Securing Active Directory:

How to Reduce Blind Spots and Paralyze Attackers

Microsoft & Illusive Networks

Agenda

01 Why is Active Directory such an attractive attack target?

02 An introduction to attack surface management

- A deep dive into the conceptual framework that provides the key to protecting identities in cloud environments like Azure

03 Putting attack surface management into practice with Active Directory & Azure Active Directory

- Out of the theoretical and into the practical. Here we examine how to easily and efficiently close security gaps

04 Q&A

Why is AD/AAD such an attractive target?

Active Directory—a Favorite Target

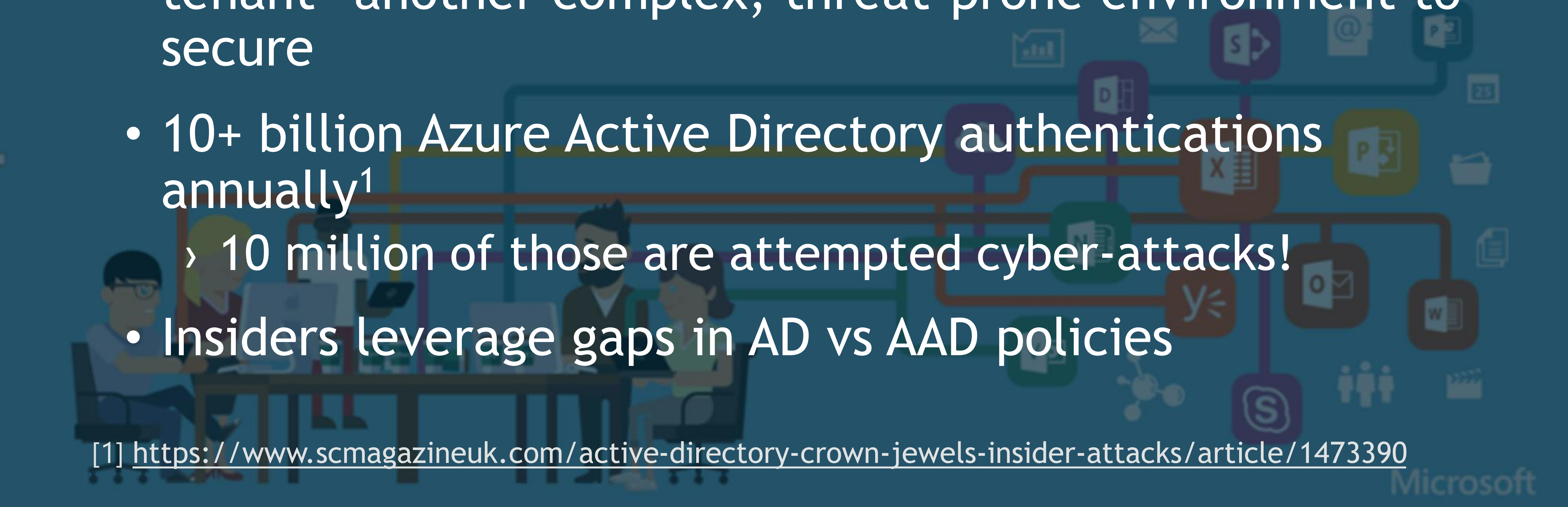
- 90% of the world's enterprise organizations use Active Directory (AD) as primary method for authentication and authorization[1]

- If attackers can penetrate AD, they potentially gain access to the entire network
- According to Microsoft, 95 million AD accounts are under cyber-attack on a daily basis[1]

[1] https://www.scmagazineuk.com/active-directory-crown-jewels-insider-attacks/article/1473390

Office 365 Increases AD’s Attack Surface

- Azure Active Directory is used by all Office365 apps
- Every Office365 instance requires a separate Azure AD tenant—another complex, threat-prone environment to secure
- 10+ billion Azure Active Directory authentications annually[1]
  - 10 million of those are attempted cyber-attacks!
- Insiders leverage gaps in AD vs AAD policies



[1] https://www.scmagazineuk.com/active-directory-crown-jewels-insider-attacks/article/1473390

What's the Risk?

- AD is based on LDAP which is designed to deliver information to the querying host
- A DSQuery reveals a TON of information about the environment and where the goodies are
- Privileged accounts are always attacker targets—ALWAYS
- Any access gained through on-premise AD can have repercussions in AAD or web-based applications leveraging AAD

OK…So How Do You Defend AD?

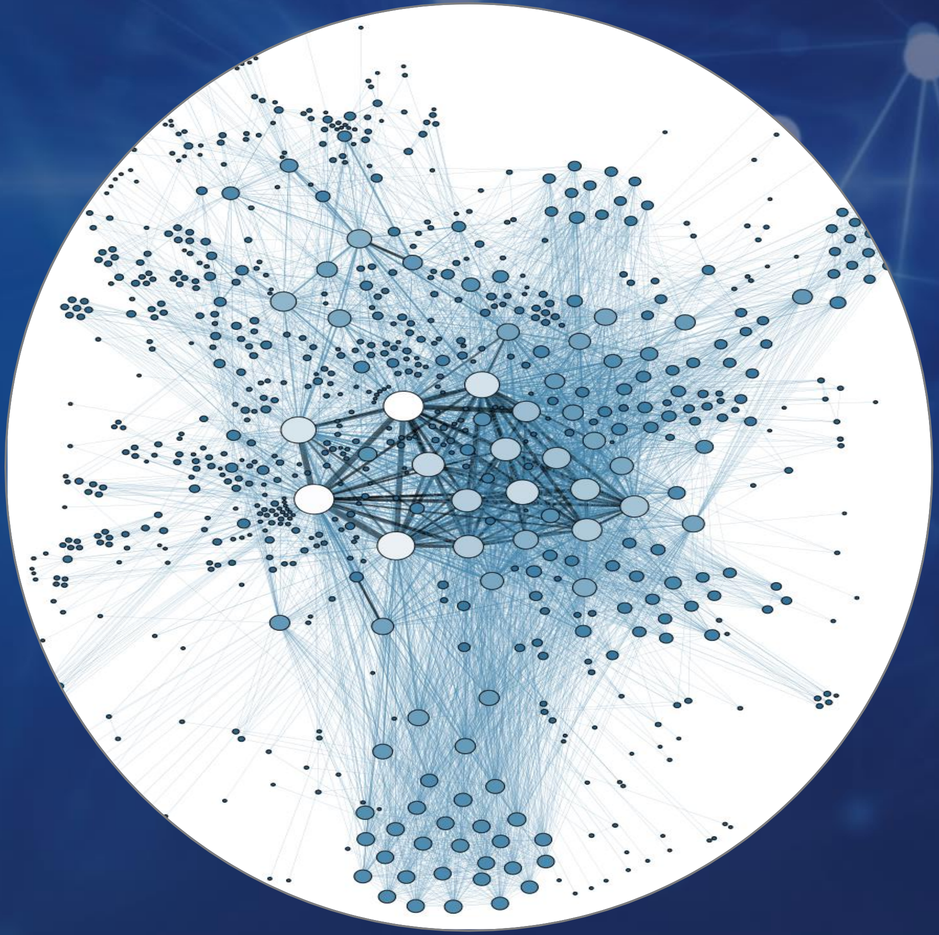
Continuous audit and visibility

+ Remediation of privilege credentials violations

= Attack Surface Management

An Introduction to Illusive Attack Surface Manager

A Dangerous Lack of Visibility



What can an attacker do inside my environment?

Your real connectivity

- This connectivity is—
- Volatile, created through normal business activity
- Vast, reflecting the complexity of the infrastructure
- Invisible with today’s security technologies

Attackers "Ride" Your Connectivity to Reach Their Targets

The Attacker's Fuel:
Credentials and host-to-host connections

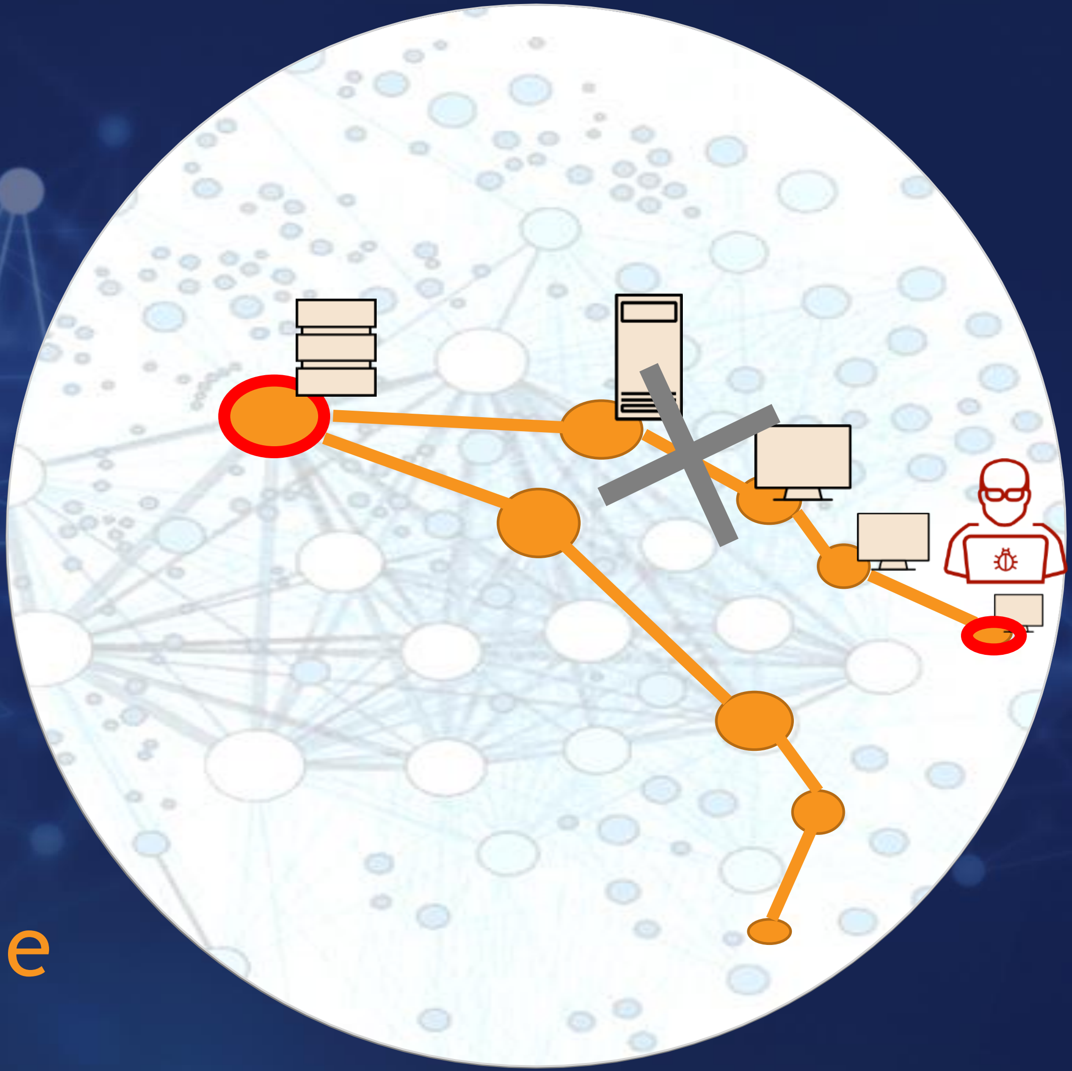
Excess credentials and connections:

- Increase attacker movement options
- Increase attacker velocity

Illusive Attack Surface Manager Preemptively Blocks Attacker Movement Without Impeding Business Agility

Illusive Attack Surface Manager

- Reducing lateral movement risks in Microsoft AD/AAD environments
- Continuously eliminates conditions that fuel it
- Easy definition of policies
- Global visibility on potential attack paths to critical assets
- Easy removal of violations and excess connectivity



Clear visibility on the high-risk areas

Automatic Exposure of High Risk Conditions

ILLUSIVE ATTACK SURFACE RULES ENGINE

1 USER CREDENTIALS

Finds Microsoft AD creds & hosts with stored credentials that could allow attackers to expand their foothold

2 CROWN JEWELS CONNECTIONS

Finds connections to the organization’s critical assets

3 LOCAL ADMINS

Finds hosts with local admin credentials that could be used to execute admin-level actions

4 WINDOWS SHADOW ADMINS

Finds high-privilege users & groups that are not members of known groups (domain admins, etc.)

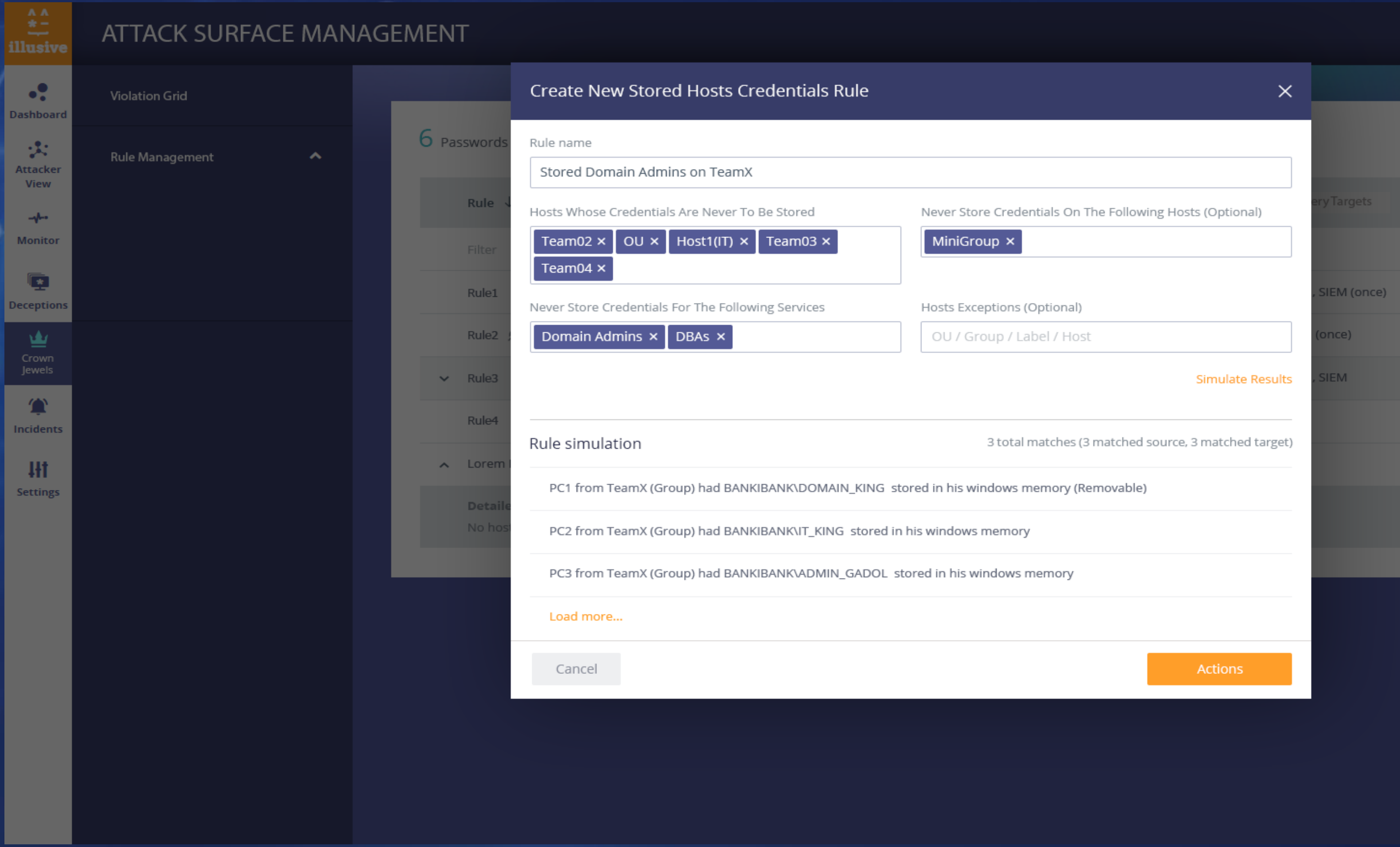
5 MICROSOFT AZURE PRIVILEGED IDENTITIES

Microsoft AAD configuration and integration

Simple Definition of Hygiene Policy

- Control proliferation of credentials between groups and functions
- Stage and tune rules through simulation feature
- Selectively send notifications to SIEM

ILLUSIVE ATTACK SURFACE RULES ENGINE



Create New Stored Hosts Credentials Rule

Rule name: Stored Domain Admins on TeamX

Hosts Whose Credentials Are Never To Be Stored: Team02 × OU × Host1(IT) × Team03 × Team04 ×

Never Store Credentials On The Following Hosts (Optional): MiniGroup ×

Never Store Credentials For The Following Services: Domain Admins × DBAs ×

Hosts Exceptions (Optional): OU / Group / Label / Host

Simulate Results

Rule simulation

3 total matches (3 matched source, 3 matched target)

PC1 from TeamX (Group) had BANKIBANK\DOMAIN_KING stored in his windows memory (Removable)

PC2 from TeamX (Group) had BANKIBANK\IT_KING stored in his windows memory

PC3 from TeamX (Group) had BANKIBANK\ADMIN_GADOL stored in his windows memory

Load more...

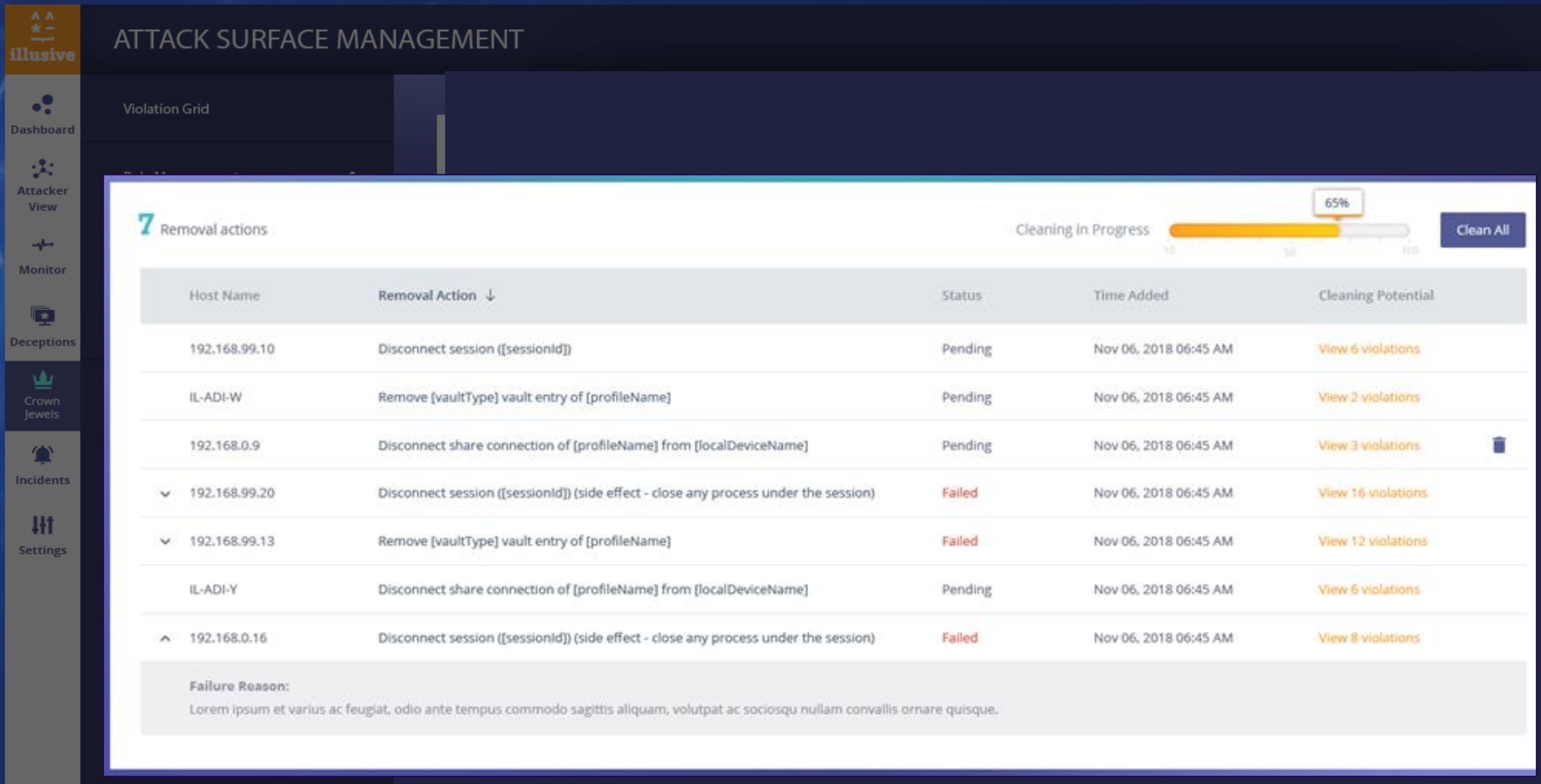
Cancel

Actions

Easy and Ongoing Removal of Violations

- **Eliminate** user credential violations
- **Eliminate** unauthorized connections to critical assets
- Action options
  - › Manually triggered
  - › Act simultaneously on groups of hosts
  - › Fully automated

ILLUSIVE ATTACK SURFACE RULES ENGINE



7 Removal actions

	Host Name	Removal Action ↓	Status	Time Added	Cleaning Potential
	192.168.99.10	Disconnect session ([sessionId])	Pending	Nov 06, 2018 06:45 AM	View 6 violations
	IL-ADI-W	Remove [vaultType] vault entry of [profileName]	Pending	Nov 06, 2018 06:45 AM	View 2 violations
	192.168.0.9	Disconnect share connection of [profileName] from [localDeviceName]	Pending	Nov 06, 2018 06:45 AM	View 3 violations
⌄	192.168.99.20	Disconnect session ([sessionId]) (side effect - close any process under the session)	Failed	Nov 06, 2018 06:45 AM	View 16 violations
⌄	192.168.99.13	Remove [vaultType] vault entry of [profileName]	Failed	Nov 06, 2018 06:45 AM	View 12 violations
	IL-ADI-Y	Disconnect share connection of [profileName] from [localDeviceName]	Pending	Nov 06, 2018 06:45 AM	View 6 violations
^	192.168.0.16	Disconnect session ([sessionId]) (side effect - close any process under the session)	Failed	Nov 06, 2018 06:45 AM	View 8 violations

Failure Reason:
Lorem ipsum et varius ac feugiat, odio ante tempus commodo sagittis aliquam, volutpat ac sociosqu nullam convallis ornare quisque.

Continuously enforce policies through admin-controlled automation

Attack Surface Management in Action

Real Results from Illusive Assessments

A SECURITY PRODUCT FLAW

- Strong security program
- Found 4,000 Domain Admin credentials— in clear text
- Planted by a faulty security product
- No other product saw it

[~18,000 ENDPOINTS]

MISCONFIGURED SERVICE ACCOUNTS

- ~400 Domain Admins found on servers in a datacenter
- Believed necessary to enable a management tool
- Prompted deeper investigation, which led to correction

[~7,000 ENDPOINTS]

POLICY ENFORCEMENT GAPS

- Same Local Admin password on >60% of the laptops surveyed
- IT Ops: *“It doesn’t matter— it’s an old user”*
- Account still active; situation was corrected in less than one hour

[~150,000 ENDPOINTS]

Putting Attack Surface Management Into Practice Protecting Cloud Assets

Illusive Cloud Capabilities

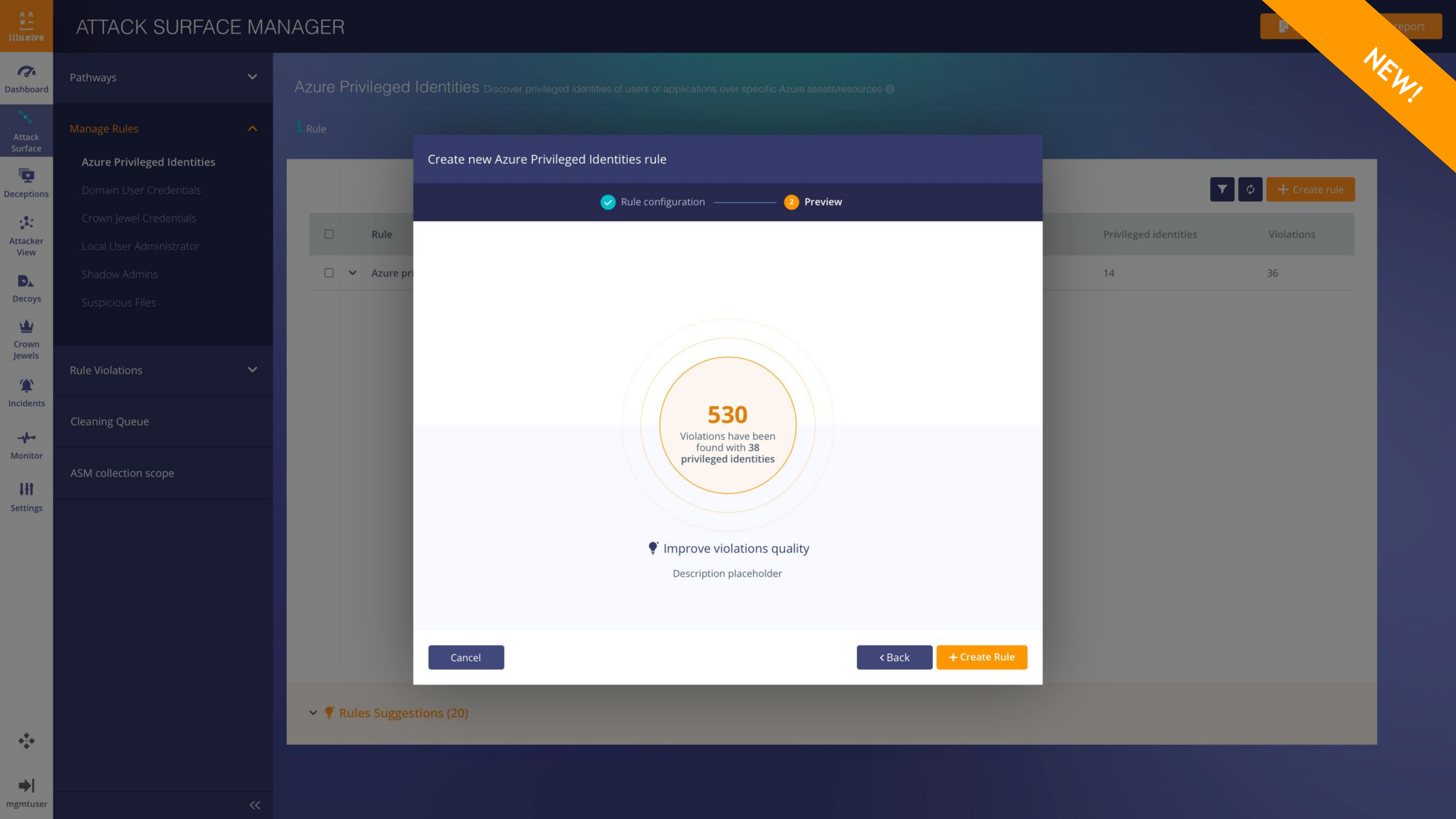
Attack Surface Manager

Problem:

Managing privileges & access to the organization’s cloud resources and services, introduces **new complexities and might be handled incorrectly**, leaving behind:

- **Redundant** identities
- Identities with **excessive privileges**
- Dangerous **bad practices**
- **Vulnerable privileged identities**

ASM Uncovers: Privileged identities and violations over Azure assets



Azure Privileged Identities Discover privileged identities of users or applications over specific Azure assets/resources

□	Rule	Privileged identities	Violations
□	Azure pri	14	36

Create new Azure Privileged Identities rule

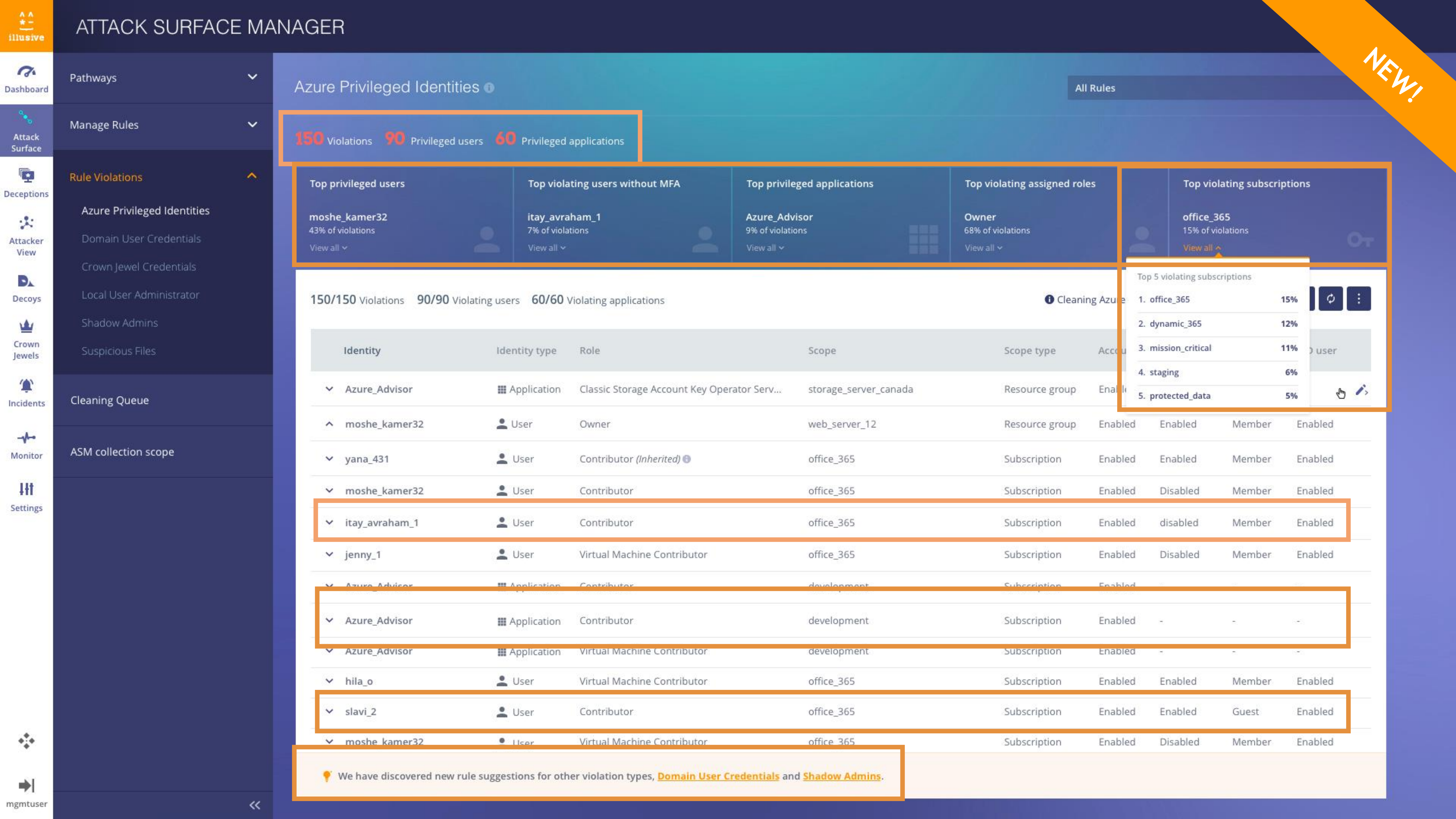
✓ Rule configuration —— 2 Preview

530

Violations have been found with **38 privileged identities**

Improve violations quality

Description placeholder



Azure Privileged Identities

150 Violations 90 Privileged users 60 Privileged applications

Top privileged users
moshe_kamer32
43% of violations

Top violating users without MFA
itay_avraham_1
7% of violations

Top privileged applications
Azure_Advisor
9% of violations

Top violating assigned roles
Owner
68% of violations

Top violating subscriptions
office_365
15% of violations

Top 5 violating subscriptions

1. office_365	15%
2. dynamic_365	12%
3. mission_critical	11%
4. staging	6%
5. protected_data	5%

150/150 Violations 90/90 Violating users 60/60 Violating applications

Identity	Identity type	Role	Scope	Scope type	Acc			user
Azure_Advisor	Application	Classic Storage Account Key Operator Serv...	storage_server_canada	Resource group	Enal			
moshe_kamer32	User	Owner	web_server_12	Resource group	Enabled	Enabled	Member	Enabled
yana_431	User	Contributor *(Inherited)*	office_365	Subscription	Enabled	Enabled	Member	Enabled
moshe_kamer32	User	Contributor	office_365	Subscription	Enabled	Disabled	Member	Enabled
itay_avraham_1	User	Contributor	office_365	Subscription	Enabled	disabled	Member	Enabled
jenny_1	User	Virtual Machine Contributor	office_365	Subscription	Enabled	Disabled	Member	Enabled
Azure_Advisor	Application	Contributor	development	Subscription	Enabled			
Azure_Advisor	Application	Contributor	development	Subscription	Enabled	-	-	-
Azure_Advisor	Application	Virtual Machine Contributor	development	Subscription	Enabled	-	-	-
hila_o	User	Virtual Machine Contributor	office_365	Subscription	Enabled	Enabled	Member	Enabled
slavi_2	User	Contributor	office_365	Subscription	Enabled	Enabled	Guest	Enabled
moshe_kamer32	User	Virtual Machine Contributor	office_365	Subscription	Enabled	Disabled	Member	Enabled

We have discovered new rule suggestions for other violation types, Domain User Credentials and Shadow Admins.

Illusive Cloud Capabilities

Attack Surface Manager

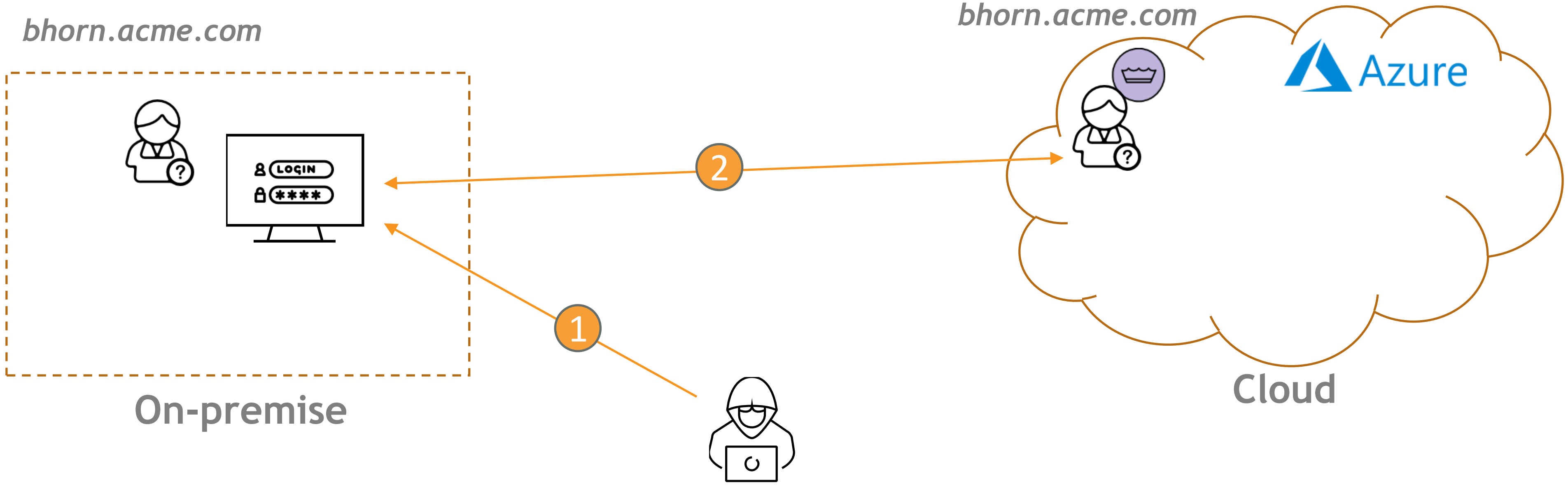
Problem:

Cloud Privileged users are not necessarily **admins on the on-premise domain**, therefor their implications on the attack surface remain **invisible.**

A compromised host with **cached credentials of a privileged cloud user**, will provide the attacker extensive capabilities in the cloud

ASM Suggests: New cloud-based rules in Domain User Credentials and Shadow Admins, in order to discover and eliminate stored credentials of cloud privileged users

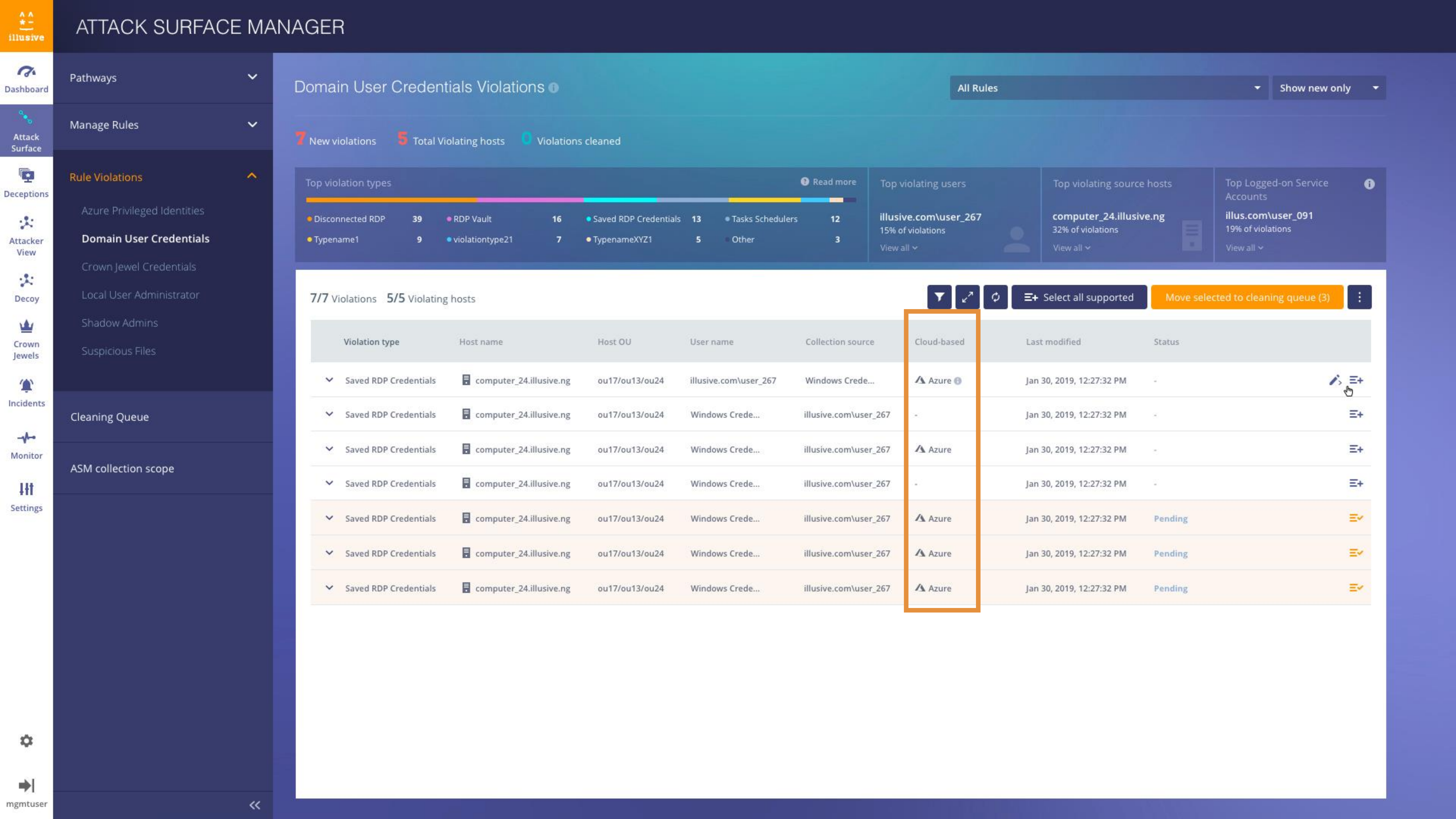
ILLUSIVE CLOUD CAPABILITIES – **ASM**



1 Harvesting/Shadowing

2 Can utilize cloud resources

Domain User Credentials and Shadow Admins new enriched rules



ATTACK SURFACE MANAGER

Domain User Credentials Violations

All Rules: Show new only

7 New violations 5 Total Violating hosts 0 Violations cleaned

Top violation types — Read more

Disconnected RDP 39	RDP Vault 16	Saved RDP Credentials 13	Tasks Schedulers 12
Typename1 9	violationtype21 7	TypenameXYZ1 5	Other 3

Top violating users
illusive.com\user_267
15% of violations
View all

Top violating source hosts
computer_24.illusive.ng
32% of violations
View all

Top Logged-on Service Accounts
illus.com\user_091
19% of violations
View all

7/7 Violations 5/5 Violating hosts

Violation type	Host name	Host OU	User name	Collection source	Cloud-based	Last modified	Status
Saved RDP Credentials	computer_24.illusive.ng	ou17/ou13/ou24	illusive.com\user_267	Windows Crede...	Azure	Jan 30, 2019, 12:27:32 PM	-
Saved RDP Credentials	computer_24.illusive.ng	ou17/ou13/ou24	Windows Crede...	illusive.com\user_267	-	Jan 30, 2019, 12:27:32 PM	-
Saved RDP Credentials	computer_24.illusive.ng	ou17/ou13/ou24	Windows Crede...	illusive.com\user_267	Azure	Jan 30, 2019, 12:27:32 PM	-
Saved RDP Credentials	computer_24.illusive.ng	ou17/ou13/ou24	Windows Crede...	illusive.com\user_267	-	Jan 30, 2019, 12:27:32 PM	-
Saved RDP Credentials	computer_24.illusive.ng	ou17/ou13/ou24	Windows Crede...	illusive.com\user_267	Azure	Jan 30, 2019, 12:27:32 PM	Pending
Saved RDP Credentials	computer_24.illusive.ng	ou17/ou13/ou24	Windows Crede...	illusive.com\user_267	Azure	Jan 30, 2019, 12:27:32 PM	Pending
Saved RDP Credentials	computer_24.illusive.ng	ou17/ou13/ou24	Windows Crede...	illusive.com\user_267	Azure	Jan 30, 2019, 12:27:32 PM	Pending

Summary of ASM Azure AD Capabilities

- Visualize and automate discovery of cloud Crown Jewels
- Find and eliminate common attacker pathways towards Crown Jewels
- Link violations and privileged access to the cloud and back
  - Map and connect Azure high-privileged users to on-premise Active Directory
- Set rules for monitoring and remediation

Another Layer of Protection

Leverage AD Objects to Create Authentic-Looking Deceptions

- Customize the deceptive story for each endpoint
- Use a gradient of believability to further complicate the problem for the attacker
- Automatically update the story based on changes in the environment so that the deceptions are continuously relevant

Illusive Is Agentless

- No need to install or uninstall anything on a protected machine
- Unobtrusive and invisible to legitimate end users
- Undetectable and impenetrable to attackers
- Scales to support organizations of any size
- Low endpoint overhead
- Low cost to operate

KEY TAKEAWAYS

- Securing Active Directory is Critical
- Continuous visibility into vulnerable credentials and connections
- Remediation and Cleaning
- Frustrate attackers with authentic-looking deceptions

Thank you! Questions?

Next Steps:

Request a demo at www.illusivenetworks.com/demo

Learn more at www.illusivenetworks.com/resources

Read our blog at www.illusivenetworks.com/blog

Follow us— in www.linkedin.com/company/illusive

🐦 @illusivenw