Attack Surface Management

Gain a real-time prioritized perspective on vulnerabilities targeted by potential attackers

Move your security from reactive to proactive

The digital landscape is a sprawling ecosystem, and every connection, device, or application is a potential entry point for cyber adversaries. Without a clear understanding of your digital footprint, you're navigating in the dark.

An organization's attack surface encompasses more than just vulnerabilities within its hosted services or applications; it includes the applications they utilize as well. A comprehensive attack surface assessment paints a holistic picture of enterprise assets, users, and weaknesses. By identifying actively leveraged weaknesses, it provides a manageable list of priorities for remediation, streamlining the process.

Underscore **Adversity Discovery Assessment (ADA)** offers structured insight in the realm of risk management, providing clarity amidst complexity. It empowers enterprises to make informed decisions regarding their security priorities, effectively reducing risks and fostering cyber resilience.

Benefits

- Gain real-time visibility into your attack surface's vulnerabilities and changes.
- Expedite incident response with actionable threat intelligence.
- Prioritize remediation efforts based on business risk.
- Reduce mean time to remediation.
- Automate your cybersecurity with an easy-to-use platform.
- Benefit from robust reporting capabilities.
- Reduce ongoing compliance costs with a single source of truth

*

Key Features

Real Time Monitoring
Continuously monitor changes in your attack surface, ensuring you are promptly alerted to new vulnerabilities, misconfiguration.

Complete Visibility
Discover all assets, including those in the cloud, forgotten infrastructure, unintended gaps.

Stronger Security Posture
Reduce risk and fix issues that provide measurable results for your security program.

Seamless Scalability
Discover and assess multiple attack surfaces from one interface.

Security Automation
Create alerts for new anomalies and automate key cybersecurity risk management functions.

Risk Intelligence Insights
Automatically applied to the attack surface to determine what is exposed & continuously monitor risk.

Real Time Alerts
Receive alerts for critical changes and potential threats allowing for rapid response and mitigation.

Capabilities

Discover, identify & classify – devices, platform/OS and applications automatically across the enterprise network in a non-intrusive manner.

Detects presence of malicious insiders and target applications and services

Determines, correlates & priorities weakness in live with the current threat/risk perception

"Network Kill-switch" to forestall offending insiders

Forecasts weakness at great risk of future compromise leveraging activity trend.

Identify risk in wireless networks

Identify risk potential using OSINT