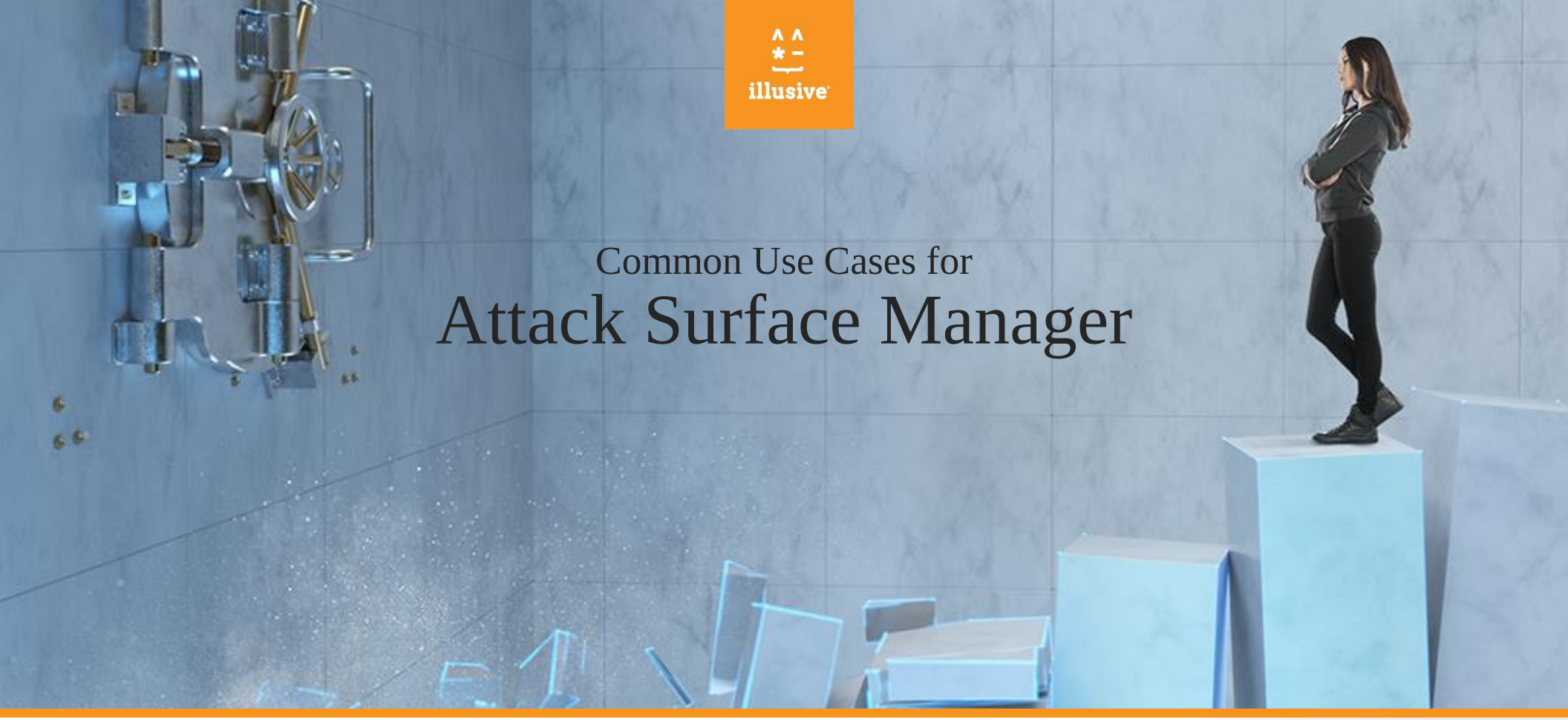

Common Use Cases for Attack Surface Manager

Attack Surface Manager (ASM) gives security teams unprecedented power to defend against advanced attackers by exposing and removing hidden credentials, rogue connections, and other conditions that facilitate lateral movement.

Credentials and connections—the "fuel" for living-off-the-land attacks— are the artifacts that enable attackers to traverse the network under the radar of traditional security monitoring and controls. ASM fills a critical defense gap by stalling or preventing attackers from reaching their targets.

Here we present common uses for ASM that allow Illusive customers to:

- Improve cyber hygiene
- Fill gaps in PAM/PIM solutions
- Identify malicious insider activity
- Streamline Red Teaming

Making a leap in cyber hygiene

Use Case #1

The Carnegie Mellon Software Engineering Institute (SEI) defines cyber hygiene as "a set of practices for managing the most common and pervasive cybersecurity risks faced by organizations today," which, of course, encompasses many domain areas. ASM deals specifically with the discovery and clean-up of excess, high-risk connectivity—a foundational use case for ASM.

Because organizations need connectivity in order to function, a vast and volatile matrix of credentials and connections is created on a daily basis through ordinary business activity. Well-trained security administrators know how these conditions occur; for example:

- User credentials get stored in browser history;
- Access data is stored in applications to enable software updates or other maintenance;
- Domain Admin credentials remain accessible following an improperly terminated RDP session;
- User privileges are inadvertently escalated because of Active Directory complexity.

Without automation, minimizing the spread of this "access footprint" is not feasible. It's also impossible to discern which conditions are acceptable and which pose an untenable level of risk unless you have a comprehensive picture of how systems interconnect across the network.

ASM makes it possible to easily and effectively manage this aspect of cyber hygiene. ASM:

- Perpetually discovers the actual system-to-system pathways across the entire network;
- Enables easy definition of rules and policies, and discovers violations;
- Removes violations through automated or semi-automated actions;
- Discovers all pathways to critical assets and Domain Admin credentials;
- Filters this vast array of data into actionable presentation of high-priority issues;
- Provides connectivity and risk ratings that enable ASM users to quickly judge where and how connectivity can be reduced without negatively impacting the business;
- Provides cyber risk posture information to security leaders via risk metrics and trend data.

Shining a light on privileged accounts

Use Case
#2

"This product alone justifies renewing my Illusive license."

For an attacker, obtaining Domain Admin credentials is a milestone: the attack can now be accelerated.

The ability to guard Domain Admins---to know and control who owns them, how they are used, and what purpose they serve— is obviously an essential security function.

Equally, or perhaps more important is to know where "shadow" admins exist; these could be Service Accounts or any other accounts with elevated privileges that are not part of official Domain Admin groups. Unaccounted for, they pose additional risk because they are not subject to normal monitoring and control via Privileged Access Management (PAM) or Privileged Identity Management (PIM) solutions,

PAM/PIM solutions are considered "must-haves" in most cybersecurity programs, but they also leave dangerous conditions in the shadows.

ASM uncovers these high-risk accounts by:

- Perpetually discovering Domain Admins residing on each endpoint or server in the network;
- Perpetually identifying shadow admins, and users and user groups with elevated privileges across many machines;
- Discovering the chains of machines that, through lateral movement, could enable access to Domain Admins;
- Showing how many "hops" there are between a machine containing Domain Admins and systems tagged as "crown jewels";
- Identifying idle or improperly closed RDP sessions, which can enable caching of associated Domain Admin credentials.

Once discovered, security teams can identify and investigate instances of privilege abuse, take correction action to right-size privileges, or place valid privileged account under PAM/PIM governance.

Next, we show a case of malicious insider activity, that demonstrates why this is so critical.

Detecting a disgruntled employee

Use Case #3

"This product fits perfectly…. We have a lean and focused team. Above all, the tools they use must be practical."

Imagine the following: Oscar, a server admin, had been a loyal employee for over ten years. During that span, he was involved in major deployments of new systems and software, and therefore knew much of the company's core IT infrastructure. A decision was made to eliminate Oscar's position, but because he was regarded as a loyal employee, he was asked to stay on for two weeks to complete some urgent projects, But he felt betrayed, and decided to take action.

During his last few days, Oscar transformed several domain user accounts into shadow admins by assigning direct ACL privileges, and also created multiple Local Admin accounts in the area where new laptops are provisioned. He kept a record of IP addresses for the company's domain controllers, file servers, and mail servers; he planned to target these systems after leaving the company.

Monitoring the daily ASM discovery, security administrators could see a rash of newly created credentials with Domain Admin-level authority in the path of critical systems. Minor investigative effort revealed that Oscar had recently connected to several core systems. ASM also automatically identified the new Local Admin accounts. It was easy to see that they had been created within the same timeframe. Before Oscar could enact his plan, the security team preempted the attack. Oscar was removed from the premises, malicious accounts were removed, and passwords for the targeted systems were changed.

Though not designed mainly for threat detection, by surfacing users associated with an exceptional number of high-risk conditions, ASM reveals anomalous conditions that are invisible to other security technologies.

For organizations using Illusive's endpoint-based deceptions (Illusive Attack Detection System), ASM also plays an important role in magnifying the effectiveness of deceptive credential and connection artifacts; by reducing the number of real lateral movement options from any given machine, the odds increase that attackers will opt to use fake (deceptive) artifacts.

Facilitating the Red Team battle test

Use Case
#4

Red Teaming is gaining in popularity because nothing—even with the most data-rich cyber risk dashboard—will provide more precise visibility into the actual security posture of critical systems and services than a Red Team challenge.

Red Teamers commonly use Bloodhound, Mimikatz and a variety of other attacker tools to establish the lay of the land and determine how they can move laterally. This process is as labor-intensive for a Red Team expert as it is for an advanced attacker.

Through the capabilities described in the use cases above, ASM creates for the Red Team all the visibility they need through a single application and visual interface.

Red Teaming, because it requires rare, specialized skills, is a function that many organizations have chosen to outsource. Through ASM, organizations can incorporate a "perpetual Red Team" function as an integral part of their routine operations, saving time and money—and bringing in-house a function that may previously have been impossible to handle effectively.

See it for yourself!

Contact us to receive a half-day Attack Risk Assessment. Discover the hidden conditions an attacker could use today to reach your critical business systems.

illusive

Illusive Networks stops today's advanced, targeted threats by destroying an attacker's ability to move laterally toward critical assets through a simple, agentless approach that scales and adapts as the business environment changes.

www.illusivenetworks.com
info@illusivenetworks.com
US: +1 844.455.8748
EMEA / AsiaPac: +972 73.272.4006