Attack Surface Manager

Daily activity in your organization creates fertile ground for cyber attackers—unless you can perpetually reduce your attack surface.

Every day, as employees routinely use applications and share data, they leave behind an invisible "access footprint"—credentials and connections to other systems. These are the basic tools—keys—that advanced attackers use once inside your network to move from their initial point of entry to their targets. The richer the access footprint, the faster the attacker can move.

Attack Surface Manager enables security teams to efficiently and continuously minimize the proliferation of credentials to make the network as resistant as possible to attackers—without impeding the business.

Deprive attackers of the keys they need to reach your critical assets

With every system an attacker reaches, the damage they can cause increases. Though you can't always prevent advanced attackers from establishing presence in your network, you *can* reduce the business impact of targeted attacks by preemptively hardening your environment.

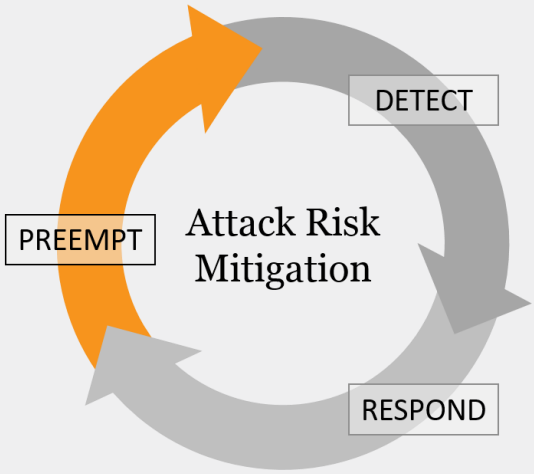
Sometimes people acquire credentials they're not supposed to have, but most of the access footprint is a byproduct of authorized activity. For example:

- User names and passwords are inadvertently captured in browser history;
- Domain administrator credentials can be retained in system memory after a remote support session;
- Access data is stored in applications to enable software updates or other maintenance routines.

Security teams cannot manually locate and remove "hidden" credentials at the scale required in enterprise environments.

Preempt attackers to speed detection and response

By automating discovery and remediation, ASM enables you to slow or stall attackers—until they're detected and expelled. By reducing the real artifacts attackers can use to move forward, ASM strengthens the odds that attackers will activate deceptions—and therefore helps detect attackers earlier and buys time for well-orchestrated incident response.



ASM hardens the network to impede attacker activity—the preemptive function of a comprehensive strategy to mitigate Targeted Attack Risk.

illusive

ASM's analyst dashboard

Attack Surface Manager features

An analyst dashboard provides summary visualizations that enable detailed drill-down into current conditions for every unit and division, and help security teams prioritize remediation activity.

A rules engine that allows operators to easily define acceptable distribution of credentials across the organization, aided by an intuitive interface that suggests rules based on intelligent discovery of the environment.

Mapping in Illusive's Attacker View shows potential attack paths and policy violations in relation to the location of critical systems.

An actions engine enables single violations or large groups of violations to be corrected on demand or through various degrees of automation.

An ASM screen in Attacker View highlighting system-to-system connections enabled by credentials that violate policies

Minimize attacker mobility without impeding the business

- **Uncover invisible risk factors**—across the entire organization
- **Prioritize remediation** by seeing how violations could provide access to business-critical assets
- **Efficiently enforce policies and resolve violations** through smart, human-controlled automation
- **Detect attackers faster** by increasing the odds that attackers will activate deceptions

Contact us

Illusive Networks is a leader in deception-based cybersecurity solutions, empowering security teams to take informed action against advanced, targeted cyberattacks by inhibiting and detecting the lateral movement of adversaries toward critical assets early in the process to prevent damage to the business.

For more information:

Visit us and subscribe to our blog at www.illusivenetworks.com

Email us at info@illusivenetworks.com

Call us at: US: +1 844.455.8748
EMEA and AsiaPac: +972 73.272.4006

Find us: