



CONTINUOUS THREAT EXPOSURE MANAGEMENT

Continuous Visibility Across Your Attack Surface

Discover internal exposure, internet-facing assets, and emerging risk before attackers do

From Attack Surface Visibility to Exposure Intelligence

Organizations do not have a static attack surface. New devices, applications, services, users, cloud workloads and configuration changes continuously create new exposure. Periodic assessments can miss assets and weaknesses that appear between reviews.

Underscore's Adversity Discovery Assessment (ADA) is a Continuous Threat Exposure Management solution that continuously discovers internal assets and exposures, identifies vulnerabilities and risky conditions, detects threats with honeypots, and prioritizes risk using exploit likelihood, asset criticality and business impact.

ADA extends exposure discovery beyond internal infrastructure with Internet-Based Organizational Asset Intelligence. Starting with an IP prefix, IP address, domain or subdomain—or a keyword or identifier—security teams can discover related internet-exposed assets, URLs, documents and potentially sensitive information with contextual risk indicators.

Benefits

- Maintain continuous visibility into internal and internet-exposed attack surfaces.
- Discover unknown, unmanaged and related assets before they become blind spots.
- Prioritize remediation using exploit likelihood, asset criticality and business impact.
- Identify exposed sensitive information and organization-related documents through Internet search.
- Reduce ongoing compliance costs with a single source of truth

Core Capabilities

Continuous Asset Discovery

- Continuously discover users, endpoints, servers, applications and infrastructure across the internal environment.
- Identify hidden and rogue assets across wired and wireless networks.
- Perform service and port discovery plus OS and device fingerprinting to understand what is connected and exposed.

Internal Exposure & Vulnerability Discovery

- Identify lateral movement paths, privilege escalation opportunities, vulnerable systems and unmanaged assets.
- Detect network segmentation weaknesses, known vulnerabilities, misconfigurations, weak authentication controls and high-risk services.
- Assess exposure without touching production systems through non-intrusive risk assessment.

Internet-Based Organizational Asset Intelligence

- For an IP prefix, IP address, domain or subdomain, identify related and exposed domains, subdomains and other associated assets.
- Surface relevant intelligence about information publicly available or accessible through the Internet and what an external party could discover about the organization.

Keyword-Based Internet Search & Exposure Discovery

- Search the Internet from the ADA interface using an organization-related keyword, identifier or term.
- Identify URLs where the keyword appears, with a risk severity rating for each finding.
- Surface potentially exposed sensitive information such as Aadhaar, PAN, passport, driving-licence, email and phone details, along with related documents and contextual information.

Risk-Based Prioritisation

- Prioritize risks using exploit likelihood, asset criticality and business impact.
- Focus remediation on exposures most relevant to the organization instead of treating every finding equally.
- Track exposure reduction over time to measure the effectiveness of remediation.

Threat Detection with Honeypots

- Deploy honeypots to detect attacker activity and identify active threats inside the network.
- Capture attacker behaviour and support faster investigation of suspicious activity.

Threat Intelligence Correlation

- Correlate threat intelligence with discovered assets and vulnerabilities to identify emerging threats and relevant exposure.
- Enhance risk understanding with context specific to the organization, industry or region.

Continuous Monitoring & Actionable Analytics

- Monitor changes in the attack surface and surface critical changes or potential threats through alerts.
- Turn complex exposure data into actionable risk intelligence and support reporting for security teams.

Key Advantages

Feature	Value Delivered
Complete Attack Surface Visibility	Continuously discovers internal assets, hidden infrastructure, services, applications and exposure conditions.
Internet Exposure Intelligence	Maps related public-facing domains, subdomains and associated assets from IP and domain-based inputs.
Sensitive Exposure Discovery	Searches the Internet for organization-specific keywords and surfaces potentially exposed PII, documents and contextual risk information.
Risk-Based Prioritisation	Focuses remediation on exploit likelihood, asset criticality and business impact.
Threat Detection with Honeypots	Detects attacker activity and provides visibility into active threats and attacker behaviour.
Non-Intrusive Assessment	Assesses vulnerabilities and exposure without touching production systems.
Continuous Monitoring	Tracks changes in the attack surface and supports ongoing exposure reduction.
Actionable Analytics	Converts complex discovery and exposure data into clear, actionable risk intelligence.
High-Fidelity Assessment	Uses multi-vector detection and threat context to improve the relevance of risk findings.

About Underscore:

Contact Us: