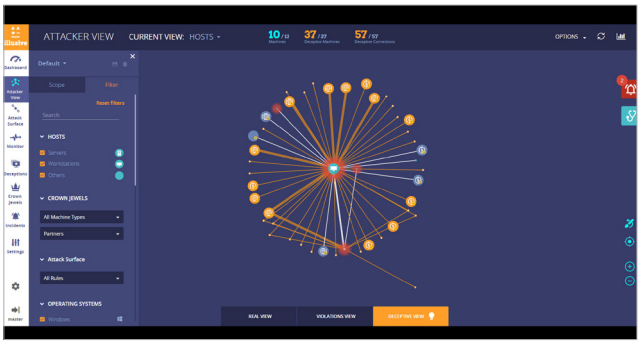
Illusive Networks

Deception Management System V3.1.105



DETAILS

Vendor Illusive Networks

Price pricing available upon request

Contact illusivenetworks.com

Features	★★★★★
Documentation	★★★★★
Value for money	★★★★★
Performance	★★★★★
Support	★★★★★
Ease of use	★★★★★

OVERALL RATING ★★★★★

Strengths The Attack Surface Manager does not require an administrator to be sophisticated in security. It is a basic, standalone product, simple to rollout and incredibly effective. This efficiency is backed by Illusive's undefeated history against Red Teams.

Weaknesses None that we found.

Verdict The Illusive Networks Deception Management System stops attacks by disrupting the human-decision making process behind lateral movement.

488 Madison Avenue, Suite 1103
New York, NY 10022
1-844-455-8748
info@illusivenetworks.com
Website: www.illusivenetworks.com

Illusive Networks Deception Management System stops attacks by disrupting the human-decision making process behind lateral movement through proactively hardening the network by removing excess credentials, connections and pathways to critical assets. It detects attackers early on by planting fake data on endpoints that trigger alerts. The solution simplifies the incident response process by compiling real-time forensic data from the endpoints and decoys.

Illusive's Deception Management System avoids impact on systems and applications crucial for business operations. By focusing on and cutting off lateral movement options from attackers without affective business agility, they are stopped before damage occurs without imposing controls on dynamic business environments.

We were really impressed with the Attack Surface Manager (ASM) platform. It looks at known best practices against what it is finding in the environment. Based on common rules violations, ASM acts and cleans the systems and removes old credentials and attack pathways. Objects are planted and monitored to see if they are used. This gives rise to the preempt, detect, and respond capabilities. User and host behaviors are monitored, and then deceptive planting mimics them. Distinguishing deception from reality is extremely difficult. As behavior changes, so do the deceptions.

ASM forces attackers to reveal themselves early in the attack process by disorienting and manipulating their decision-making process. It also enables rapid, effective response and remediation when attackers are present by providing contextual source and target-based forensics. It offers visibility to pathways that represent possible attack vectors between assets to crown jewels and credentials.

The Violations View shows pathways between systems that provide opportunities for moving privileged credentials. This is particularly hard to distinguish from production behavior, so Illusive came up with an attack risk score to represent the mathematical likelihood an attacker can move laterally without detection.

The Attacker View shows that indicate a history of interaction between hosts. This is what an attacker would see if they got access to one of the systems. Interactions are historical, not theoretical. Instead of leveraging an agent, the tool pushes a binary to the endpoints to scan systems for fresh information, clean policy violation and sensitive information, then goes back and plants deceptive information onto those host making it extremely difficult for an attacker to navigate the environment.

Deception View shows where decoys are within the Real View (real assets). It uses game theory to predict information the attacker will be looking for on a host. The attacker only sees historical connections. This is a big data problem because attackers must sift through everything, which is everchanging. With every interaction, the history is updated.

Attack Surface Manager does not require security sophistication to use. It is a basic, standalone product, simple to rollout and incredibly effective. The focus is on production systems themselves, with deceptions deployed on nearly all production systems. Illusive's undefeated history against Red Teams underscores its efficiency.

Pricing is available upon request. Standard support hours are 8/5. Premium Service is available for a supplemental fee and offers support 24/7.

— Katelyn Dunn
Tested by Tom Weil