

# The Evolving Cyber Threat Landscape

**Michael Freistetter**  
**Tim Stock**

Cloud Solution Architect Security



## The New York Times

### *Once, Superpower Summits Were About Nukes. Now, It's Cyberweapons.*

But with the ease of denying responsibility and the wide range of possible attackers, the traditional deterrents of the nuclear age no longer work.

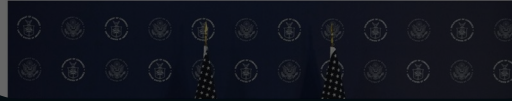


## POLITICO

CYBERSECURITY

### Chinese hackers nab 60,000 emails in State Department breach

Among the most sensitive information stolen, the staffer said, were victims' travel itineraries and diplomatic deliberations.



## The New York Times

### *In Cyberattacks, Iran Shows Signs of Improved Hacking Capabilities*

A monthslong hacking campaign targeted the governments of regional rivals, including Israel, and marked a turn, a new report says, as the attacks were used to collect intelligence, not just disrupt services.

Share full article

## The Washington Post

TECH POLICY

### Cybersecurity faces a challenge from artificial intelligence's rise

While defenders have been racing to keep pace with increasingly sophisticated threats, progress

By Joseph Menn  
May 11, 2023 at 7:00 a.m. EDT



### Cybercrime to Cost the World \$405 Trillion Annually by 2025

If it were measured as a country, then cybercrime – which is predicated to inflict damages totaling \$6 trillion USD globally in 2021 – would be the world's third largest economy after the U.S. and China.

## THE WALL STREET JOURNAL

### The Chinese groups accused of hacking the U.S. on Tech



## FINANCIAL TIMES

Cyber Security

+ Add to myFT

### ECB tells banks to run cyber stress tests after rise in hacker attacks

Lenders will assess online resilience after 'significant increase' in incidents since outbreak of Ukraine war



## The Washington Post

THE CYBERSECURITY 2022

### Think ransomware gangs won't thrive this year? Think again, experts say

Analysis by Tim Shorrock  
with research by David S. Schwartz  
March 20, 2022 at 10:52 a.m. EDT

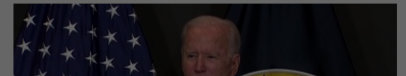
Comment 1 Get Email Sign

Welcome to The Cybersecurity 2022! And greetings from just

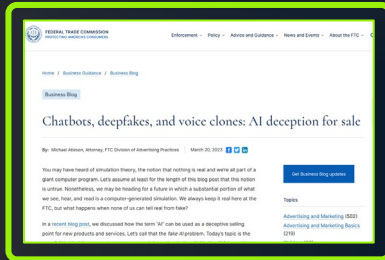


World

### Biden: If U.S. has 'real shooting war' it could be result of cyber attacks

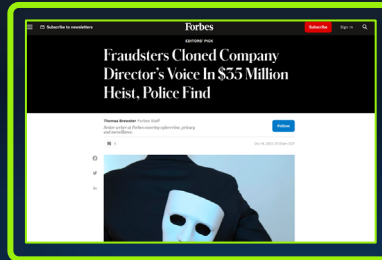


# AI-enabled Cyberattacks



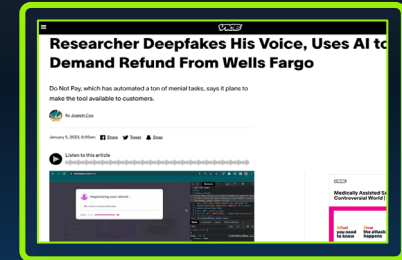
[Chatbots, deepfakes and voice clones](#)

Federal Trade Commission Article



[Fraudsters Cloned Company Directors Voice](#)

Forbes Article



[Researcher Deepfakes His Voice](#)

Vice Article



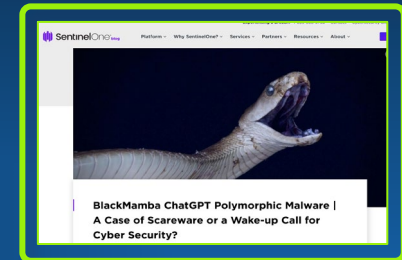
[WithSecure-Creatively Malicious](#)

PDF



[How Hackers Use Generative AI](#)

Article



[Blackmamba Chatgpt polymorphic](#)

Blog post

# Ransomware infection to full victim encryption

3 Days

2019



# Ransomware infection to full victim encryption

1 Day

2021





Today

<15 Minutes



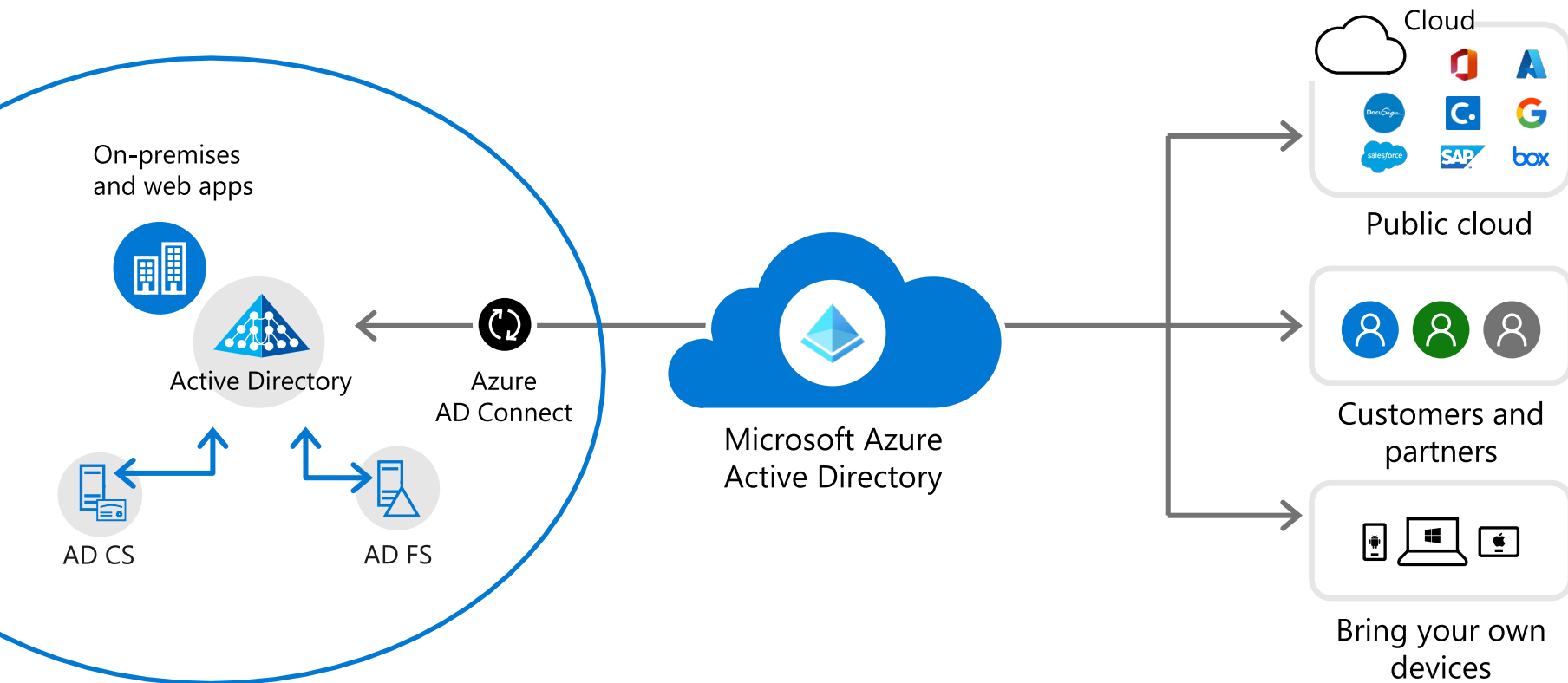
Destructive human operated ransomware breach to full tenant encryption  
fueled by the growth in **cybercrime-as-a-service**

Protection?



# Enterprise identity security landscapes

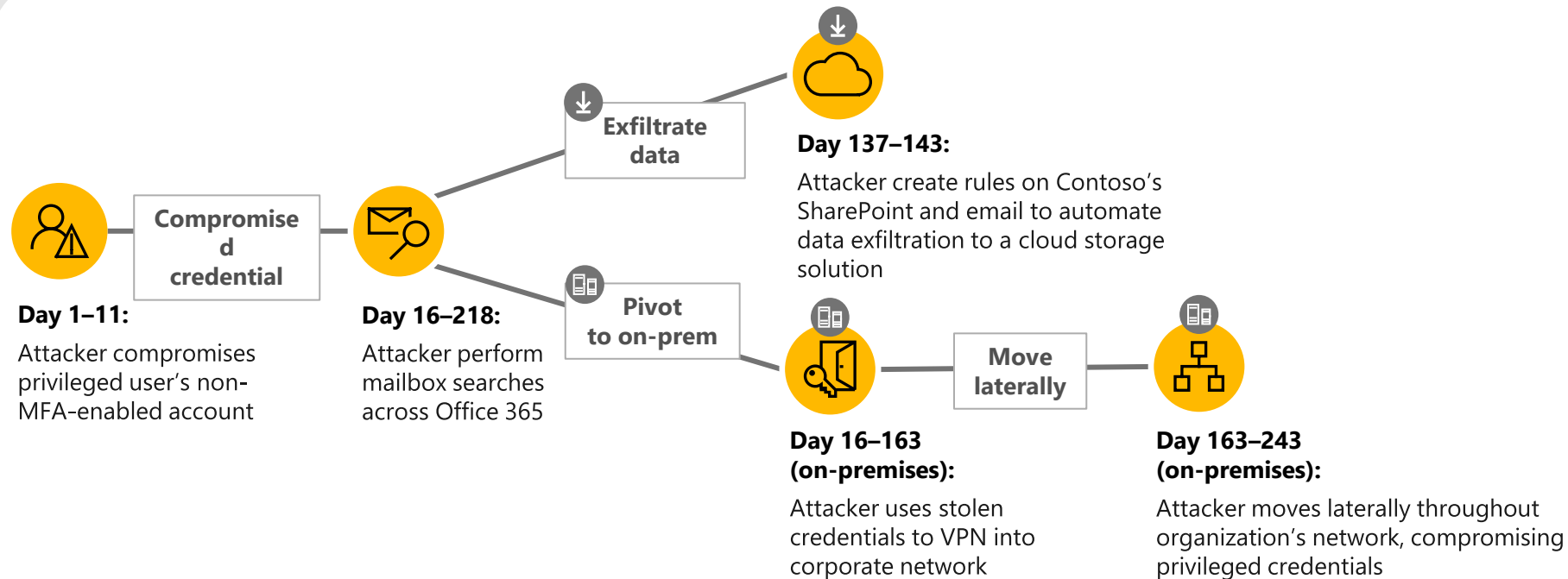
Security environments are complex—and include both on-premises and cloud assets





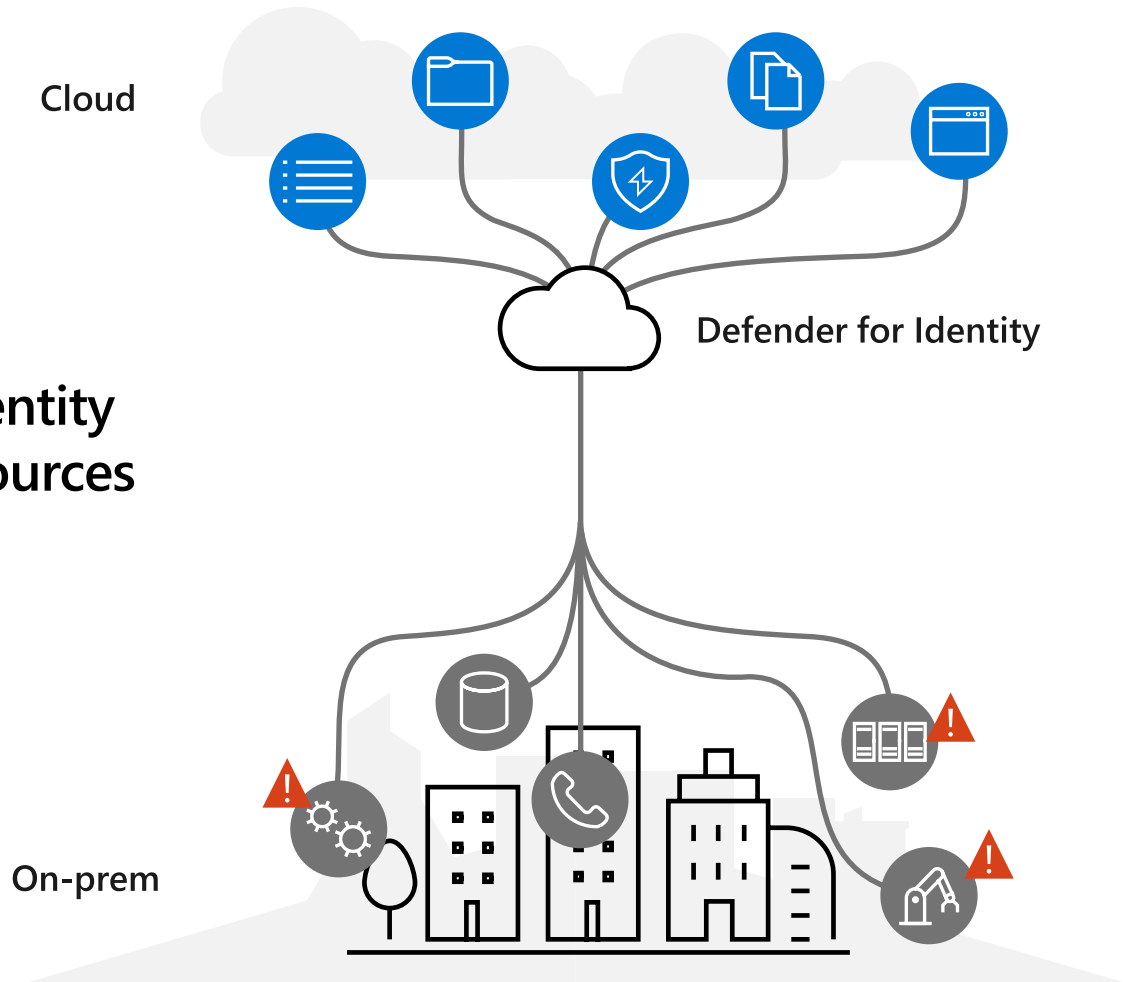
# Anatomy of an on-premises and cloud environment attack

An example of an attack that compromises an entire organization





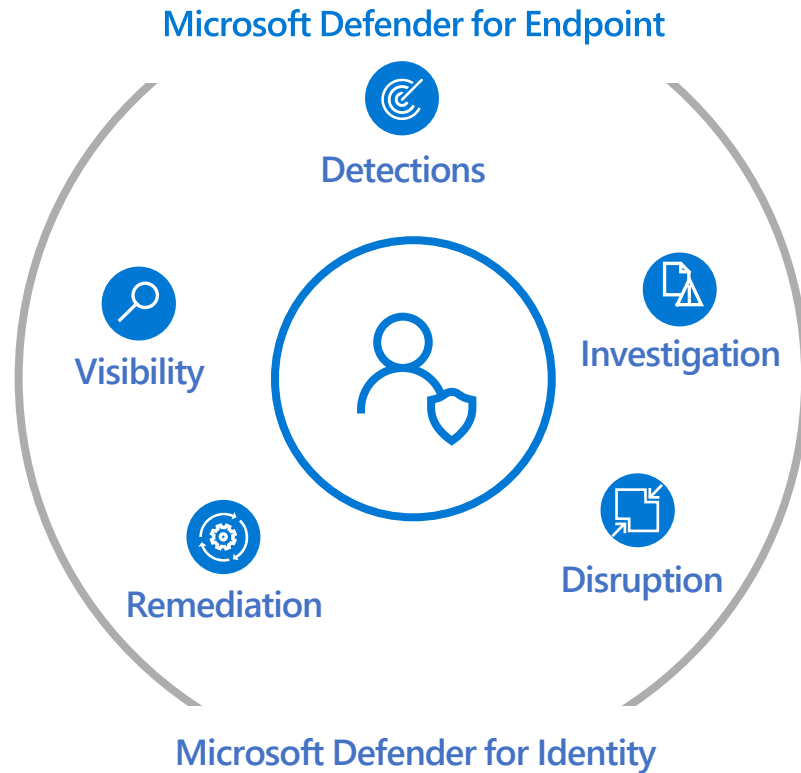
Microsoft Defender for Identity  
monitors on-premises resources  
and integrates with cloud  
security solutions



# MDI and MDE Better Together

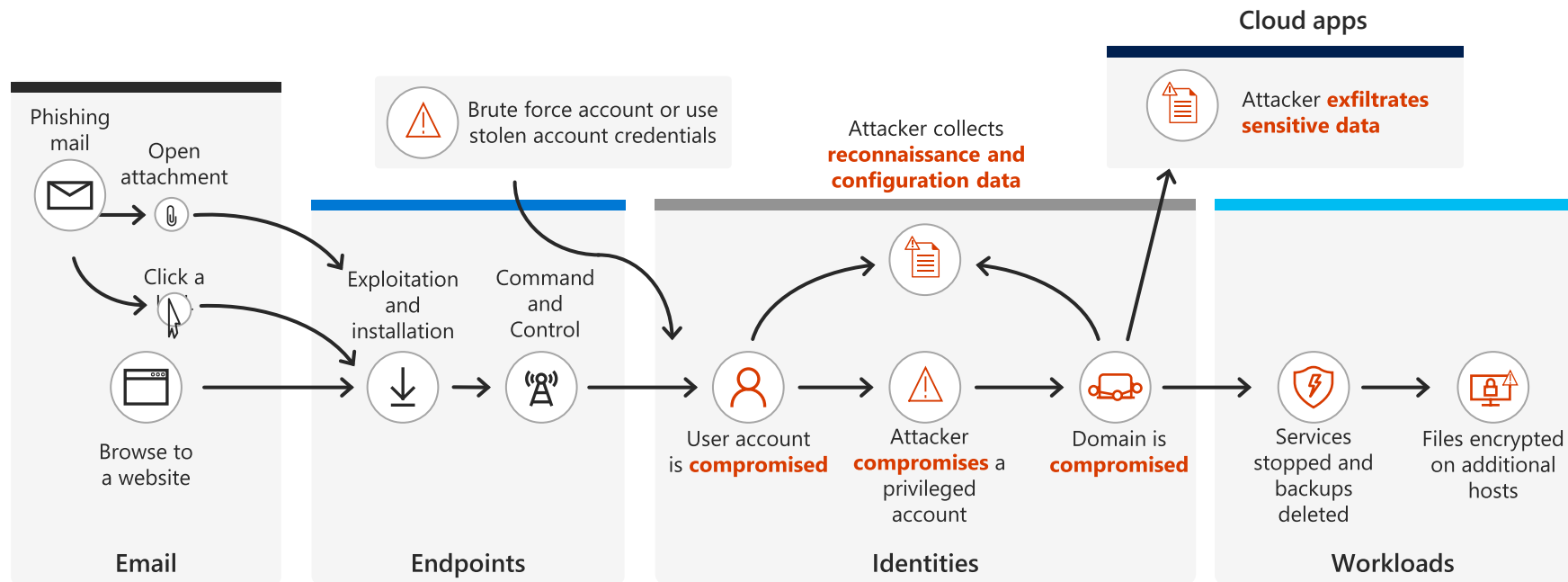


MDE + MDI = XDR



# Attacks are crossing modalities

## Typical human-operated ransomware campaign

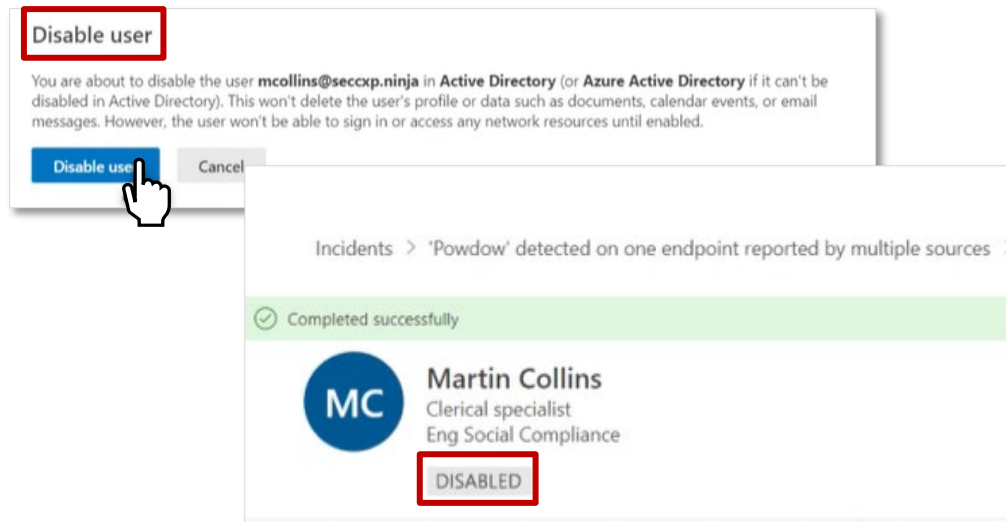




# Supported Actions (MDI)

## Disable user in Active Directory

- Leverage MDI's remediation actions
- Prevent user from logging in to the on-premises network
- Identity status will be synced to AAD in the next AD sync



And Cloud?



# Entra ID Protection

Unique insights powered  
by trillions of signals



## Autogenerated

- High quality heuristic-based detections
- Detections from other first parties



## Expert generated

- Security researchers
- Customer support
- Dedicated human labelers



## End user generated

- Build feedback loops
- End users/admins/secops
- Remove errors

Assess Risk Levels via  
real-time evaluation engine



Risky Users



Risky Sign-ins



Risky Workload Identities

Secure Access via policy  
enforcement and unified  
investigation experience



Auto-remediation with  
Risky based CA policies



Azure Portal Identity  
Protection risk reporting  
dashboard and Microsoft  
Graph API



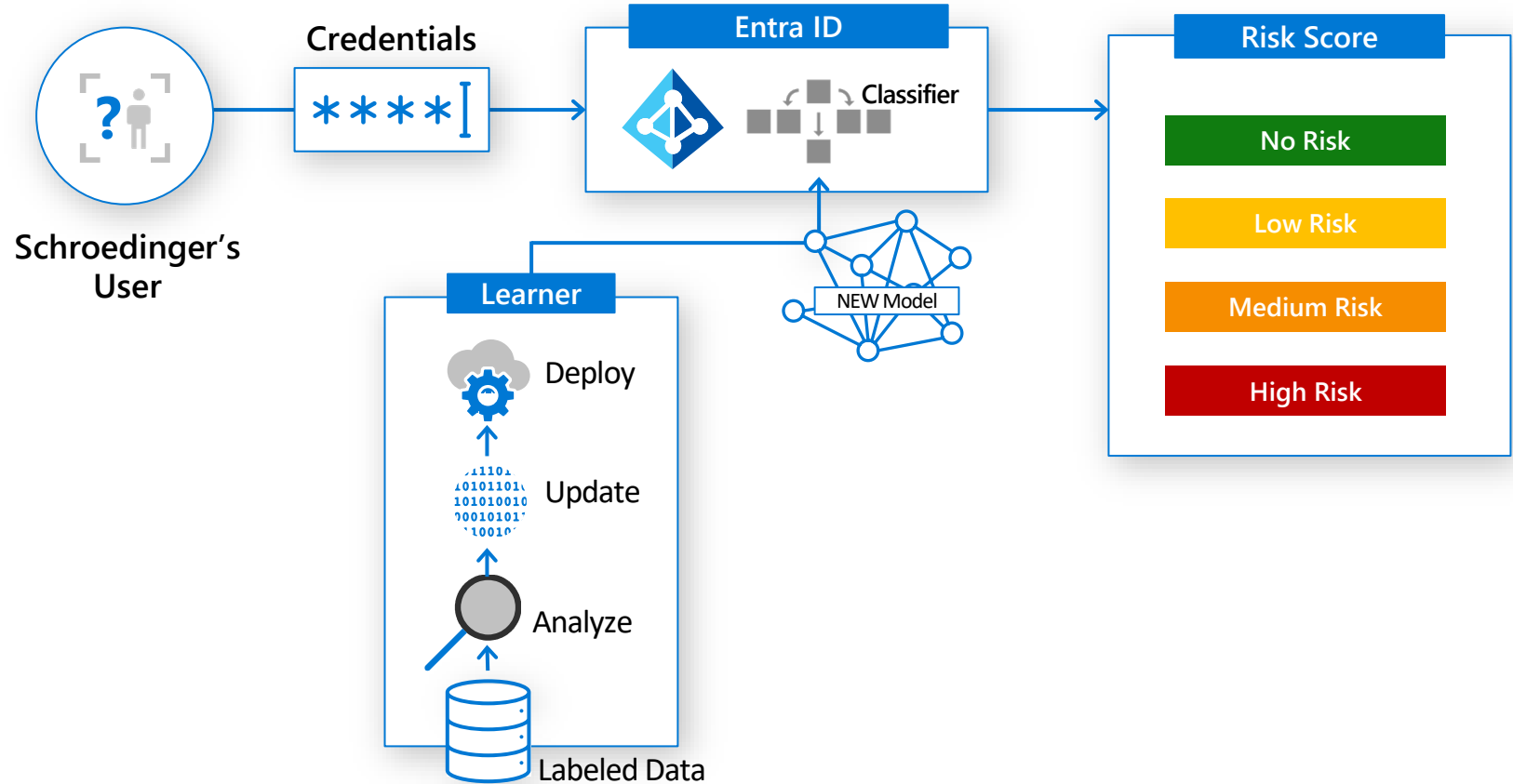
Seamless integration via  
Azure Monitor/Sentinel



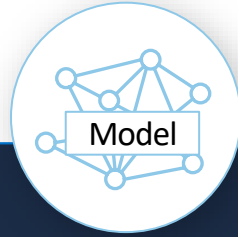
Routing risky alerts to  
Third-party SIEMs



# ML to calculate session risk



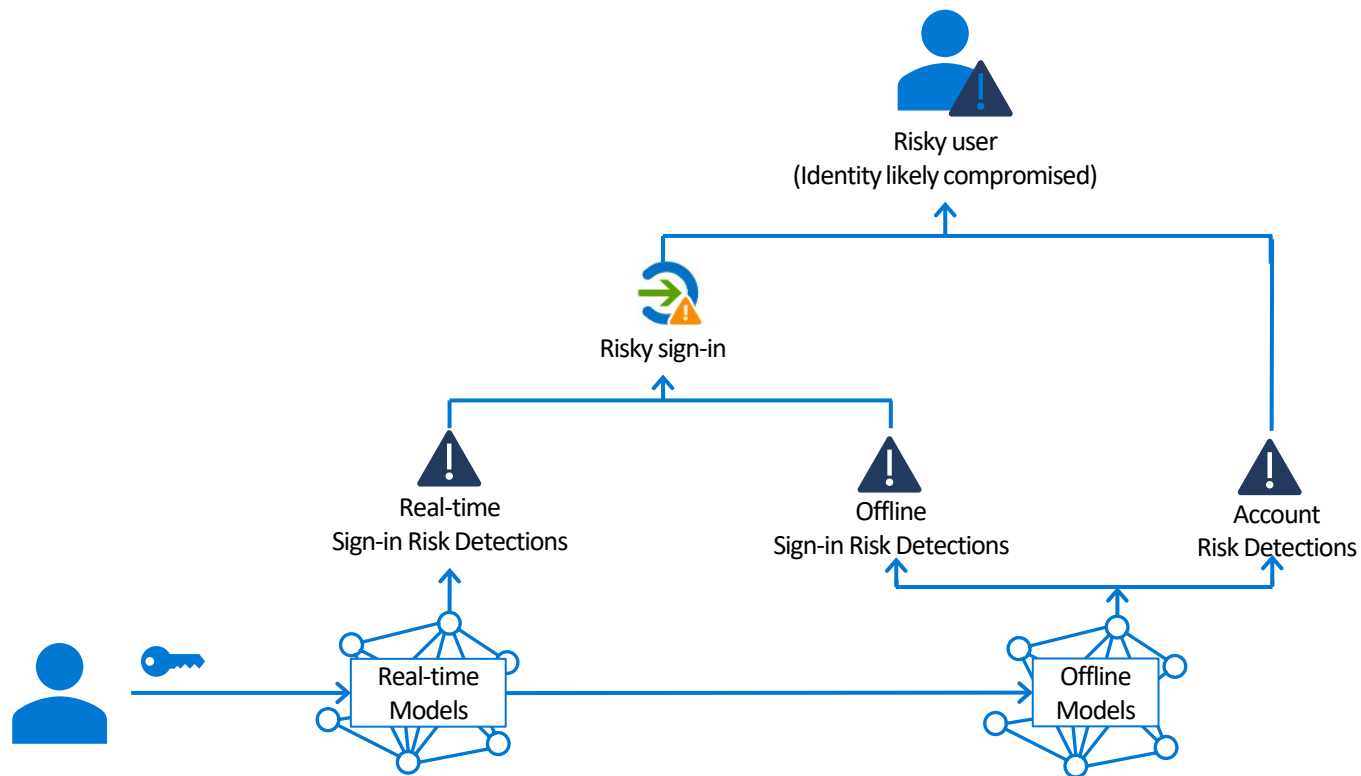
# ML model weighting example



Feature				
IsNormalTimeOfDay	lb			
IsFamiliarDevice	lb	lb	lb	
IsFamiliarApp	lb	lb		
IsFamiliarIP	lb	lb	lb	
IsFamiliarCountry	lb	lb	lb	lb
...				

- Model Training indicates what is the most important compromise indicators at that point in time based on the training data
- Allows the ML system adapt to new attacks on the fly, just retrain the model

# Risk reporting



Security Copilot



# Microsoft Security Copilot

## Announced March 2023

# Microsoft Security Copilot

Defending at machine speed

*"It takes us three minutes to do a task that used to take at least a few hours"*

- Private preview customer



Enable **response in minutes**, not hours



**Simplify the complex** with natural language prompts and easy reporting



**Catch what others miss** with deeper understanding of your enterprise



**Upskill your security talent** with cyber-trained generative AI

Demo






# Security Copilot Demos

Microsoft Security Copilot Preview / My sessions / Rabellam-Entra



▶ Run

 **Rabellam-Entra**

Rabellam-Entra

Phanindra Pampati

Prompts (6)

Tell me about user <USER\_NAME>

Is that account risky?

Show me the most recent 5 sign-in logs for that user.

What authentication methods is that user enabled for?

What security groups does that user own?

Does that user have any active role assignments?

Tell me about user Phanindra Pampati

✓ 3 steps completed 25s

> ✓ Chose Entra 7s

> ✓ Processed your request 9s

> ✓ Prepared your response 8s

Nov 3, 4:57 PM | 25.28s

I found a user named Phanindra Pampati with the foll

- Display Name: Phanindra Pampati
- Given Name: Phanindra
- Surname: Pampati
- Email: [ppampati@woodgrove.ms](mailto:ppampati@woodgrove.ms)
- User Principal Name: [ppampati@woodgrove.m](mailto:ppampati@woodgrove.m)

ID: 70064413-5-13-1070-13-7-1-1000000000

# Takeaways



Use Azure AD  
Conditional Access with  
risk-based policies

---

Use the APIs to get  
information and post  
operations to manage risk



Thank you





# Danke an unsere Sponsoren

## PLATINUM SPONSOR



WE LIVE IT



## GOLD SPONSOR

