Three Cyber Attack Surfaces: Monitoring, Mitigation and Remediation

External Attack Surface

An organization’s external attack surface compromises the points on its digital perimeter that are vulnerable to penetration by hackers, including public-facing websites, APIs, cloud services, mobile applications, email servers and third-party services and platforms.

Vulnerabilities in an external attack surface include open or poorly secured ports on network services, weak passwords, unpatched web applications, unsecured third-party tools or software, and misconfigurations in cloud platforms.

Careful management of an organization’s external attack surface discovers vulnerabilities before hackers can exploit them, minimizes risk to its business in the form of data breaches and interruptions in operations, and strengthens its security posture. In addition, many industry regulators require frequent security assessments under GDPR, HIPAA, PCI-DSS and other frameworks.

RECONIZER™’s agentless External Attack Surface Management platform uses AI-based predictive analytics to track and gather data on potential attackers and hackers’ evolving tactics, techniques, and procedures. It scans the digital landscape including hacker forums, social media, and all layers of the web to uncover hidden attack vectors such as leaked data and stolen passwords and Personally Identifiable Information, while reducing false positives to less than 5%.

RECONIZER™ identifies and continuously monitors all external-facing assets and probes for weaknesses with simulated attacks. RECONIZER™ also evaluates the security posture of third-party vendors and partners to ensure they do not introduce threats. Armed with those insights, RECONIZER™’s AI algorithm predicts and detects cyber vulnerabilities and prioritizes them by criticality and severity, then offers strategies and recommendations to remediate them.

Internal Attack Surface

An organization’s internal attack surface comprises the points within an organization's internal network that can be exploited by malicious or negligent employees or contractors who already have some access, or by hackers who made it through the external perimeter.

An unsecured internal attack surface permits attackers to move laterally across systems, exploiting misconfigured permissions, unpatched software vulnerabilities, or weak access controls. It lets them upgrade their privileges, gain further access to sensitive data, and compromise critical systems. Malicious or negligent insiders who already have administrative privileges in a system can misuse their access to steal data, sabotage systems, or plant malware. Systems or devices such as printers, IoT devices, or unsecured databases can become targets for internal exploitation.

Regular internal attack surface assessments can reveal whether sensitive elements of the network are adequately segmented from one another and can help reduce the attack paths available to intruders or insiders and make it harder for them to escalate privileges.

RECONIZER™'s AI-driven Insight platform navigates your network's topography and organizational policies to identify, monitor and patch potential vulnerabilities before they are exploited. It offers visibility and monitoring of a company's shared files and folders to uncover and eliminate malicious content, and maintains vigilance over role and permission configurations to prevent unauthorized access. The AI algorithm prioritizes uncovered vulnerabilities by criticality and severity, and offers strategies and recommendations to remediate them.

Human Attack Surface

The human attack surface is all the ways in which attackers target employees, contractors, or customers to gain access to systems and sensitive data by exploiting human behavior, error and even trust. Humans are the weakest facet of cybersecurity because they can be manipulated or make mistakes, which neutralizes the strongest technical defenses.

In phishing attacks, actors send deceptive emails or messages to trick users into giving up sensitive information such as passwords or personal details. These can be used to strike an organization's internal attack surface. In another technique called social engineering, attackers manipulate victims into revealing confidential information or performing actions that compromise security. For example, they may pose as tech support workers to convince someone to reset a password or provide login details.

Attackers often steal large volumes of user credentials from third-party services, then sell or share the data on the dark web.

Regular cybersecurity training helps staff recognize and report suspicious activities. Employees should be required to use strong, unique passwords on the organization' systems, and should use password managers to generate and store secure passwords and avoid credential reuse. Multi-Factor Authentication should be required on all internal and customer-facing systems.

RECONIZER™'s agentless artificial intelligence platform searches social media and all layers of the web for leaked user credentials and compromised accounts pilfered in mass data breaches. R-MOR offers comprehensive Cyber Awareness Training to individuals and organizations, to update them on the latest cyber threats and how to protect against them. The training covers topics such as social engineering, phishing and other human-based attacks. R-MOR's phishing simulation service also provides a secure and monitored platform to evaluate and train employees on preventing phishing attacks.