Recorded Future®

DATA SHEET

Attack Surface Intelligence Module

Discover and Defend Your Changing Attack Surface

Challenge

Digital transformation initiatives have resulted in assets being scattered across the internet. Often created without proper security oversight or hygiene, many internet-facing assets are left forgotten and unsecured. This results in security teams operating with limited visibility into their attack surface, causing delayed responses to critical vulnerabilities, a backlog of exposures to remediate, and an unclear picture of what needs to be prioritized.

Due to a lack of visibility or context, 76% of organizations have experienced some type of cyberattack in which the attack itself started through the exploit of an unknown, unmanaged, or poorly managed internet-facing asset (Enterprise Strategy Group). You can't defend what you can't see.

Solution

Recorded Future Attack Surface Intelligence helps organizations confidently reduce risk by improving asset visibility, prioritizing exposures to address, and enforcing security controls. Backed by the world's largest repository of present and historical DNS data, Attack Surface Intelligence presents security teams with a real-time view of an organization's internet-facing assets, and actionable insights on associated exposures to help stay ahead of changes, anomalies, and vulnerabilities across their attack surface.

Stop relying on cobbled together technologies and manual processes to protect your attack surface.

Asset Visibility

Monitoring an expanding list of external assets has become a major challenge for most organizations. Attack Surface Intelligence provides automated and continuous discovery of internet-facing assets, attributes them to the organization for an up-to-date inventory, and delivers valuable information on each asset for further investigation.

Exposure Prioritization

Most security issues are not a result of zero-day vulnerabilities or advanced attack techniques. They primarily stem from misconfigurations and exposures caused by simple errors. This means organizations require greater insights into whether an asset is vulnerable, risky, or exhibiting irregular behavior. Attack Surface Intelligence detects high risk CVEs, misconfigurations, end-of-life software, and additional types of exposed assets. For each exposure identified, dynamic scoring and evidence are provided to aid in prioritization and remediation.

Key Benefits

- **Automate -** real-time discovery of new internet-facing assets
- **Detect -** Identify visible and hidden assets, vulnerabilities. misconfigurations, and other risks
- **Prioritize -** Address the exposures most likely to be exploited against your organization
- **Integrate -** Plug into your ticketing systems, SOAR platforms, SIEM solutions, or simply export data

Key Capabilities

- Continuous identification of new assets
- Transparent exposure scoring, context, and evidence
- Persistent and prioritized view of the external attack surface
- Access to the largest archive of past and present DNS history
- Support from world-class attack surface experts for onboarding, training, and ongoing support

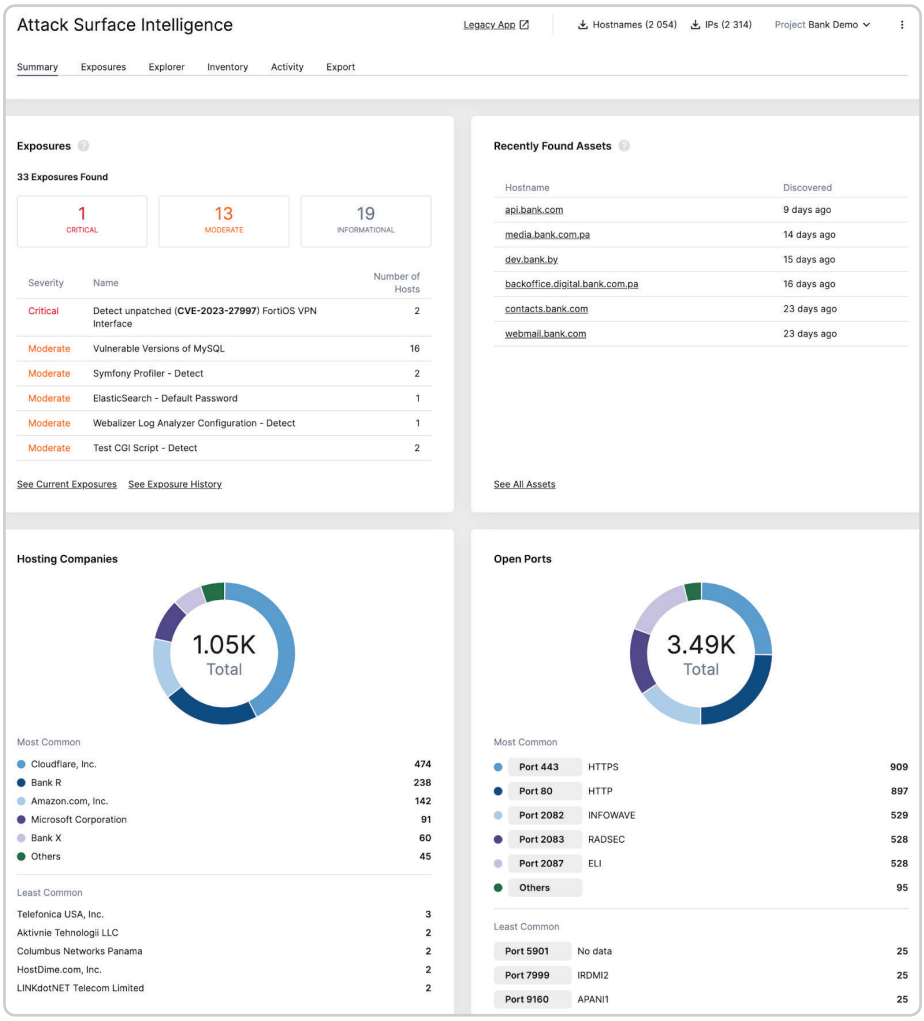
Security Controls Enforcement

Organizations invest significant time and effort creating security policies meant to safeguard their operations. However, modern technology enables employees to spin up new assets, oftentimes outside the purview of IT. Attack Surface Intelligence provides an automated and real-time stream of new internet-facing assets and details as to whether assets adhere to the appropriate policies and standards. For example, are assets being hosted by the right provider? Are they behind a web application firewall (WAF)? Are any administrative panels exposed to the public internet? If assets fall out of policy, visibility ensures they're quickly put back in a defensible position.

Trusted to Protect an Expanding Attack Surface

A Fortune 500 Financial Institution was running a vulnerable version of WordPress, allowing unrestricted file upload and remote code execution. Attack Surface Intelligence automatically surfaced the domain owned by the client, and assigned a critical risk score. Visibility into this domain enabled the company to immediately flag for internal investigation and remediation.

A Fortune 500 Beverage Company relies on a decentralized marketing team that often creates new internet-facing assets without proper hygiene and alerting. With Attack Surface Intelligence the company can easily track when new assets are created. Visibility also helps them improve their efforts to maintain domain hygiene and remove associations from divested brands.



Forgot static lists, manual processes and human audits. Attack Surface Intelligence provides real-time insight on internet-facing assets and supports exposure management across the business.

ABOUT RECORDED FUTURE

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,700 businesses and government organizations across more than 75 countries.

www.recordedfuture.com @RecordedFuture