Stop Malicious Lateral Movement Everywhere

Illusive Networks and Microsoft Azure Sentinel Integration

What If You Could Operate in a '000' World?

Zero

Privileged accounts accessible to attackers

Zero

False positive alerts to distract defenders

Zero

Wasted investigation time to slow responders

Illusive Can Help Build a ‘000’ World

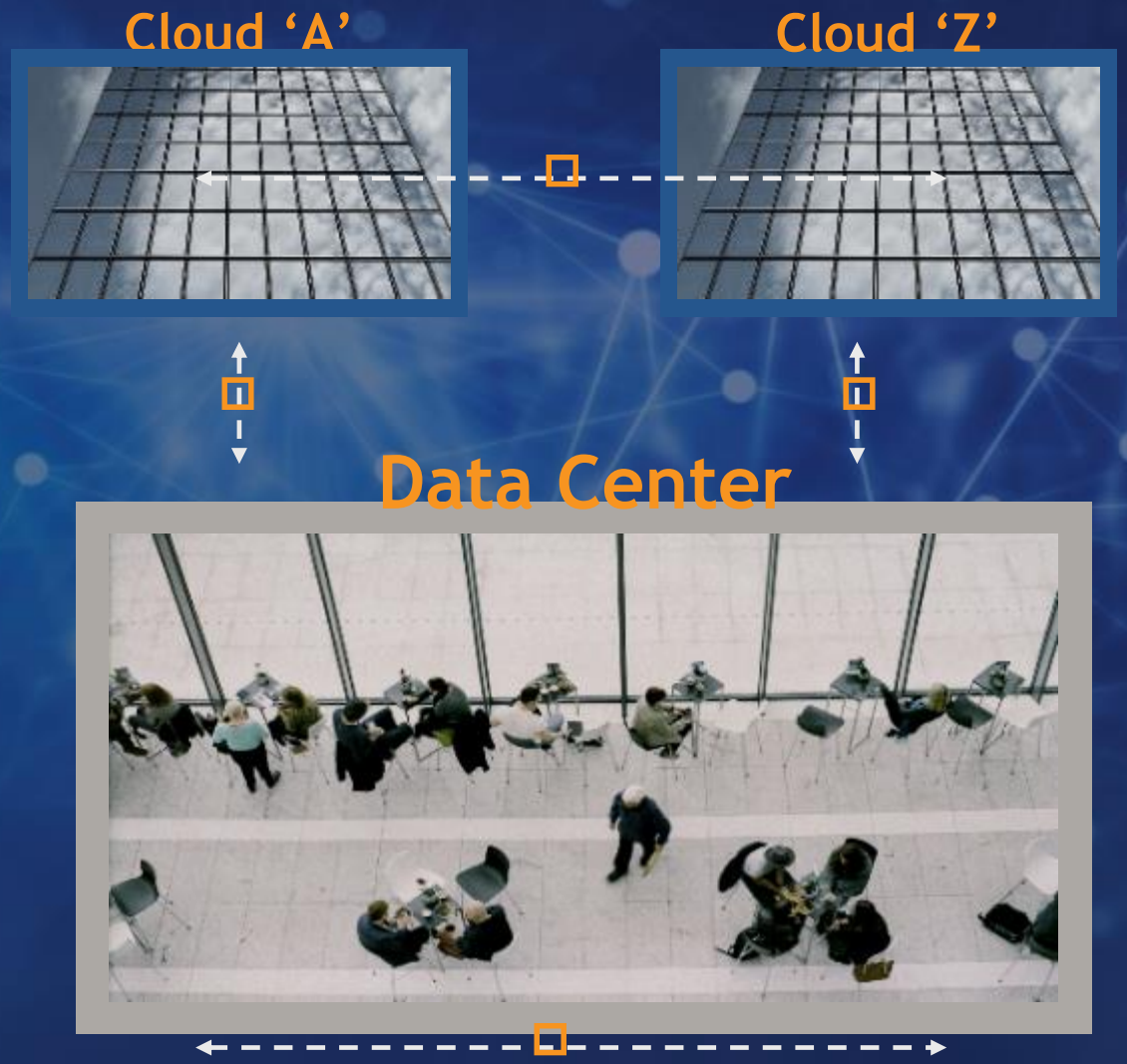
Shrink the True Attack Surface

Create the Illusion of an Expanded Attack Surface

Deliver **Analytics** and Actionable Insights

100% Agentless

The Goal: Stop Attacker Lateral Movement



Cloud movement

Across/within clouds

Vertical movement

To/from cloud

Lateral movement

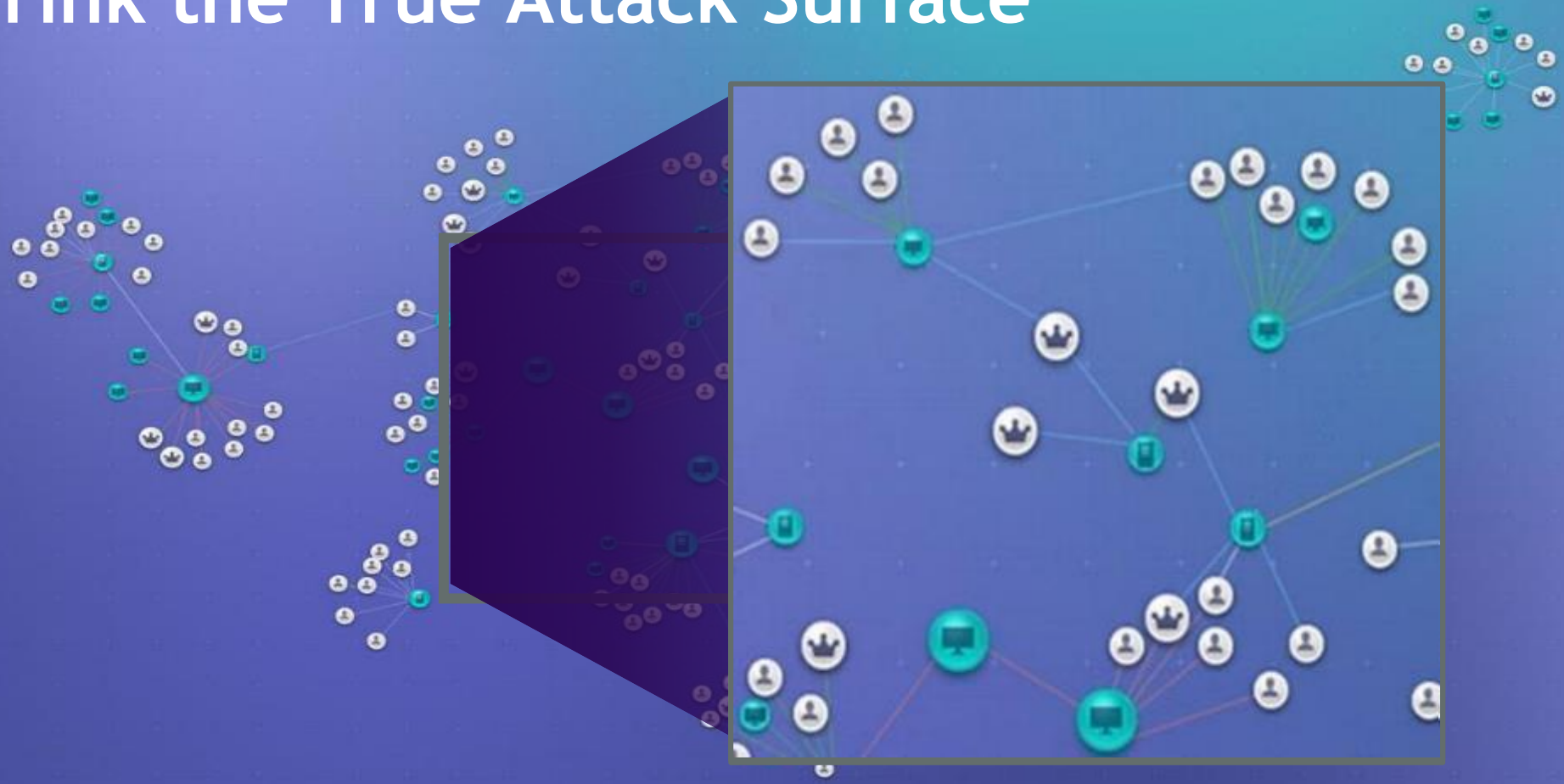
Across endpoints, datacenters, networks

Credentials and Host-to-Host Connections Are the Attacker's "Fuel"

Excess credentials and connections:

- Enable attack movement no matter where attacker lands
- Allow for evasion of other tools
- Disguise attackers in a veil of normalcy or false positive alerts

Shrink the True Attack Surface



Attack Surface Manager

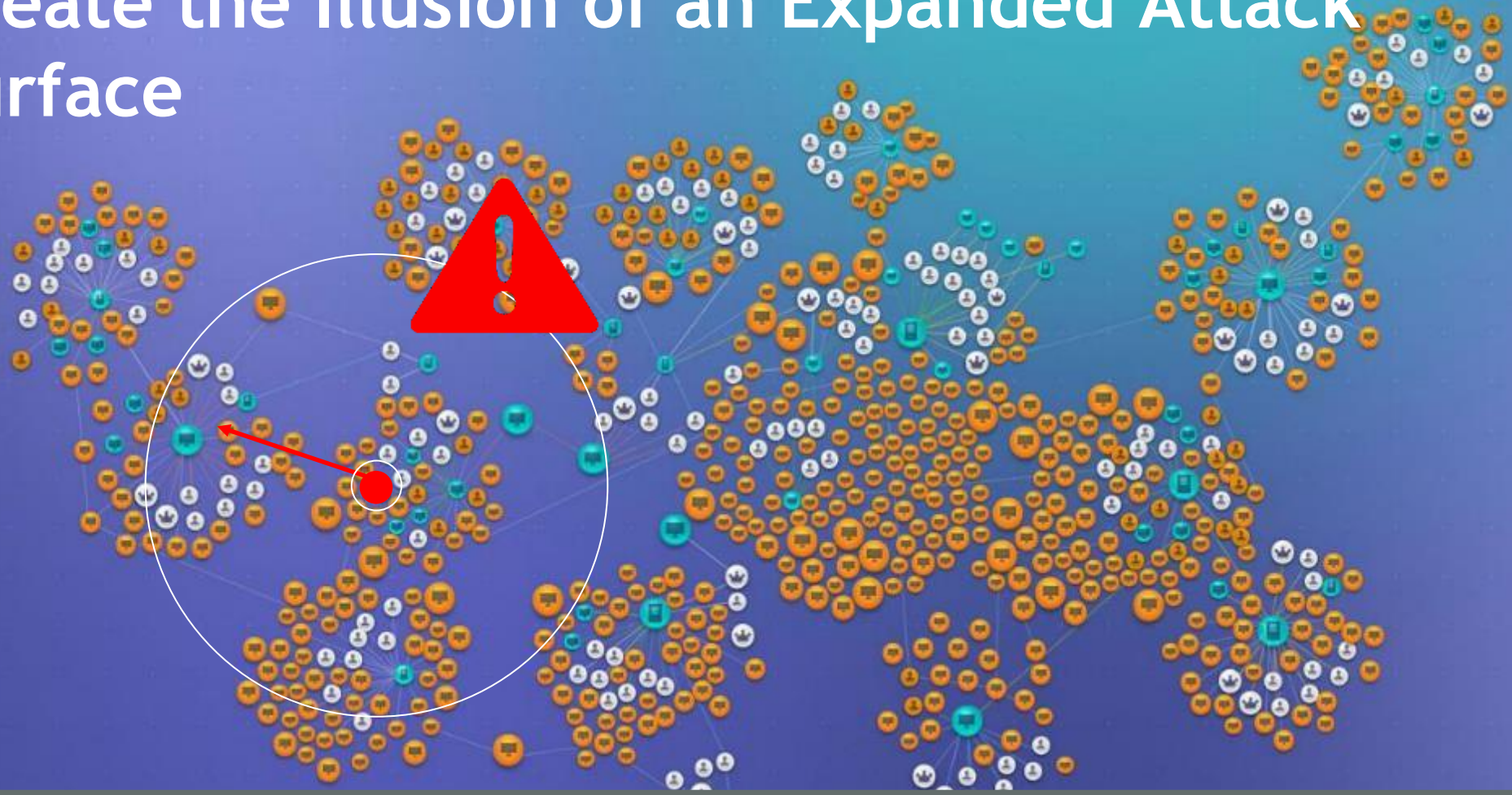
- View the attack surface through the lens of the attacker
- Identify and remove errant credentials, connections and attack pathways

Verizon reports **80%** of attacks use stolen credentials

Illusive has assessed ~500K endpoints and found:

- **19%** contained accessible privileged credentials
- Many environments were much worse

Create the Illusion of an Expanded Attack Surface



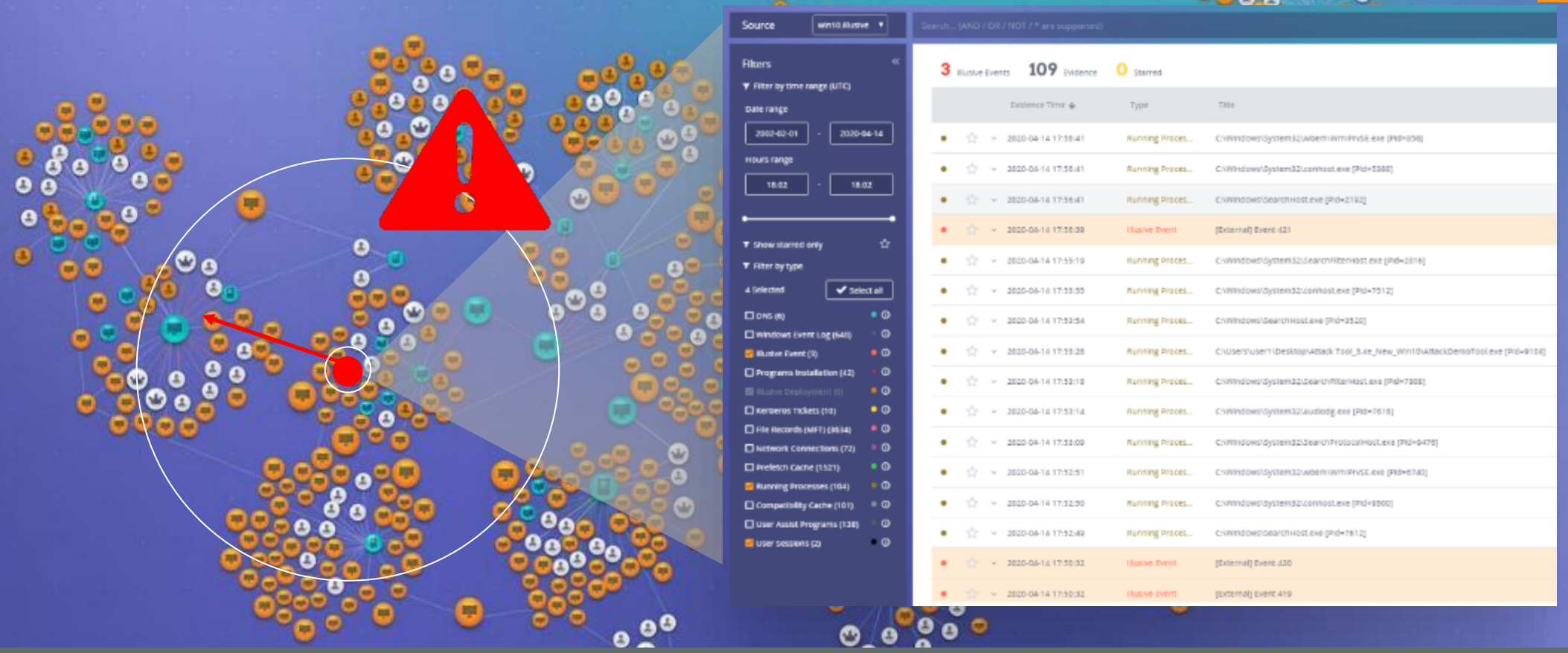
Attack Detection System

- Deploy agentless, highly authentic data, device, and decoy deceptions
- Across Data Center, IIoT/IoT, Cloud
- Force attackers to reveal themselves without generating false positives

"Organizations seeking to enhance their security posture with highly realistic, efficient, easy-to-deploy deception technology should take a close look at Illusive's real-time, automated platform."

Enterprise Strategy Group

Analytics and Actionable Insights Speed Response



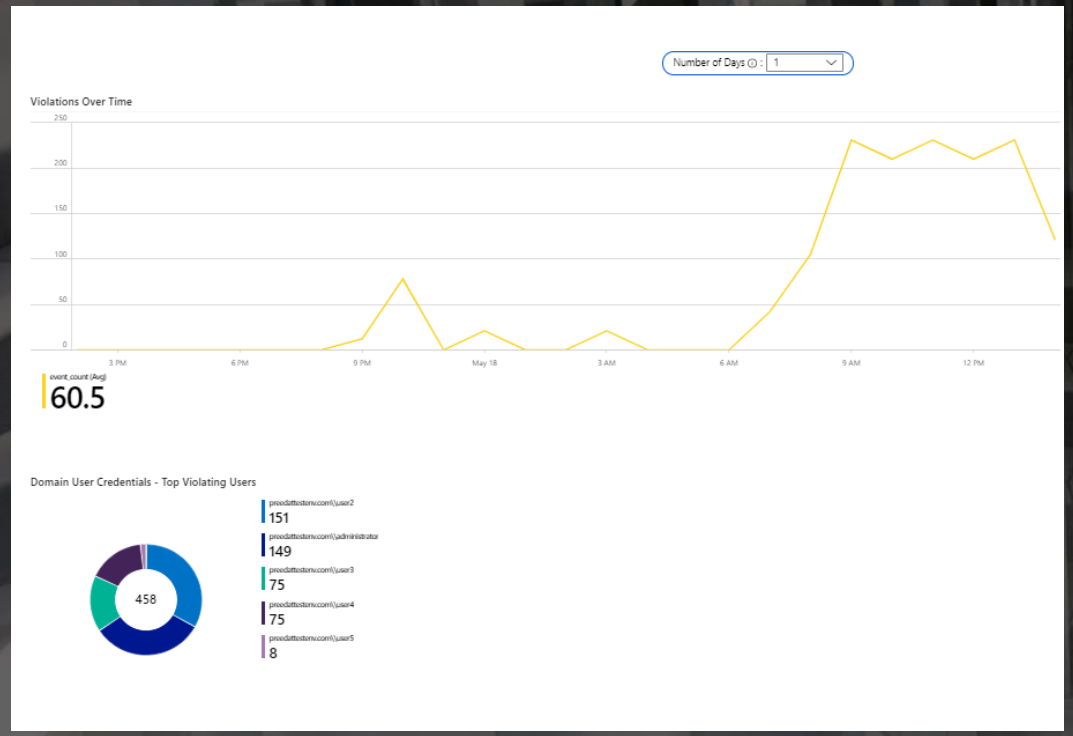
Attack Intelligence System

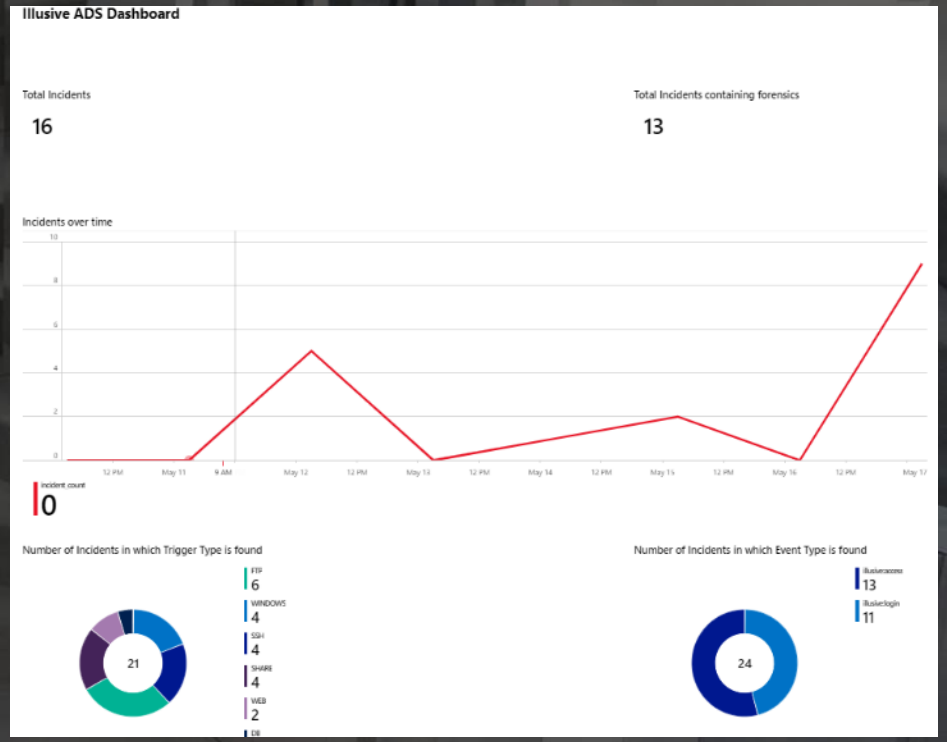
- Cut research time with on-detection and on-demand source forensics
- Build threat intelligence with rich interactive target forensics

Customers report **60-90%** reduction of SOC analyst investigation time, increasing SOC capacity at least **2X**

Azure Sentinel and Illusive

High-fidelity attack detection, incident enrichment and threat intelligence





- CEF Connector and Dashboards within Sentinel to provide Attack Surface Risk discovery & remediation
- Enrich alerts from any solution with Illusive forensics
- Enhance triage with alert correlation
- Illusive APIs and playbooks automate attack surface reduction, threat intelligence and incident response

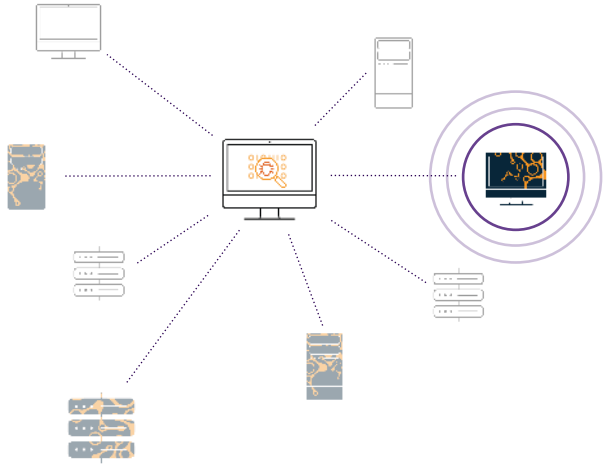
How Illusive and Azure Sentinel Work Together to Discover and Remediate Threats

1

Illusive provides the earliest possible detection of lateral movement by humans or malware on the endpoint

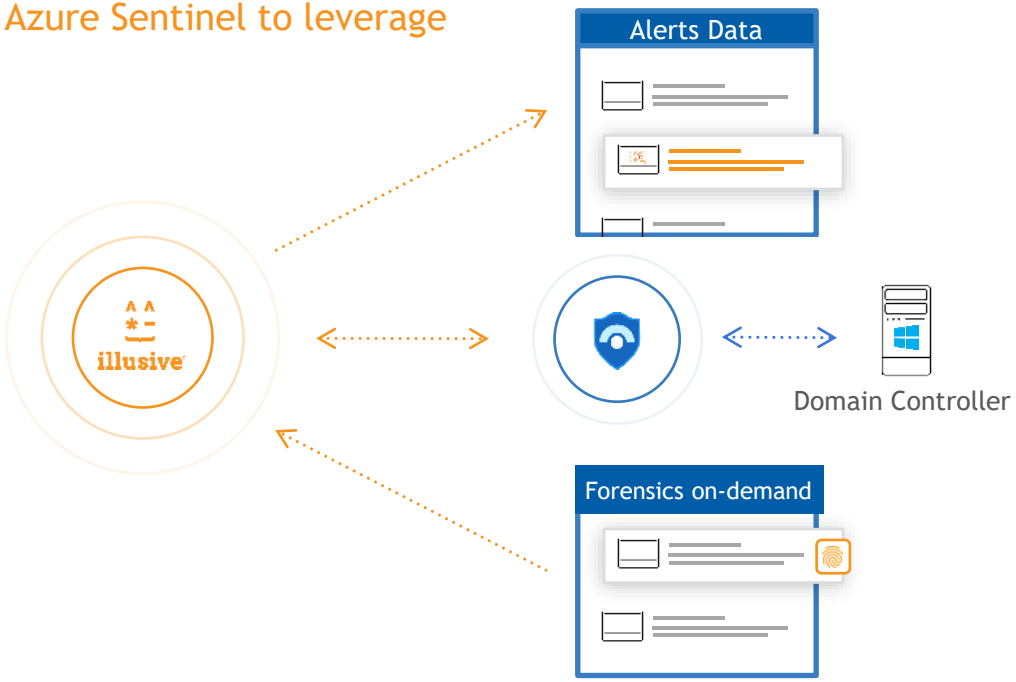
2

Attacker unknowingly accesses a highly authentic endpoint deception



Illusive sends high-fidelity alerts and forensic data for Azure Sentinel to leverage

Azure Sentinel



How Illusive Complements Behavioral Detection

- Most threat detection alerts typically only pick up movement that is anomalous, not high-fidelity attacker movement
- UEBA & AI/ML is insufficient when there is no normal in “wfh” environment. Additionally, baselining and calibration is tedious
- Common threat vectors where more visibility is needed:
  - Insider threat detection is often inefficient
  - Nation-state attackers often go undetected for months while performing reconnaissance

Voice of the SOC

“Too many alerts—too few analysts”

Tier 1: 19-24 minutes per incident (20–25 per analyst a day)

Tier 2: 60-80 minutes per incident (6-7 per analyst a day)

Tier 3: 3-6 hours per incident (2-3 per analyst a day)

Bottlenecks: Insane alert volume, context, automated response coordination

In new “no’ normal, established user behaviors and access baselines are flipped on their heads!

300%

Increase in SOC alerts

Illusive Forensics on Demand for Azure Sentinel

Instant forensic intelligence for ANY alert

- Automated forensics collection for any system generated security event within Azure Sentinel - even from other cybersecurity solutions
- Agentless retrieval from target system in <1s
- Rich artifact timeline
- Increases SOC efficiency, speeds incident response

Illusive Forensics on Demand - At a Glance

- Collected automatically
  - REST API Call
  - User request
  - Tripping a deception
- Volatile and non-volatile data
- Screenshots
- Powershell and command line history
- Attack Path to domain admins and crown jewels

Who benefits from real-time forensics collection?

- No EDR
- EDR
- Every Organization

Democratized Forensic Data Enables Shift Left

Triage Time per Incident With Illusive Precision Forensics

SHIFT LEFT

Tier 1	
Before	After
20min	1 to 5min
Avg 20 Incidents per Day	80 to 400
Time Saved: ~5hrs per day/per analyst	

Tier 2	
Before	After
60min	<10min
Avg 6 Incidents per Day	>36
Time Saved: ~5hrs per day/per analyst	

Tier 3	
Before	After
180min	<30min
Avg 2 Incidents per Day	>10
Time Saved: ~5hrs per day/per analyst	

Empower Tier 1 and 2, free up Tier 3 for what truly matters

*Times can vary depending on uniqueness of incident, triage path and technical expertise of staff

Illusive and Azure Sentinel Together

- Reduce lateral movement paths leveraged by attackers
- No normal – behavioral noise reduction needed
- Illusive provides high-fidelity attacker detection
- Illusive forensics within Sentinel reduce triage and investigation time
- Triple zero within reach – no exposed connections, false positives or wasted investigation time

THANK YOU

illusive®

www.illusivenetworks.com