IONIX

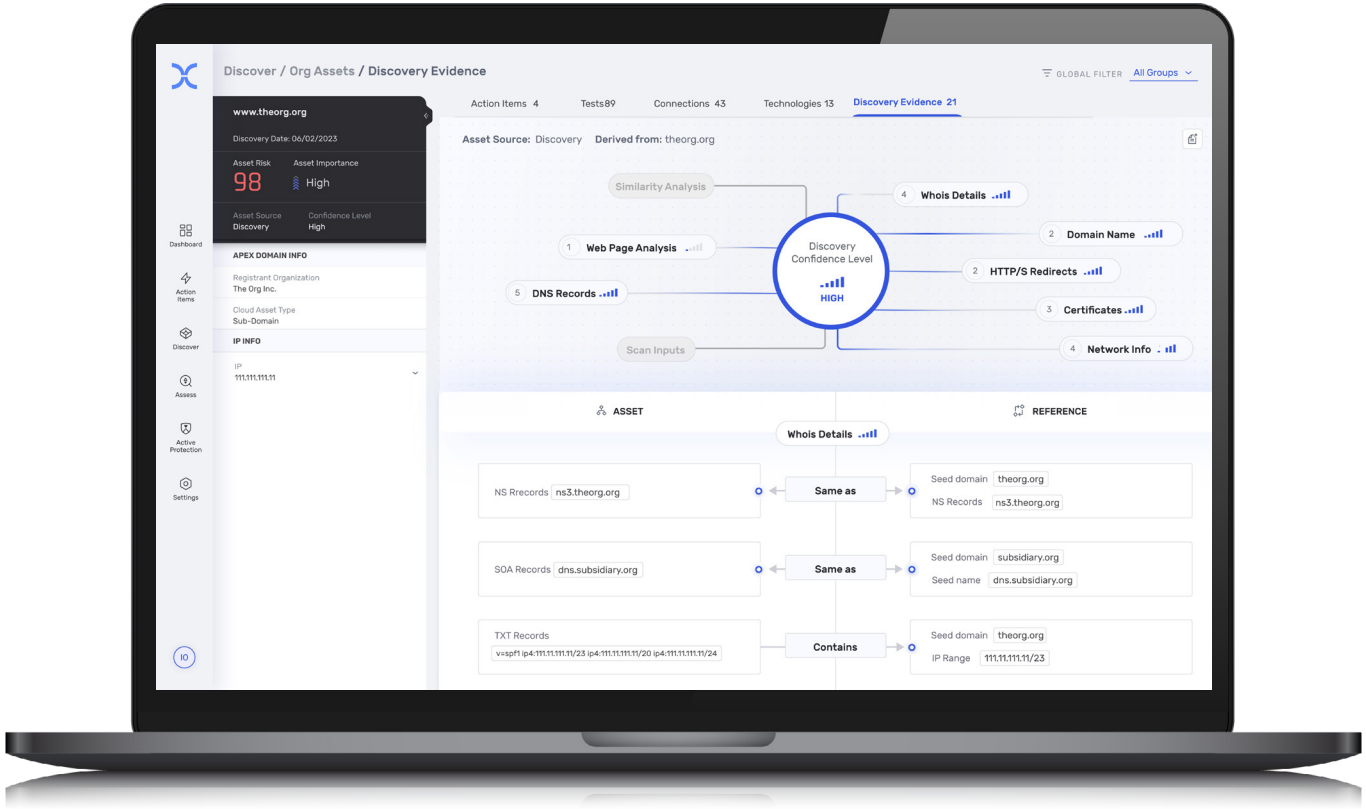
FEATURE OVERVIEW

IONIX DISCOVERY EVIDENCE

COMPREHENSIVE ASSET ATTRIBUTION WITH A CLEAR UNIFIED VIEW SETS A NEW STANDARD

Maximize coverage and minimize noise with IONIX multi-factor discovery and attribution

- **Discover more** with multi-factor attack surface discovery
- **Integrate all** discovery evidence for high-precision attribution
- **Continually improve** with machine learning models



IONIX'S MULTI-FACTOR APPROACH REDEFINES ASSET DISCOVERY AND ATTRIBUTION

Using multi-factor asset discovery and attribution, IONIX Attack Surface Management delivers unmatched coverage and precision. This approach overcomes the limitations of traditional methods to provide a more comprehensive and accurate identification of organizational assets across diverse IT environments. IONIX's unified, multi-factor evidence view provides security teams with the tools they need to gain a deeper and more reliable understanding of asset attribution across their organization's digital footprint.

THE COMPLEXITY OF ATTACK SURFACE DISCOVERY

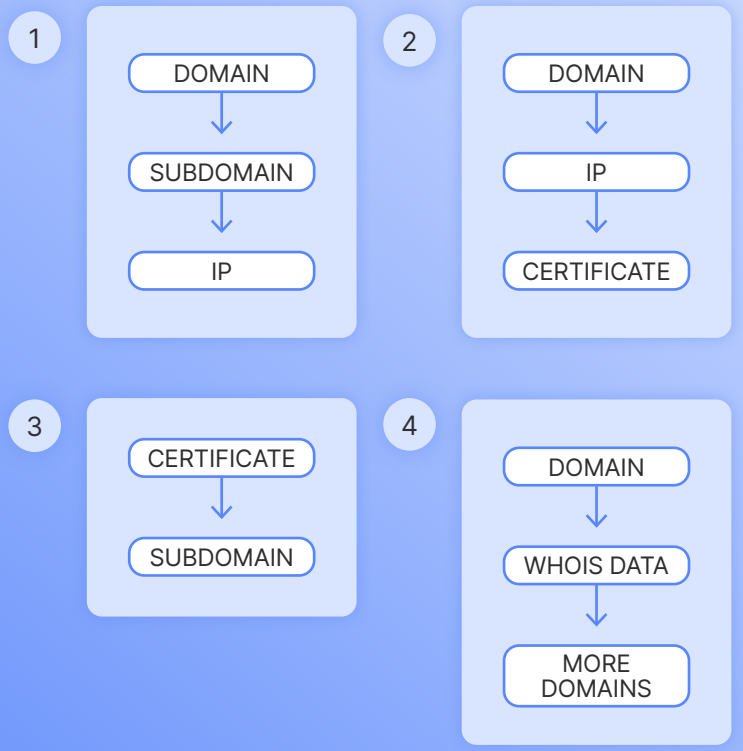
The dynamic nature of modern enterprises creates a complex and expanding digital footprint making it increasingly challenging to discover. An organization's attack surface spreads across diverse IT environments – on-premises, cloud infrastructure, vendor managed platforms, hosted/SaaS services, and shadow IT. There is no single source, or even multiple sources, that consolidate a complete inventory of an organization's internet facing assets.

SIMPLISTIC DISCOVERY APPROACH

Many Attack Surface Management solutions employ a simplistic approach to discover organizational assets. They identify assets through linear and deterministic paths derived from individual seed assets.

This is a safe yet limited approach that introduces few false positives, but suffers from many false negatives (blind spots). Such a simplistic approach is unable to detect less-obvious assets. For example, domains with no indicative 'Whois' record might be overlooked, even if they have other attributing properties such as metadata or certain visual elements.

SIMPLISTIC DISCOVERY PATHS



In simplistic discovery, every asset is attributed in a direct path to a single seed asset.

IONIX ATTACK SURFACE DISCOVERY

IONIX's multi-layered discovery engine creates a comprehensive inventory of your external attack surface from the attacker's point of view. Using connective intelligence and machine learning that combine 9 discovery methods, IONIX discovers up to 50% more organizational assets and minimizes false positives with precise attribution .

IONIX Attack Surface Discovery is a continuous process that automatically adapts to the dynamic changes across an organization's attack surface, deepens the discovery, and improves accuracy. Every iteration draws from the discovery sources and previous findings to collect asset candidates, validate attribution, and enrich context.

IONIX DISCOVERY EVIDENCE

Why does an asset belong to my organization? How did IONIX make the attribution decision? IONIX Discovery Evidence provides security professionals with easy-to-understand visibility into the evidence collection and attribution process. This unified view goes beyond simplistic linear attribution evidence reflecting the multi-factor complexity of asset discovery and attribution.

IONIX Discovery Evidence demonstrates the specific evidence collected on an asset and how this information is integrated into the conclusion that an asset belongs to the organization. The evidence is presented in relation to a seed asset or keyword (company/brand/legal name etc.) and compared across the discovery methods.

IONIX DISCOVERY METHODS

WHOIS RECORDS

Extracting details from the various fields of an asset's Whois record to identify ownership and other relevant information.

DNS RECORDS

Investigating records like nameserver, SOA, MX, etc., for hidden details that might indicate asset ownership or association.

CERTIFICATES

Utilizing details from asset certificates, such as organization names and common names, to establish connections and ownership.

WEB PAGE

Rendering a domain's HTML content, metadata, and visual elements to uncover subtle indications of asset ownership.

NETWORK INFORMATION

Analyzing IP records and CIDRs associated with the domain to map the network footprint of the organization.

HTTP/S REDIRECTS

Investigating URLs that redirect to the asset for indicative names that might reveal ownership or association.

DOMAIN NAMES

Examining Domain URLs to uncover related terms, names, or identifiers embedded within them providing insights and significance.

SIMILARITY ANALYSIS

Comparing elements, whether visual or otherwise, for similarities that might indicate common ownership or association.

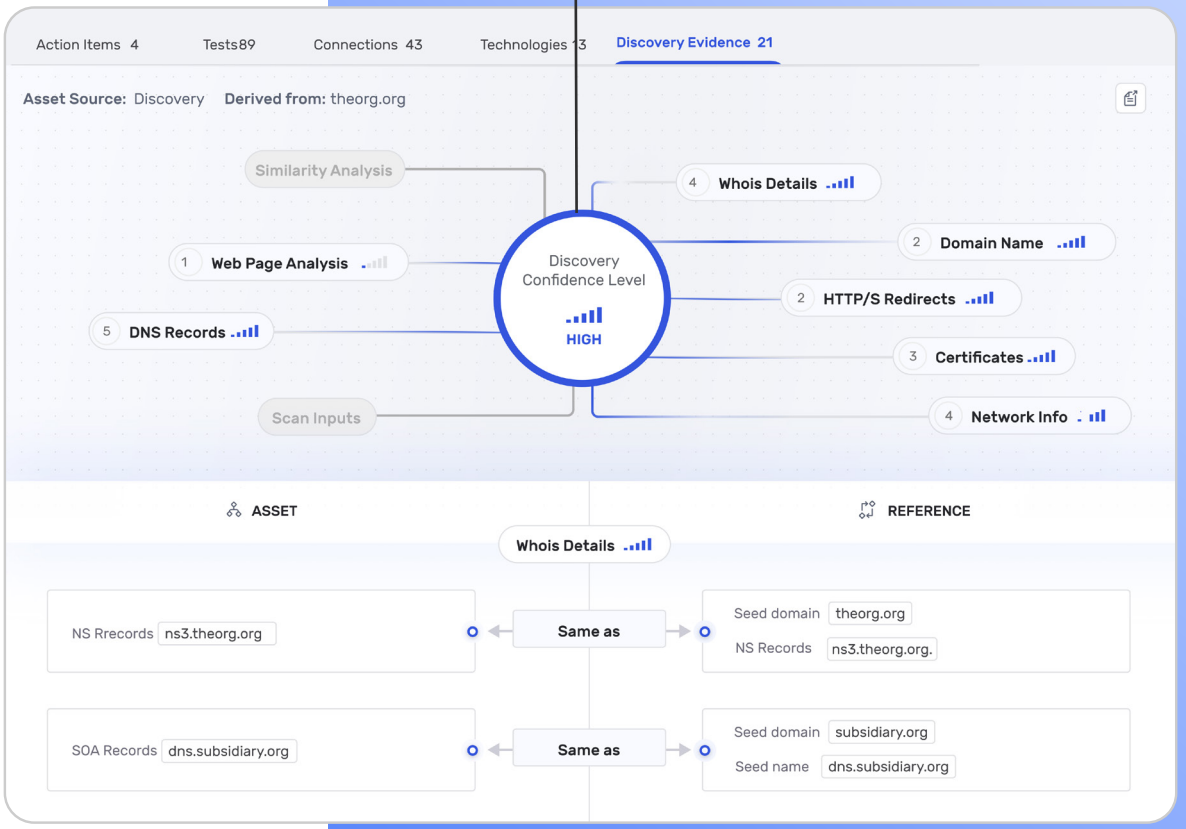
CUSTOMER INPUT

Incorporating data provided by the organization, such as domain names or brand names, to enhance the discovery process.

1. The integrated confidence level in the attribution of the specific asset, based on all the evidence.

2. The number of indicators found in discovery and level of attribution confidence per discovery category.

3. Detailed view of attribution indicators per discovery category. Each piece of evidence is provided as an asset and the attribution reference.



Feature Overview: Discovery Evidence

IONIX