing this level of detail and transparency, IONIX delivers accuracy with an extremely low rate of false positives.

3 PRIORITIZATION

IONIX 's fresh approach to attack path mapping is built on an understanding of the interdependencies between organizational assets and the impact that each asset has on other assets. We refer to this as 'Connective Intelligence'.

Connective Intelligence suggests that the security posture and risk of a given asset is not only dependent on the security hygiene and posture of the asset itself, but also on the security posture of the assets that it depends upon, directly and indirectly (2nd, 3rd to Nth degree).

Unlike other approaches to attack path mapping, the IONIX approach maps actual, rather than theoretical, dependencies that have been validated for exploitability. Connectivity and dependencies are checked and validated to help customers understand the risks they bring.



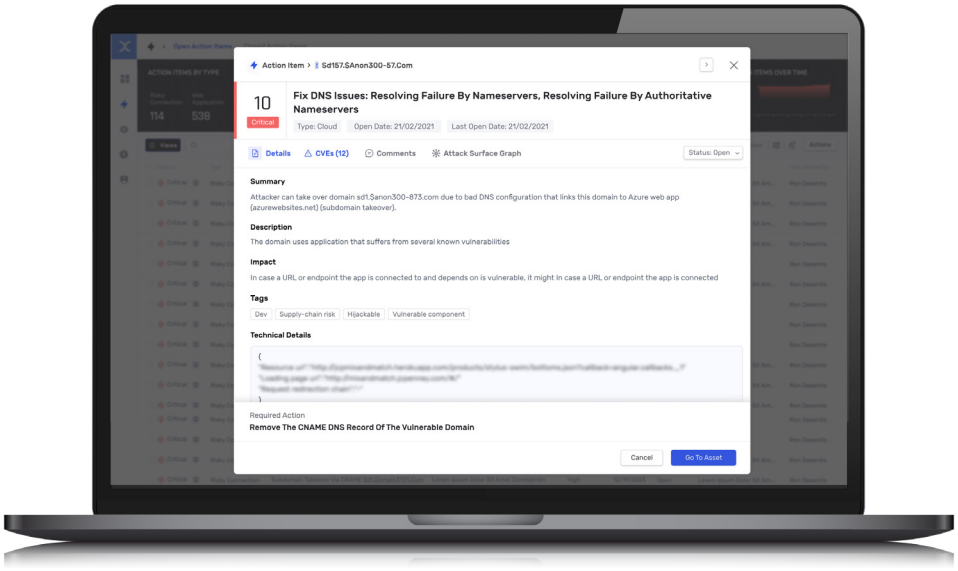
Connective Intelligence from IONIX takes Attack Surface Management to a new level by not only considering discrete assets across the Attack Surface but also highlighting the risks that are introduced by connected assets. Furthermore, connective Intelligence enables not only considering the externally facing assets that are owned or controlled by the organization but also all the 3rd party assets that constitute the digital supply chain.

4 VALIDATION

IONIX Exposure Validation leverages a toolbox of attack simulation techniques to conduct non-intrusive testing of your systems, identifying exposures without the risk of disruption. Our approach validates real-world exploitability, ensuring that security teams can focus on the most significant threats to your business. The key features of IONIX Exposure Validation include:• Non-Intrusive Testing Techniques: Designed to safely validate security controls in operational systems without impacting their functionality or performance.

- Non-Intrusive Testing Techniques: Designed to safely validate security controls in operational systems without impacting their functionality or performance.
- Exploitable Risk Identification: Pinpointing vulnerabilities that pose an actual threat to your organization, so your security teams can accelerate remediation and effectively reduce risk.
- Automated Validation: Continuous security testing that adapts to the evolving threat landscape and organizational changes, ensuring that your defenses remain robust over time.
- Automation and Efficiency: Reducing the need for extensive manual testing, saving time and resources while improving your security posture.

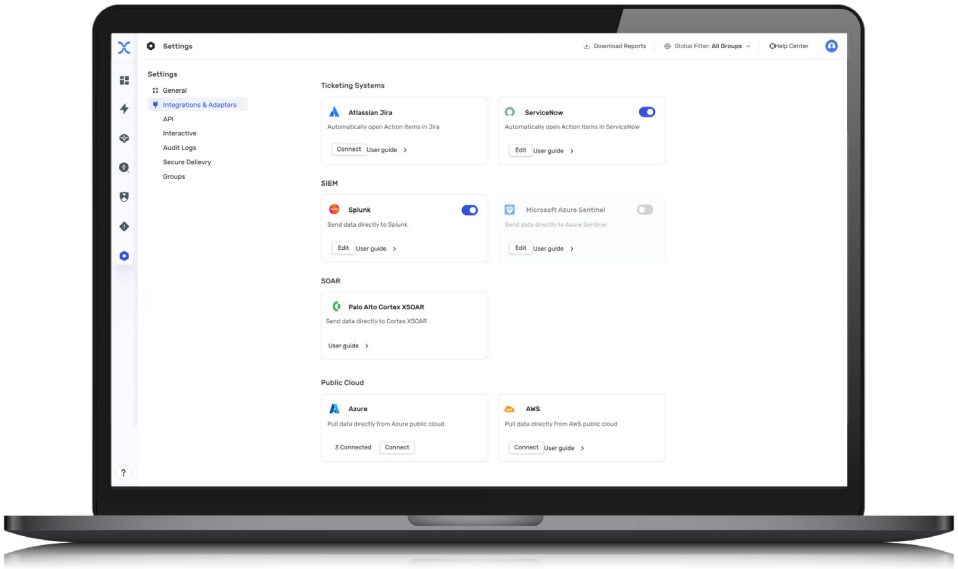
IONIX's continuous and adaptive threat management capabilities help organizations stay ahead of emerging threats, reducing exposure and potential harm.



5 MOBILIZATION

The essence of this stage is ensuring that risks are addressed and routed to the relevant teams for handling and applying the necessary remediation actions. IONIX integrates with security information and event management (SIEM) systems, SOAR, security operations center (SOC) software, and ticketing systems to facilitate the rapid remediation of critical issues.

These integrations enable organizations to optimize their activities regarding associated risks by facilitating effective communication and alignment between security teams and other stakeholders in the organization.



IONIX has also developed two critical features that enable customers to remediate quickly, Action Items and Active Protection. A key aspect of effective remediation is creating robust action items that can aggregate and solve multiple issues at once. Using Connective Intelligence, IONIX can detect that a vulnerability that has been detected across multiple assets (applications, websites, services) is originating from a single asset, thus creating a single Action Item, rather than multiple action items, one for each vulnerable asset.

IONIX is the only EM provider to offer a feature called 'Active Protection' that immediately prevents the high-risk threats that enterprises cannot otherwise address, with no human intervention. Active Protection can identify digital supply chain-related misconfigurations and can automatically neutralize these threats by essentially taking control of the asset until an organization can implement remediation on the asset.

With IONIX, enterprises can effectively manage subsidiaries and other complex organizational structures with a single centralized platform. Our solution provides automated, business-entity attribution combined with access partitioning. It enables local teams to effectively manage their attack surface while empowering centralized SOCs to implement organization-wide security standards. Each subsidiary can have its own security team with dedicated RBAC, while global organization security departments can track the risk exposure and action items across all subsidiaries.

"Exposure management is a platform that consolidates vulnerabilities and exposures with an organizational perspective, maps them on an attack path, and identifies choke points for remediation teams to prioritize."
Eric Nost, Forrester

NOT JUST GARTNER

Analysts are defining Exposure Management (EM) in various ways. Forrester Analyst Eric Nost describes it as a platform that consolidates vulnerabilities and exposures from an organizational perspective, maps them on an attack path, and identifies remediation priorities. Like Gartner, Nost views EM as a holistic approach to discovering, prioritizing, mapping, and remediating exposures. However, he emphasizes the importance of operationalizing remediation to simplify security analysts' workflows.

Implementing CTEM or EM allows businesses to continuously assess their attack surface, identify vulnerabilities, and address critical exposures in real-time. This approach helps organizations stay ahead of emerging threats, reduce overall risk, and maintain robust security.

SUMMARY

IONIX helps with CTEM implementation by offering solutions geared towards each stage of a CTEM program, including scoping, discovery, prioritization, validation and mobilization.

1. Comprehensive Asset Visibility: IONIX ensures no critical assets are overlooked, providing a complete view of the organization's attack surface, essential for effective exposure management.
2. Accurate Risk Prioritization: By minimizing false positives and validating suspected exposures, IONIX helps organizations focus on genuine threats, directing security resources toward the most significant risks.
3. Business-Oriented Approach: Integrating business context into scoping and risk assessments, IONIX ensures security measures align with business priorities, protecting critical functions.
4. Proactive Threat Management: IONIX's continuous and adaptive threat management capabilities enable organizations to stay ahead of emerging threats, reducing exposure and potential harm.
5. Simplified Operational Tasks: By helping security teams manage risk by subsidiary, grouping remediation recommendations into action items and integration with most popular SOC management tools, IONIX provides superior operational support.

IONIX ensures that organizations can implement CTEM effectively, achieving robust and business-aligned cybersecurity defenses that safeguard critical assets and maintain operational integrity. Contact IONIX for a demo today!

GET STARTED TODAY

Contact our team to get a free scan.
Get a free scan | Learn more at ionix.io