RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **PART1-R06**

Another lock? More barbed wire? It’s time to reimagine modern access security

Nitika Gupta

Principal Product Manager Lead
Microsoft Corporation
@_Nitika_Gupta

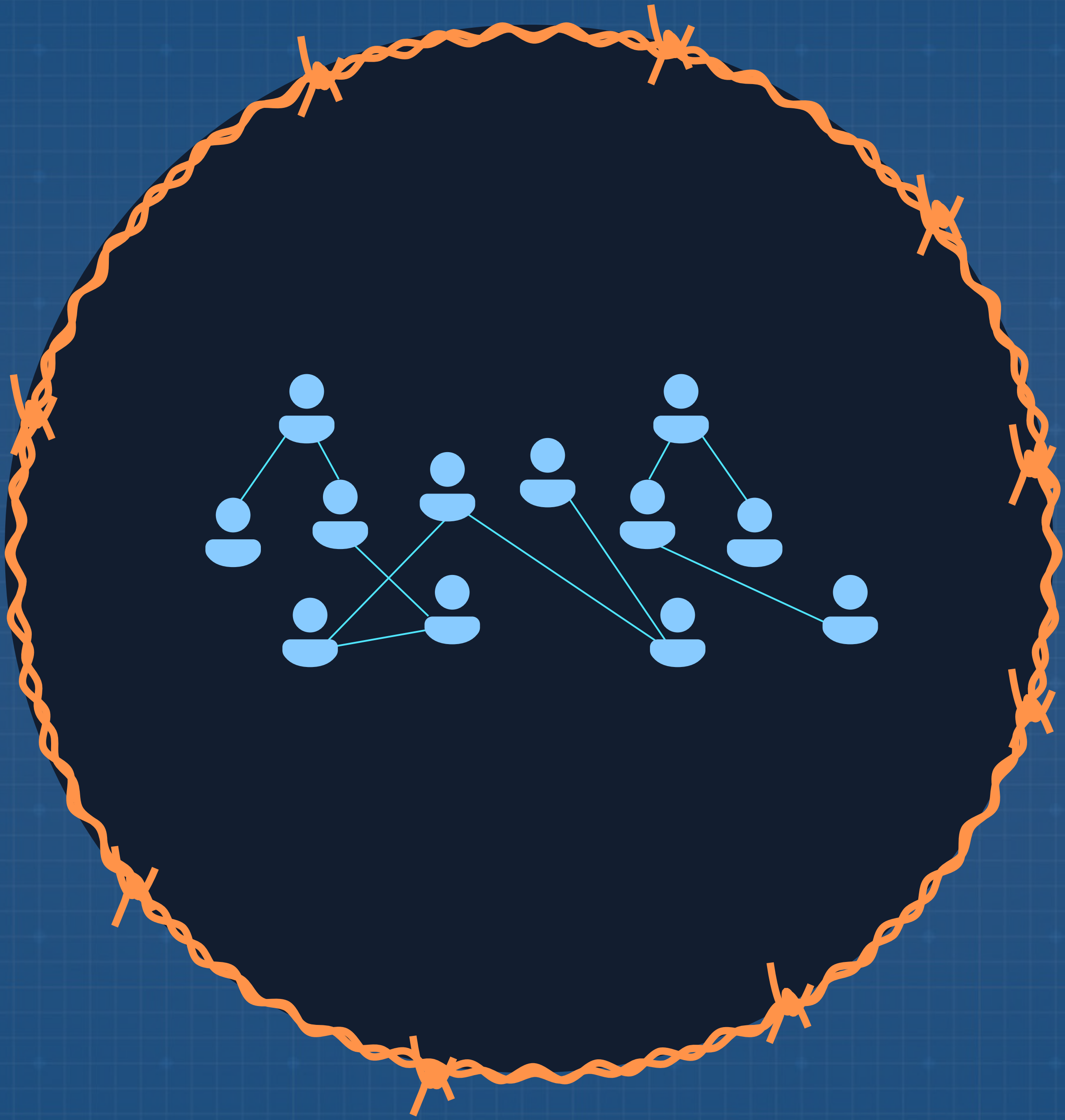
Rahul Prakash

Principal Product Manager Lead
Microsoft Corporation
@RahPrak

Disclaimer

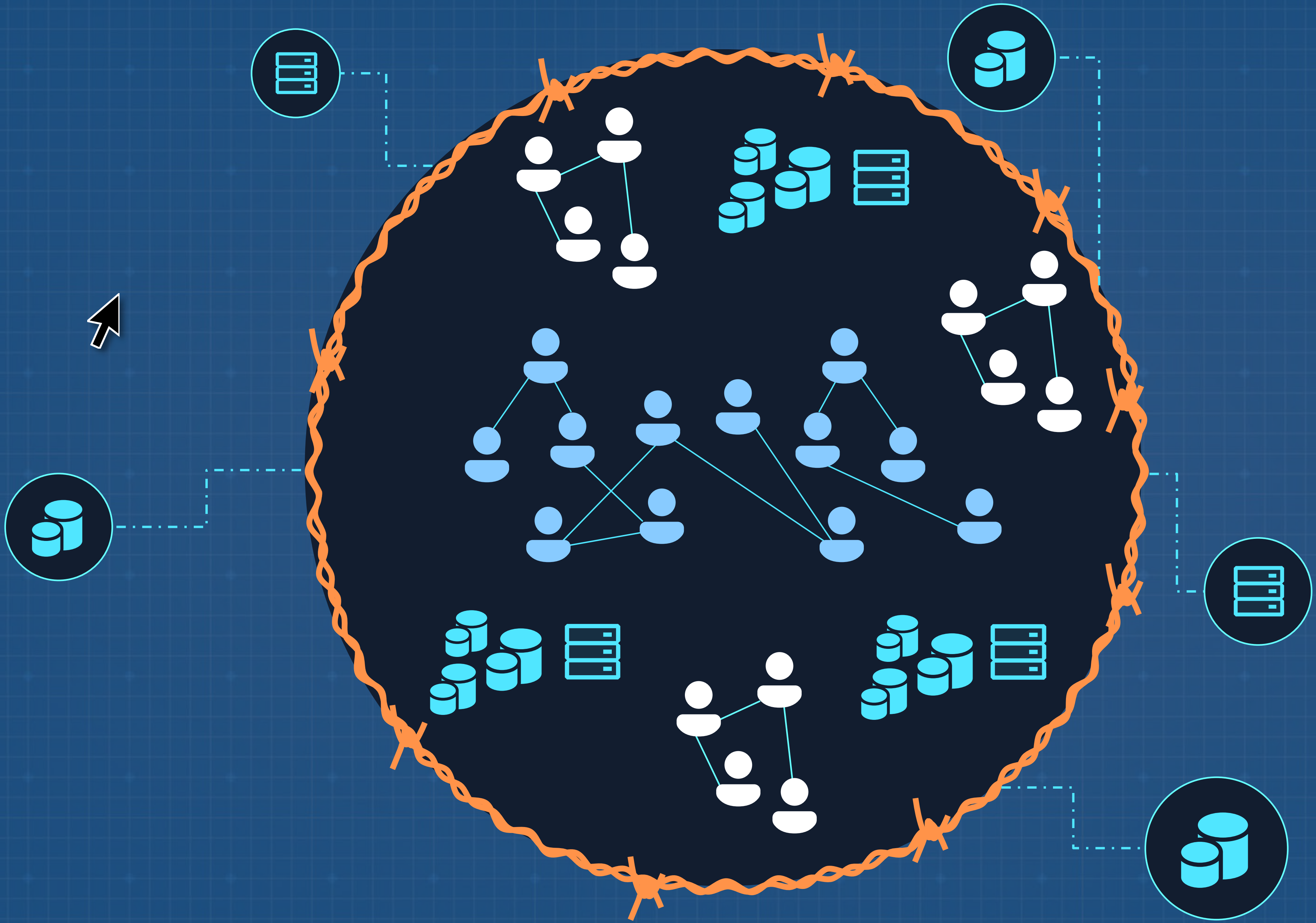
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

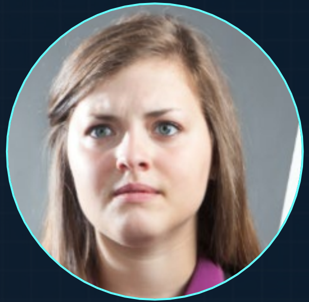
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.



Jane Doe

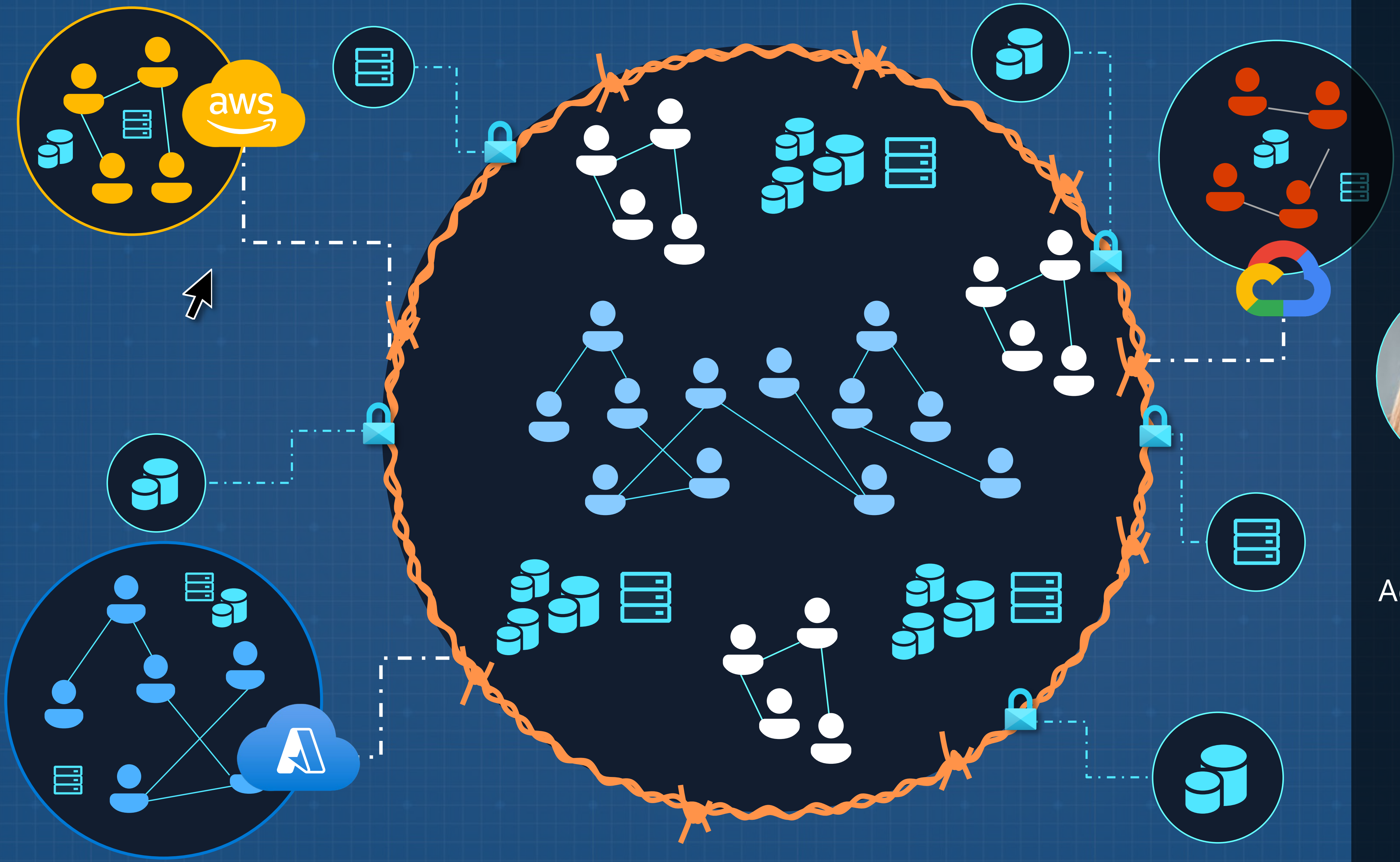
Identity Administrator

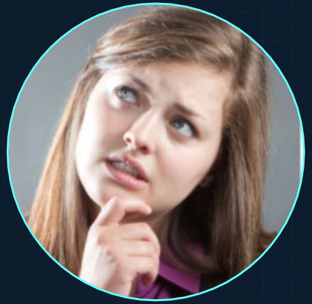




Jane Doe

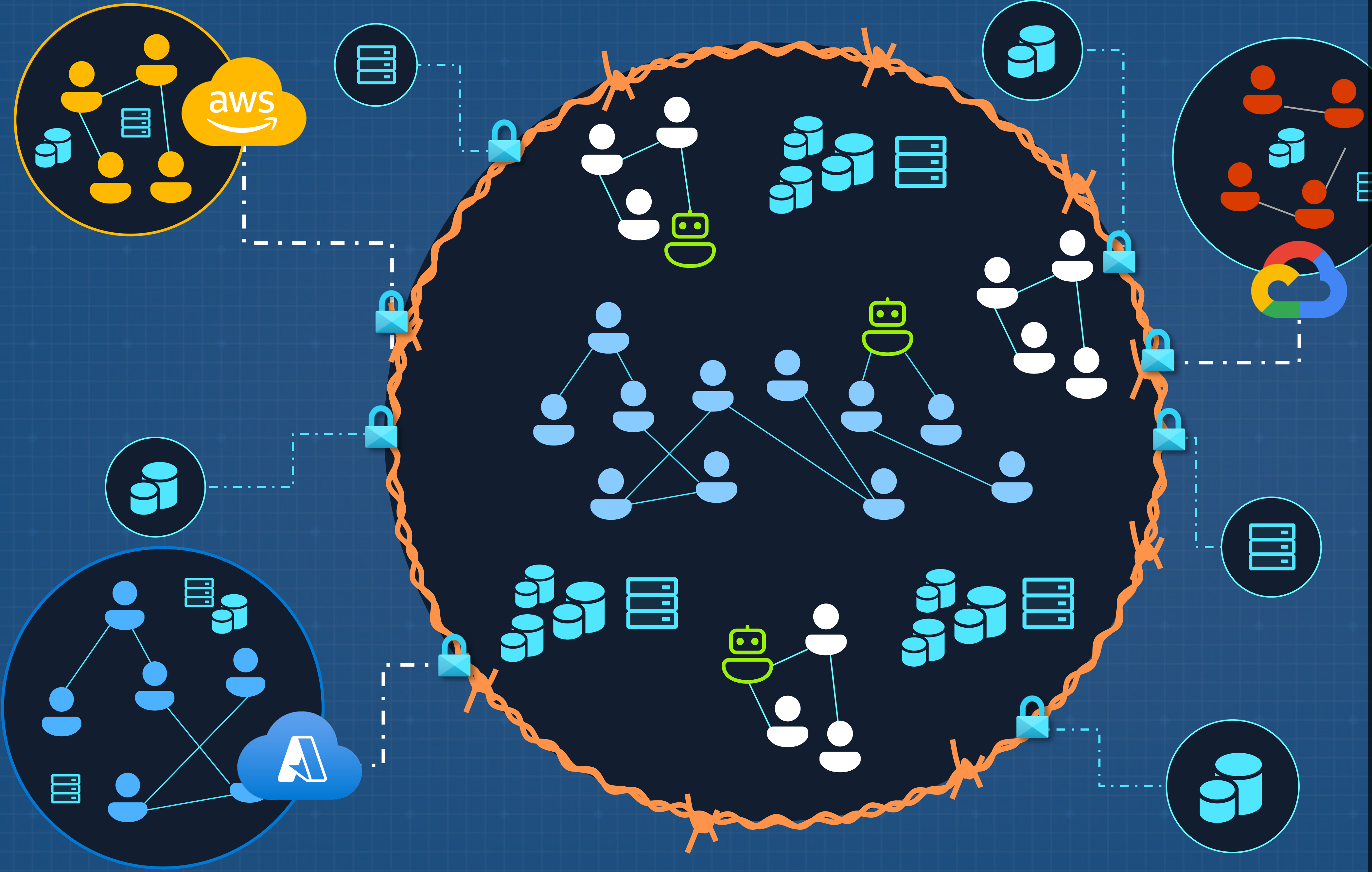
Identity Administrator

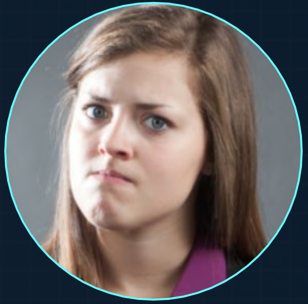




Jane Doe

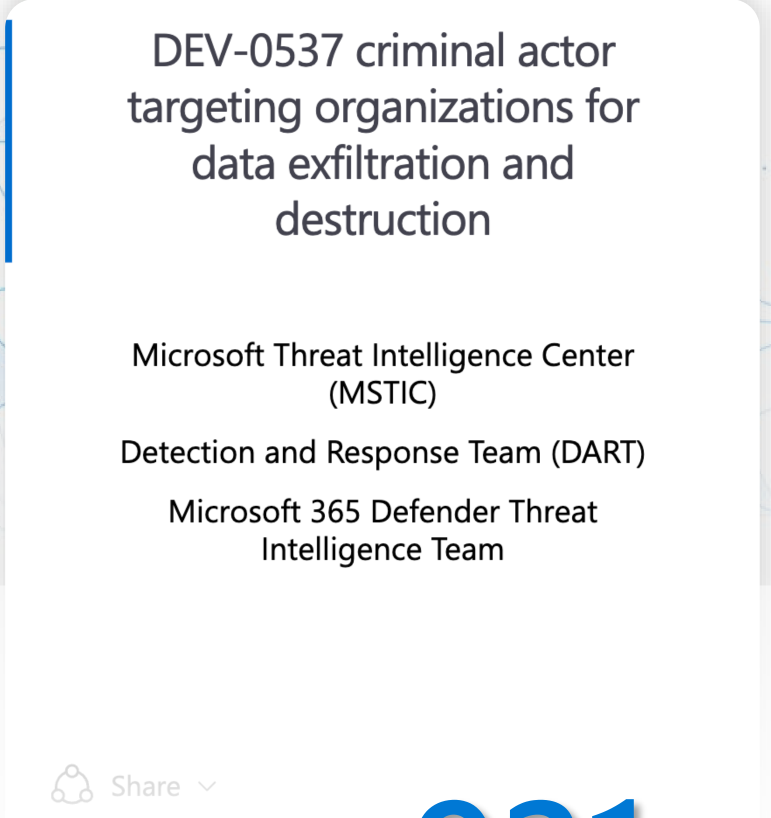
Identity Administrator





Jane Doe

Identity Administrator



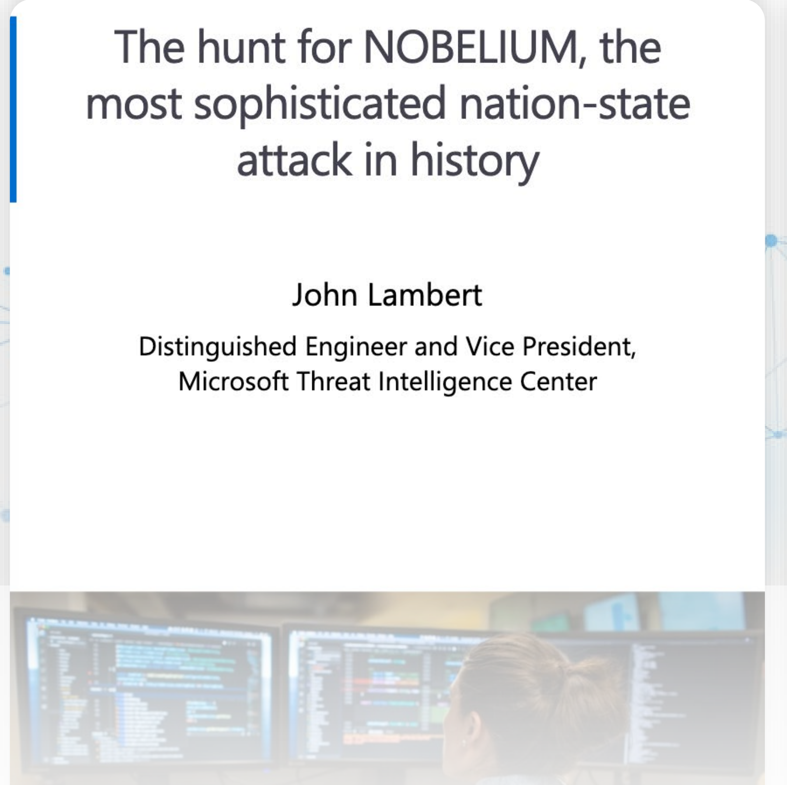
DEV-0537 criminal actor targeting organizations for data exfiltration and destruction

Microsoft Threat Intelligence Center (MSTIC)

Detection and Response Team (DART)

Microsoft 365 Defender Threat Intelligence Team

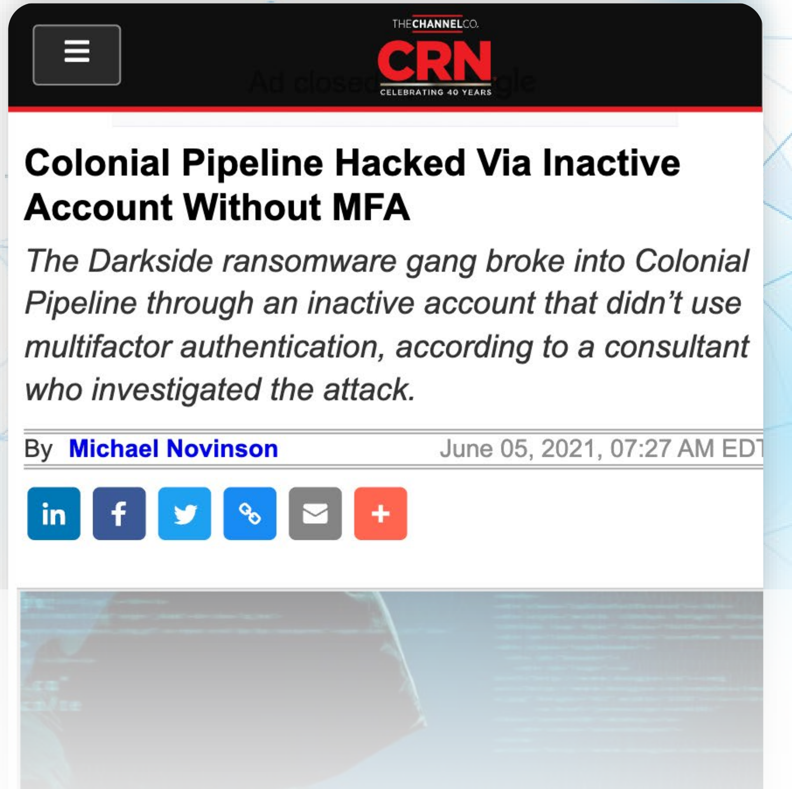
March 24, 2022 update – As Microsoft continues to track DEV-0537's activities, tactics and tools, we're sharing new detection, hunting



The hunt for NOBELIUM, the most sophisticated nation-state attack in history

John Lambert

Distinguished Engineer and Vice President, Microsoft Threat Intelligence Center



Colonial Pipeline Hacked Via Inactive Account Without MFA

The Darkside ransomware gang broke into Colonial Pipeline through an inactive account that didn't use multifactor authentication, according to a consultant who investigated the attack.

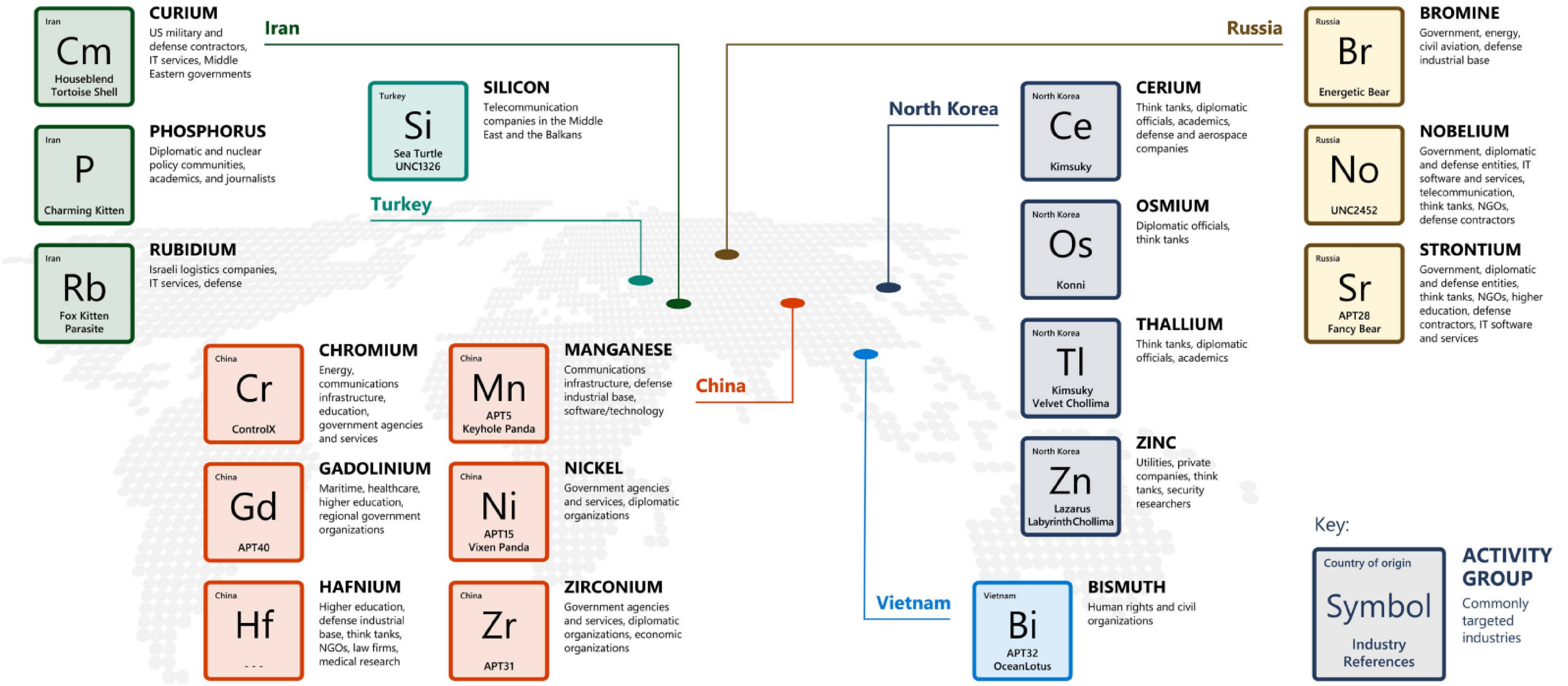
By **Michael Novinson** June 05, 2021, 07:27 AM EDT

921 password attacks every second

Nearly doubling in frequency over the past 12 months

Source: Microsoft Azure Active Directory (Azure AD) authentication log data. 2022.

Sprawl of nation state attacks



Iran

Iran
Cm
Houseblend
Tortoise Shell

CURIUM
US military and defense contractors, IT services, Middle Eastern governments

Iran
P
Charming Kitten

PHOSPHORUS
Diplomatic and nuclear policy communities, academics, and journalists

Iran
Rb
Fox Kitten
Parasite

RUBIDIUM
Israeli logistics companies, IT services, defense

Turkey

Turkey
Si
Sea Turtle
UNC1326

SILICON
Telecommunication companies in the Middle East and the Balkans

China

China
Cr
ControlX

CHROMIUM
Energy, communications infrastructure, education, government agencies and services

China
Mn
APT5
Keyhole Panda

MANGANESE
Communications infrastructure, defense industrial base, software/technology

China
Gd
APT40

GADOLINIUM
Maritime, healthcare, higher education, regional government organizations

China
Ni
APT15
Vixen Panda

NICKEL
Government agencies and services, diplomatic organizations

China
Hf
- - -

HAFNIUM
Higher education, defense industrial base, think tanks, NGOs, law firms, medical research

China
Zr
APT31

ZIRCONIUM
Government agencies and services, diplomatic organizations, economic organizations

Russia

Russia
Br
Energetic Bear

BROMINE
Government, energy, civil aviation, defense industrial base

Russia
No
UNC2452

NOBELIUM
Government, diplomatic and defense entities, IT software and services, telecommunication, think tanks, NGOs, defense contractors

Russia
Sr
APT28
Fancy Bear

STRONTIUM
Government, diplomatic and defense entities, think tanks, NGOs, higher education, defense contractors, IT software and services

North Korea

North Korea
Ce
Kimsuky

CERIUM
Think tanks, diplomatic officials, academics, defense and aerospace companies

North Korea
Os
Konni

OSMIUM
Diplomatic officials, think tanks

North Korea
Tl
Kimsuky
Velvet Chollima

THALLIUM
Think tanks, diplomatic officials, academics

North Korea
Zn
Lazarus
LabyrinthChollima

ZINC
Utilities, private companies, think tanks, security researchers

Vietnam

Vietnam
Bi
APT32
OceanLotus

BISMUTH
Human rights and civil organizations

Key:

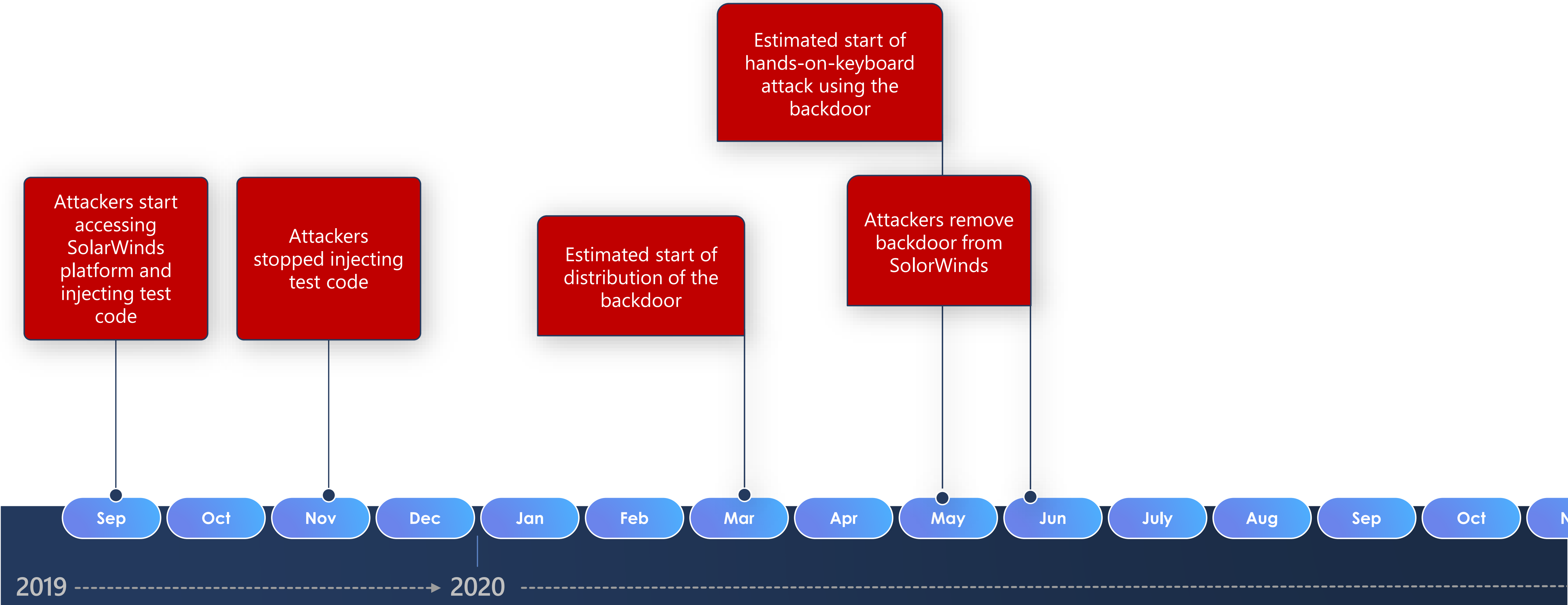
Country of origin
Symbol
Industry References

ACTIVITY GROUP
Commonly targeted industries

source: 2020 Microsoft Digital Defense Report

aka.ms/MicrosoftDigitalDefenseReport

What we learned from the NOBELIUM attacks



Attackers start accessing SolarWinds platform and injecting test code

Attackers stopped injecting test code

Estimated start of distribution of the backdoor

Estimated start of hands-on-keyboard attack using the backdoor

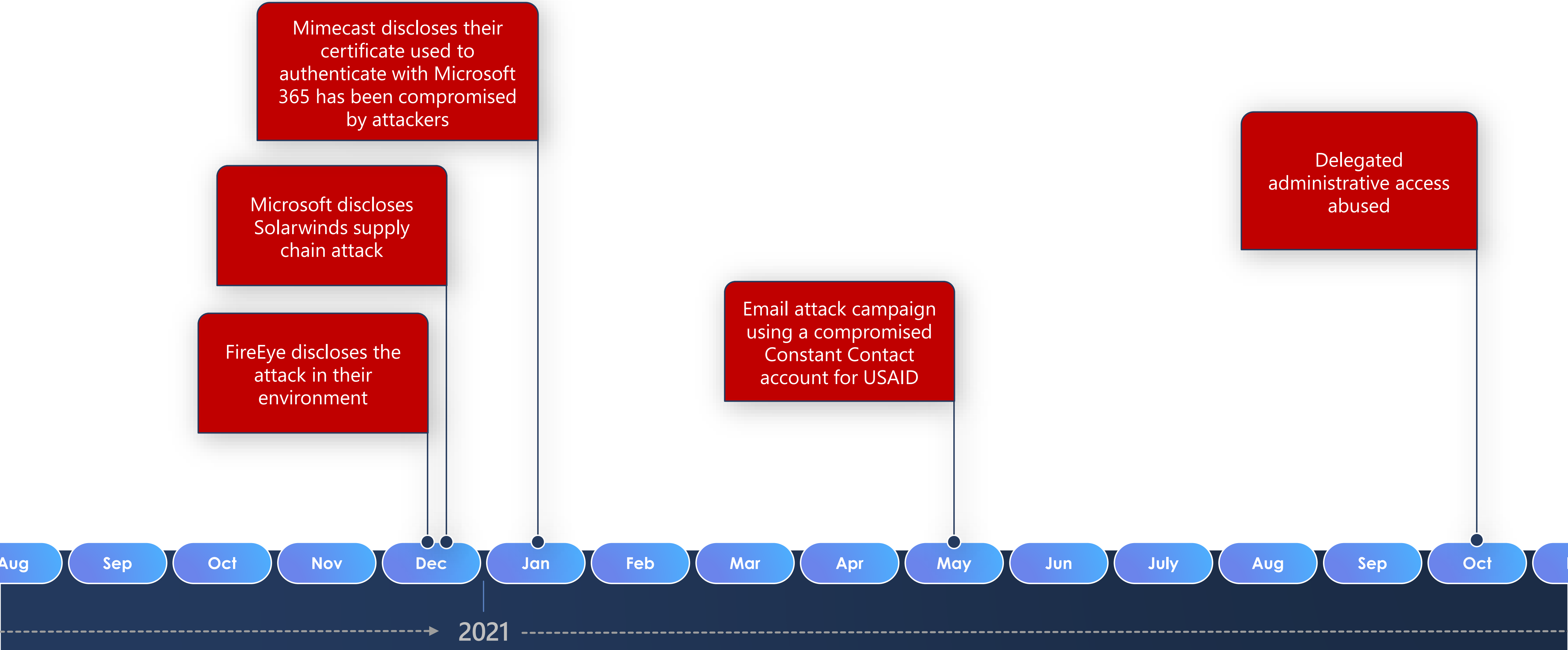
Attackers remove backdoor from SolorWinds

Sep | Oct | Nov | Dec | Jan | Feb | Mar | Apr | May | Jun | July | Aug | Sep | Oct | N

2019 → 2020

Sources: FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community, Dec. 8, 2020 | Important Update from Mimecast, Jan. 12, 2021 | FoggyWeb: Targeted NOBELIUM malware leads to persistent backdoor, Sept. 27, 2021

What we learned from the NOBELIUM attacks



FireEye discloses the attack in their environment

Microsoft discloses Solarwinds supply chain attack

Mimecast discloses their certificate used to authenticate with Microsoft 365 has been compromised by attackers

Email attack campaign using a compromised Constant Contact account for USAID

Delegated administrative access abused

Sources: FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community, Dec. 8, 2020 | Important Update from Mimecast, Jan. 12, 2021 | FoggyWeb: Targeted NOBELIUM malware leads to persistent backdoor, Sept. 27, 2021

NOBELIUM

What we learned from the NOBELIUM attacks

Suspicious **high-risk actions were allowed,** and **Workload identities** were used

Abuse of delegated admin permissions granted to managed or cloud service providers

Suspicious high-risk **actions went undetected**, time it took to detect issues

We need to reimagine the access security strategy

Definition

Zero Trust strategy

A proactive, integrated approach to security across all layers of the digital estate that explicitly and continuously verifies every transaction, asserts least privilege, and relies on intelligence, advanced detection, and real-time response to respond to threats.

Zero Trust guiding principles

- Verify explicitly
- Use least privileged access
- Assume breach

Secure access with the Zero Trust strategy

1. Strengthen access for all identities

2. Ensure least privilege for all admins

3. Utilize cloud intelligence across boundaries

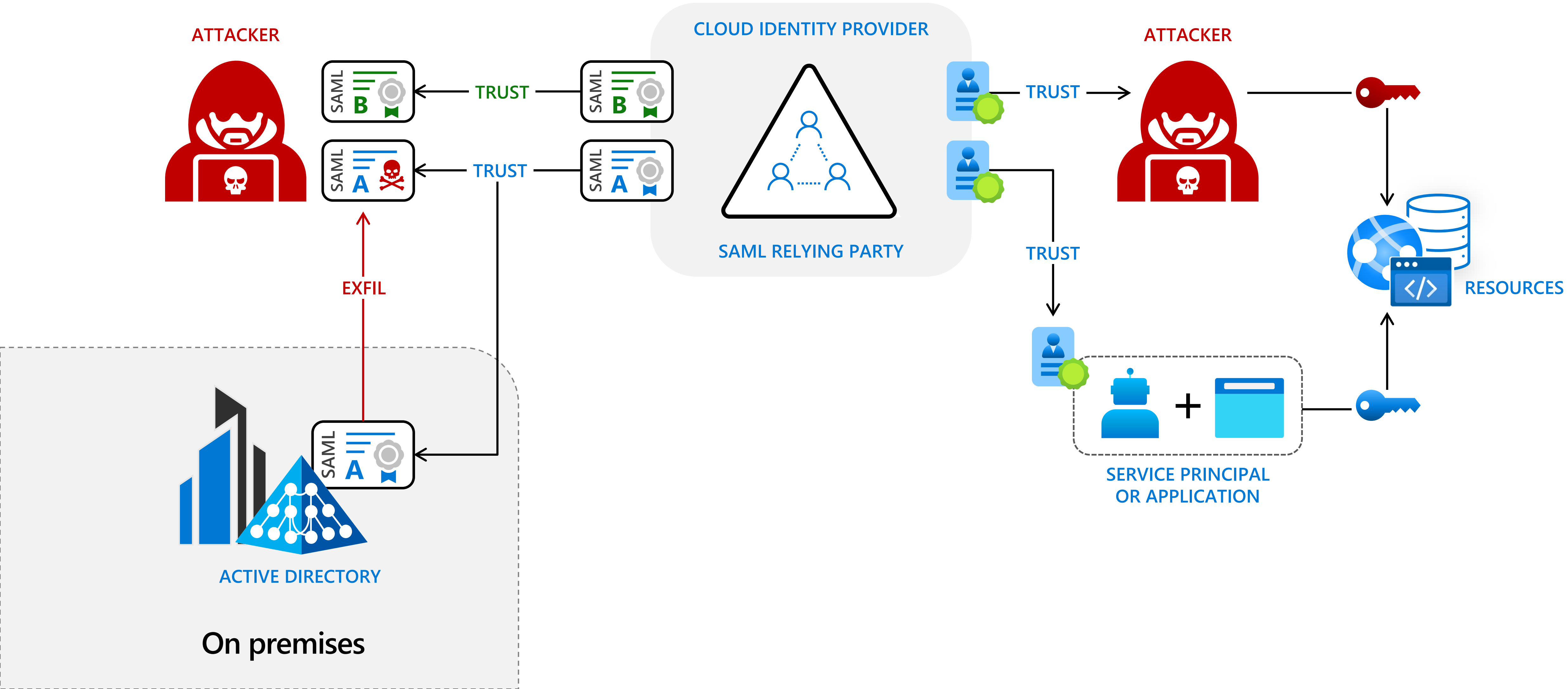
Secure access with the Zero Trust strategy

1 Strengthen access for all identities

2 Ensure least privilege for all admins

3 Utilize cloud intelligence across boundaries

Back to December 2020…



PROTECT HIGH RISK ACTIONS

Attacker forged tokens with admin privileges to make configuration changes

Recommendations

- Require fresh authentication for high-risk actions
- Require phish resistant MFA and secure/privileged access workstations
- Use risk signals to block any high-risk actions

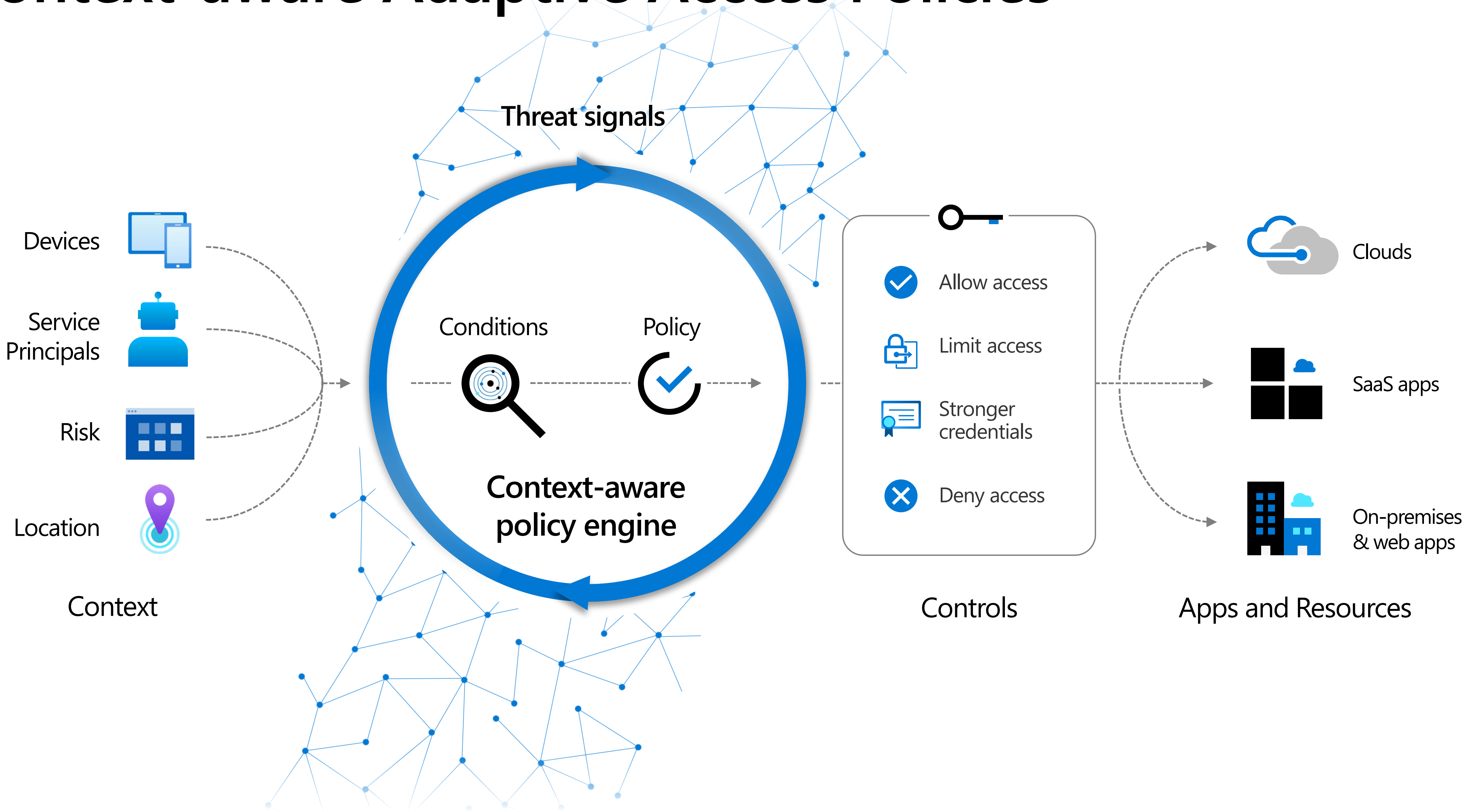
SECURE ACCESS FOR WORKLOAD IDENTITIES

Attacker added credentials to the service principal to access data

Recommendations

- Restrict access based on context (location, app, etc)
- Use risk to make access decisions
- Use stronger credentials and limit lifetimes

Context-aware Adaptive Access Policies



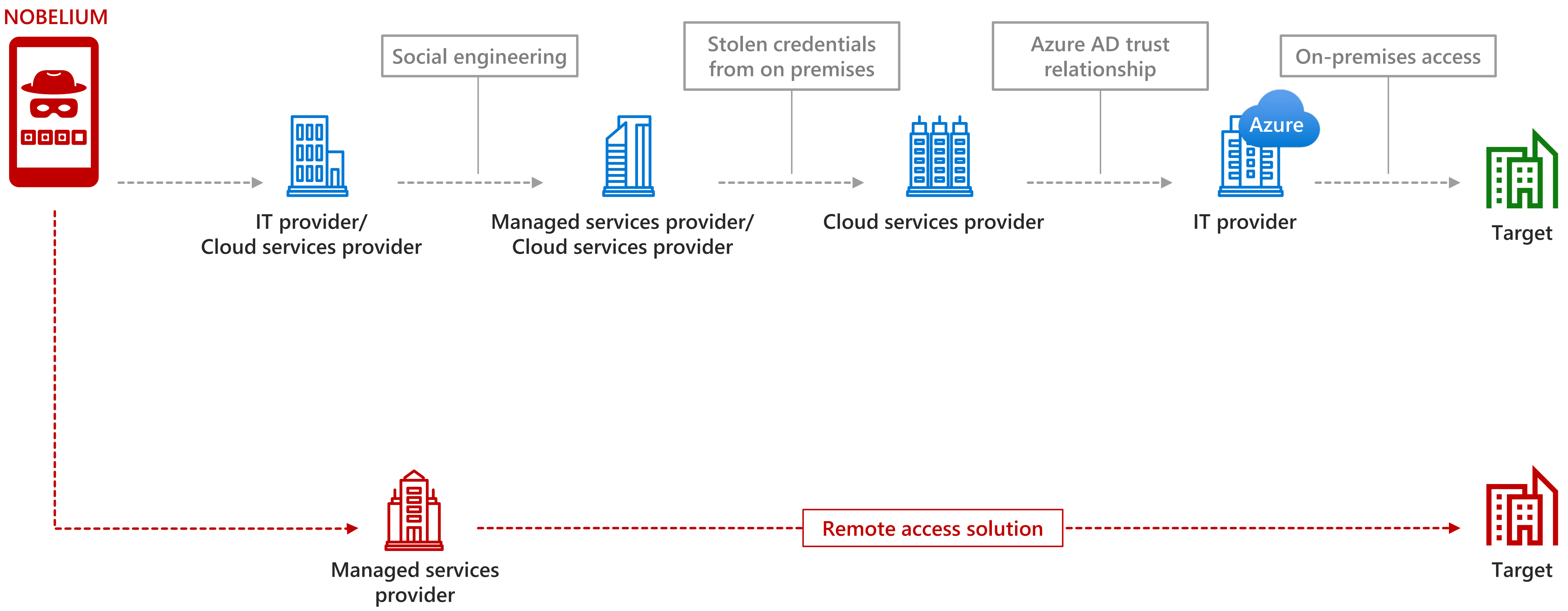
Secure access with the Zero Trust strategy

1 Strengthen access for all identities

2 Ensure least privilege for all admins

3 Utilize cloud intelligence across boundaries

Nobelium took advantage of trusted relationships


NOBELIUM
Social engineering
Stolen credentials from on premises
Azure AD trust relationship
On-premises access
Azure
IT provider/ Cloud services provider
Managed services provider/ Cloud services provider
Cloud services provider
IT provider
Target
Managed services provider
Remote access solution
Target

Wide spectrum of trusted relationships

More in-house
More outsourced

IN HOUSE	CO-MANAGED	OUTSOURCED
Managed in-house with FTEs sometimes with vendor staff augmentation	Co-managed with partner Customer-specific processes & configuration	Partner-managed: Common processes & tooling
SERVED BY		
In-house, Vendor	Systems Integrator	CSP/MSP
STAFFING		
Customer FTE, Partner vendor	Partner staffing often "Dedicated" per customer	Partner staffing often "Shared" across customers
TECHNICIAN ACCOUNTS AND ACCESS		
Technician access assigned to regular user account in **customer** tenant	Technician access assigned to guest account in customer tenant, visible in customer tenant	Technician access assigned to user account in **partner** tenant, typically not visible in customer tenant

IT ALL STARTS WITH THE CONTRACT

Attackers relied on lack of controls across the MSP-Customer relationships

Recommendations

- Review the contract: Are there contractual limitations preventing you from enabling controls?
- Verify that proper controls are maintained within the MSP: Multi-factor authentication, just-in-time access, process for granting privileged access

LEAST PRIVILEGE FOR DELEGATED ADMINS

Attackers relied on MSPs having standing privileged access to customer environments

Recommendations

- Monitor alerts on anomalous access
- Require just-in-time (JIT) access with risk-based checks for admin access
- Ensure admins only have just enough access (JEA) through automated or manual role-sizing
- Coarse-grained roles -> finer-grained tasks

LIFECYCLE CONTROLS

Admin accounts were poorly vetted **and** persisted long after required

Recommendations

- Adopt a request-and-approval workflow for new delegated admins
- Periodic and event-triggered access certification of privileged users
- Automatic expiration of admins and removal of guests from directory
- Evaluate type of account needed by admins

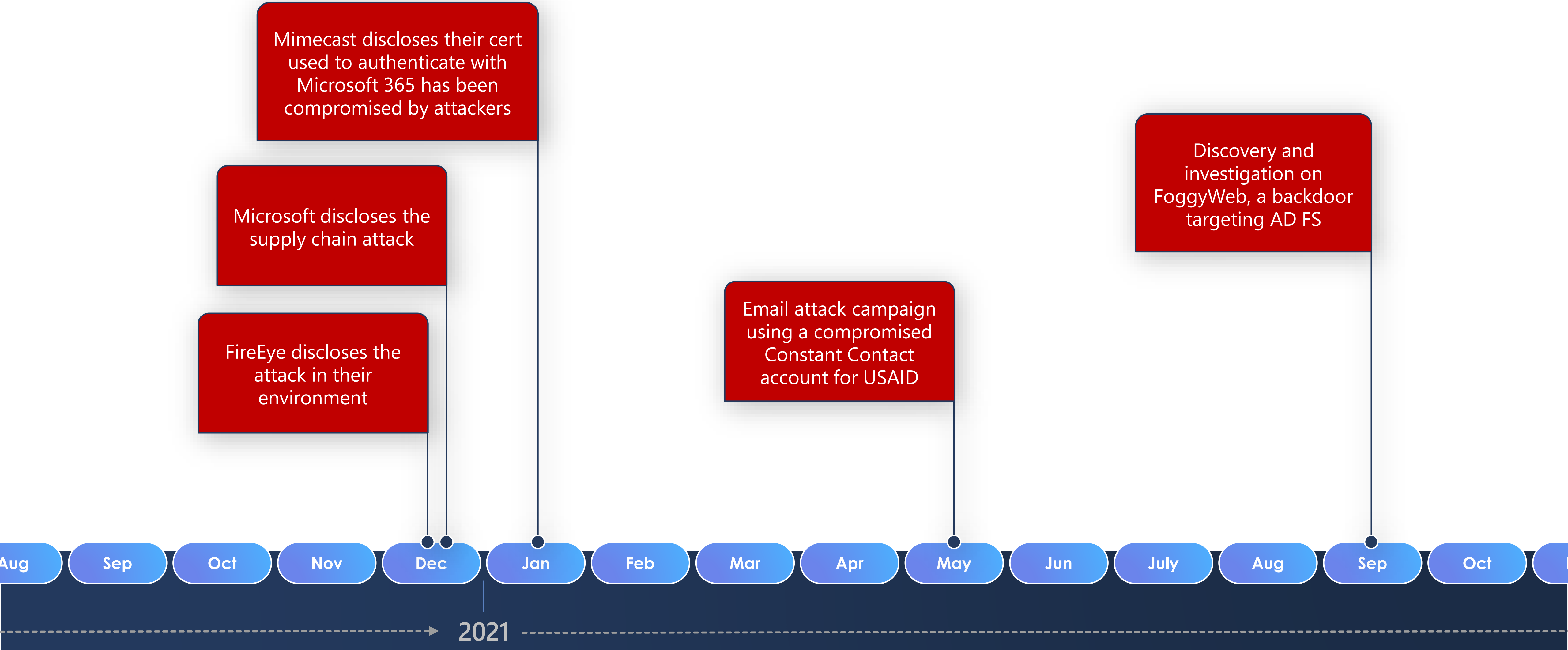
Secure access with the Zero Trust strategy

1 Strengthen access for all identities

2 Ensure least privilege for all admins

3 Utilize cloud intelligence across boundaries

NOBELIUM attack timeline



Mimecast discloses their cert used to authenticate with Microsoft 365 has been compromised by attackers

Microsoft discloses the supply chain attack

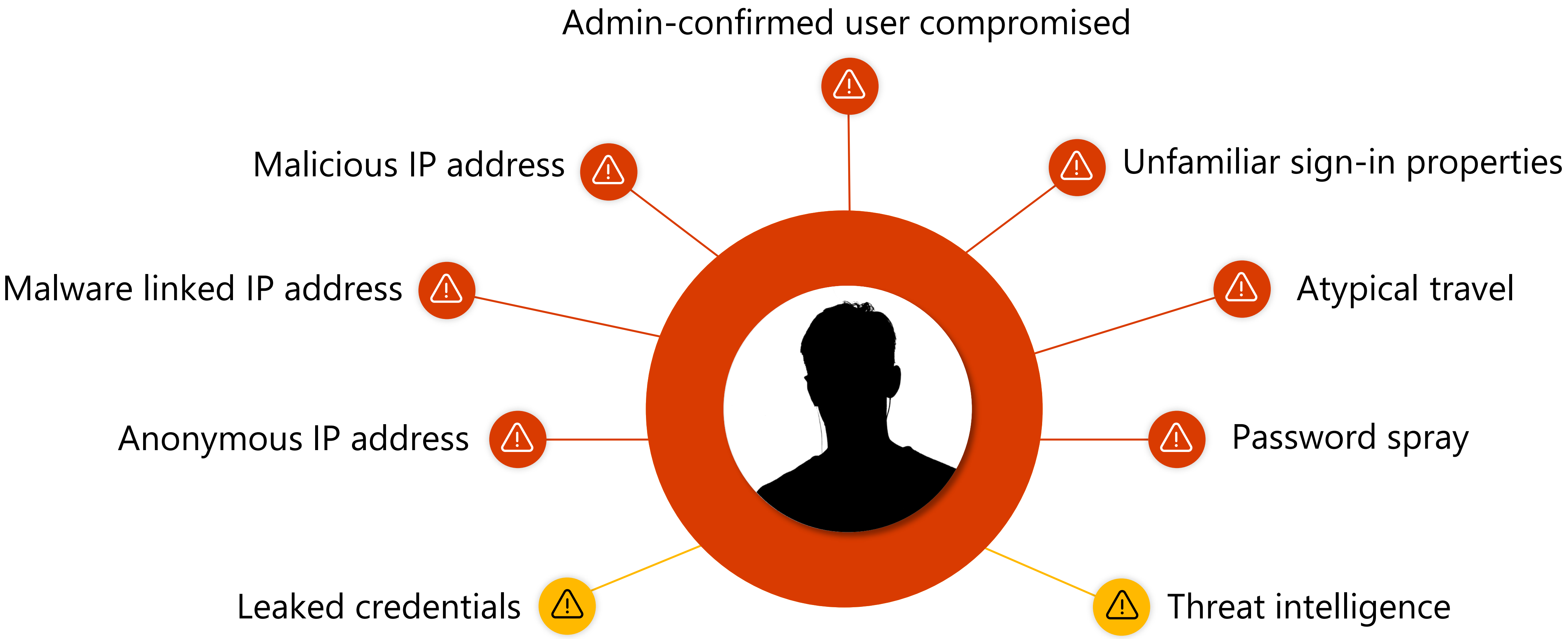
FireEye discloses the attack in their environment

Email attack campaign using a compromised Constant Contact account for USAID

Discovery and investigation on FoggyWeb, a backdoor targeting AD FS

Sources: **FireEye:** https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html
Mimecast: https://www.mimecast.com/blog/important-update-from-mimecast **FoggyWeb:** https://www.microsoft.com/security/blog/2021/09/27/foggyweb-targeted-nobelium-malware-leads-to-persistent-backdoor

Sign in risk detections



Admin-confirmed user compromised

Malicious IP address

Unfamiliar sign-in properties

Malware linked IP address

Atypical travel

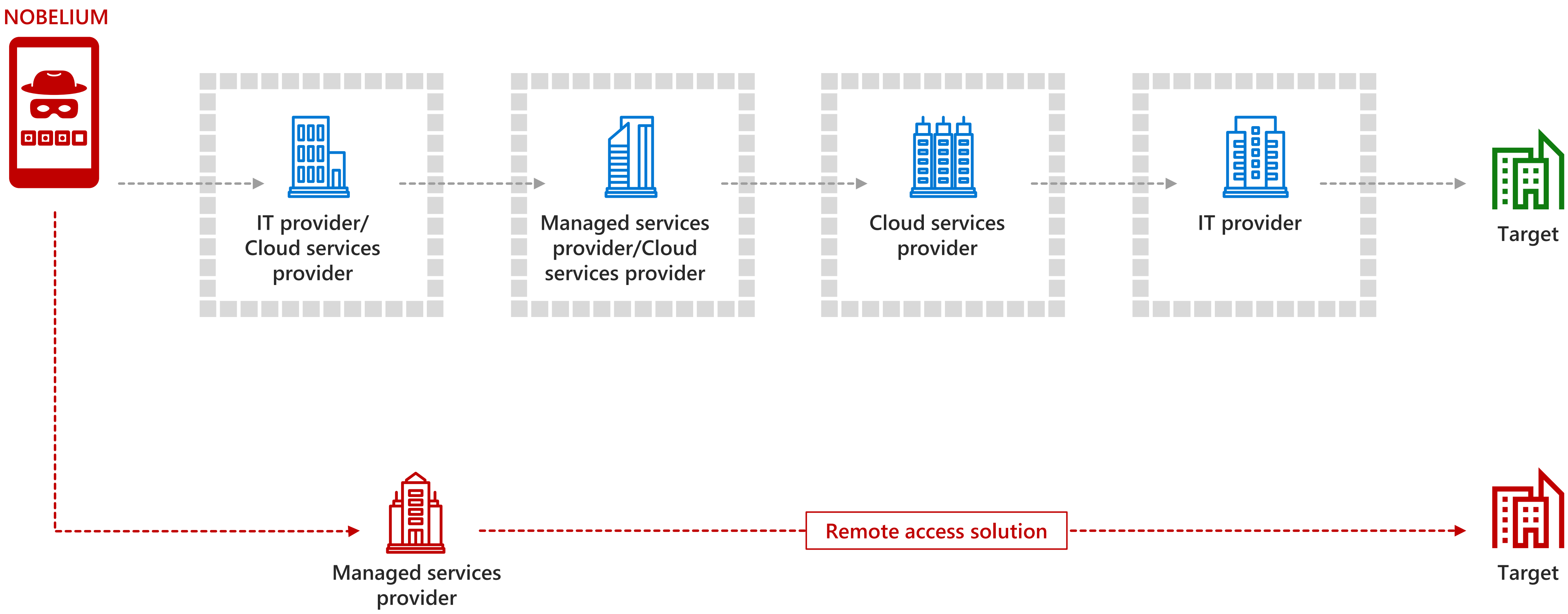
Anonymous IP address

Password spray

Leaked credentials

Threat intelligence

Permissions across boundaries


NOBELIUM
IT provider/ Cloud services provider
Managed services provider/Cloud services provider
Cloud services provider
IT provider
Target
Managed services provider
Remote access solution
Target

REVIEW CROSS BOUNDARY SIGNALS

Attackers relied on lack of visibility across boundaries

Recommendations

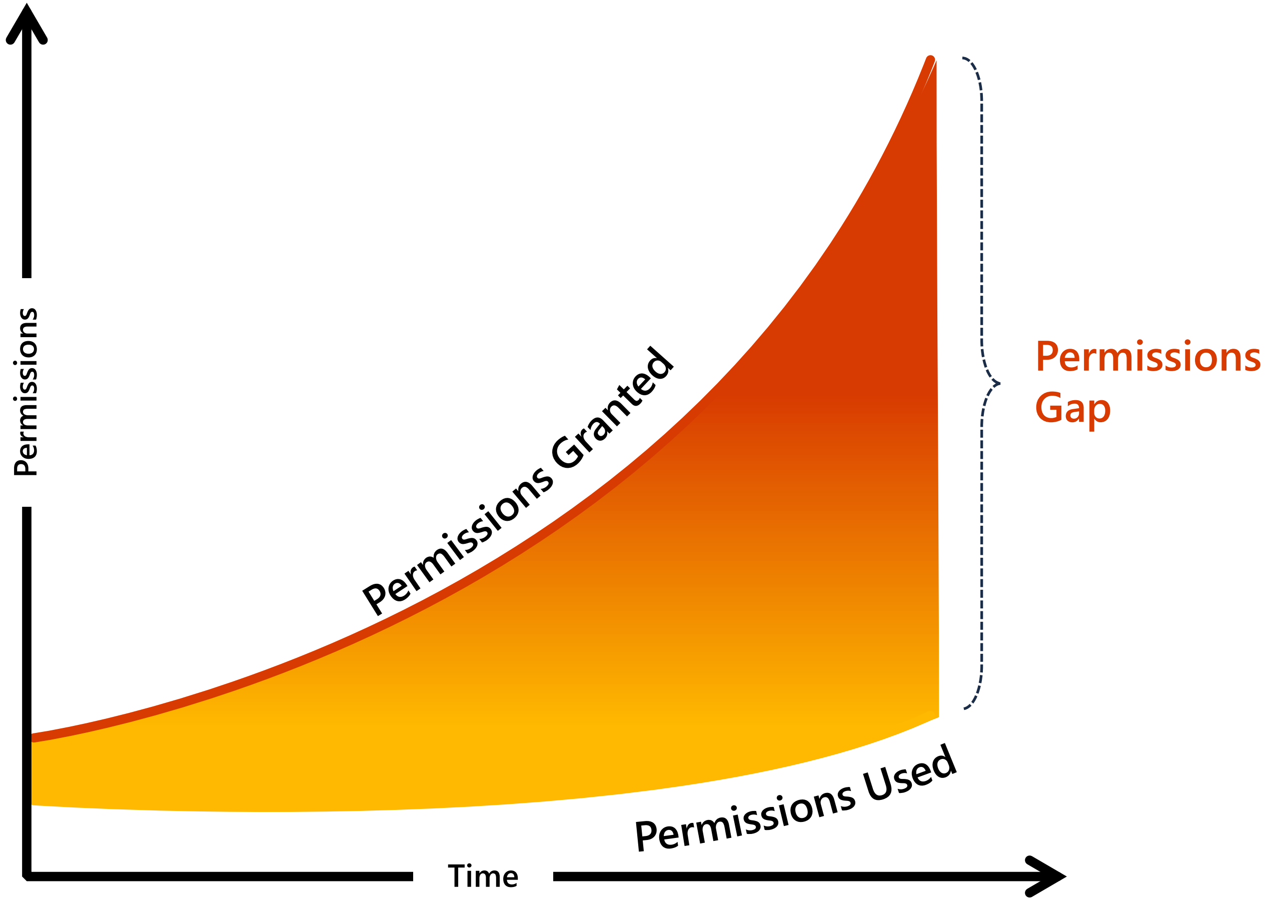
- Audit cross-tenant sign-ins and configuration changes, especially by delegated admins
- Review log availability and retention strategies
- Evaluate logs for adequacy and anomalies
- Collect all logs in a single place for forensics
- Utilize behavioral analysis and ML to alert on suspicious changes

Unmanaged permissions expand your attack surface

40,000+ permissions across clouds and growing daily

>50% of permissions are high-risk

>90% of identities are using **<5%** of permissions granted



DATA-DRIVEN PERMISSIONS MANAGEMENT

Attackers maintained permissions that were used for later abuse

Recommendations

- Evaluate cloud-permissions management tools for your Identities across SaaS Apps and IaaS platforms
- Grant permissions based on usage and activity
- Review unused or stale accounts periodically
- Continuously monitor and right-size identities to prevent permissions creep
- Tie findings into a governance tool so you can ensure that least privilege is maintained across clouds

Secure access strategies for Zero Trust architecture

- Strengthen access for all identities
- Ensure least privilege for all administrators
- Use cloud intelligence across boundaries

Invest in a holistic and integrated approach to access security

and, please, turn on MFA

RSA Conference2022

Thank you!

Nitika Gupta

@_Nitika_Gupta

Rahul Prakash

@RahPrak