Attack Surface Manager™

Preemptively harden your network against lateral movement

Stealth attackers move through your network using native connectivity—credentials and connections created by the business. Connectivity is necessary, but in every network there is more than there should be. Credentials get cached, privileges get escalated, rogue connections get established. The richer this "access footprint," the more pathways an attacker has to reach your crown jewels—and the faster damage can be done.

Do you know how attackers can move once they're inside your network?

The access footprint changes constantly as users log on and off, restart systems, change roles, and access resources. Sometimes people knowingly gain access they shouldn't have, but most connectivity results from ordinary, authorized activity. For example:

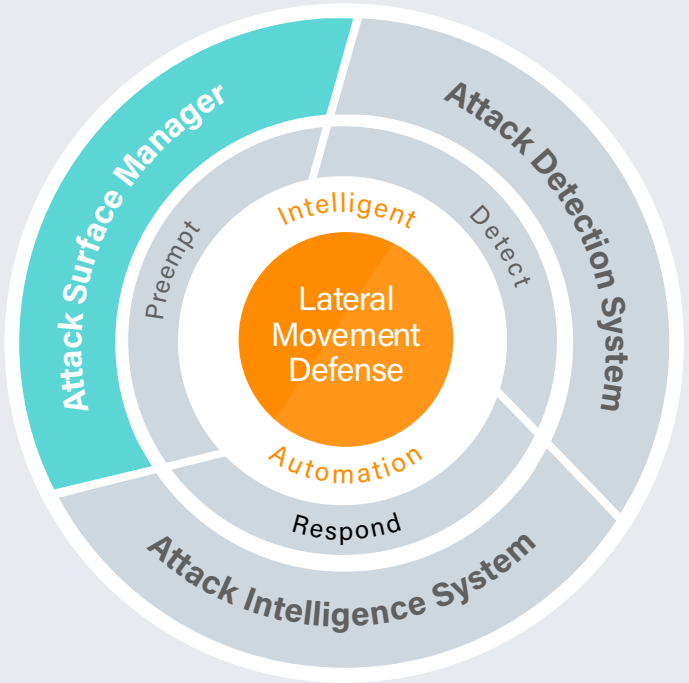
- User names and passwords are inadvertently captured in browser history;
- Domain admin credentials can be retained in system memory after a remote support session;
- Access data is stored in applications to enable software updates or other maintenance;
- User privileges are accidentally escalated due to complexity inherent in a corporate IT directory.

Until now, these conditions have only been visible when skilled analysts inspect individual systems.

Continuously reduce your attack surface—easily and at scale

Illusive Networks Attack Surface Manager automates discovery and clean-up of credential violations, allows drill-down inspection of pathways to critical assets, and provides risk insights that inform intelligent decision-making to reduce attacker mobility.

The Attack Surface Manager reveals hidden credentials and paths to critical systems so you can continuously impede attacker movement—without impeding the business.



Changing the math for early attack detection
Reducing the number of real artifacts while saturating endpoints with deceptive ones increases the odds that attackers will choose deceptions—and be instantly caught.

Attack Surface Manager features:

Pathways
A feature that automatically reveals attack paths from any machine to high-value targets, provides drill-down details on the systems in each path, and enables point-and-click elimination of excess connectivity, leveraging risk and connectivity ratings.

Attack Surface Rules Engine
An easy interface for defining and enforcing credential and connection policies for various roles and groups, including use of local admins, high-privilege credentials, and permissible connections to Crown Jewels.

Attacker View
The Illusive management console that shows location of attack surface violations in relation to Crown Jewels.

Attack Surface Reduction Engine
Action functions that allow single or large groups of violations to be corrected through your chosen degree of automation.

Reduce attacker mobility without impeding the business

- **See exactly how attackers could reach your critical assets** by uncovering invisible conditions that enable lateral movement.
- **Continuously—and easily—reduce your attack surface** using point-and-click functionality to enforce credential policy violations and remove high-risk connections.
- **Detect attackers faster** by increasing the odds that attackers will activate deceptions.
- **Improve cyber agility.** You can't stop users from connecting, but by continuously reducing attacker mobility, you can enable your dynamic organization to operate with greater confidence.

Attack Surface Manager Dashboard
A summary of attack surface metrics and highest-risk conditions that enables drill-down investigations.

FirstMove Preempt Services
Using Attack Surface Manager, Illusive analyzes your system-to-system attack surface, hardens and baselines the environment, and configures Attack Surface Manager to flag policy violations so you can perpetually improve cyber hygiene.