



Incorporating Security Intelligence and Automation Into Digital Transformation

Chris Raschke

Advanced Security Architecture – Global Black Belt

Email: chris.raschke@microsoft.com

LinkedIn: www.linkedin.com/in/raschkec

Twitter: [@raschkec](https://twitter.com/raschkec)

Agenda

- Industry trends, Innovations, and Investments
- Notable data breaches, incidents, and attacker techniques, tactics, and procedures (TTPs)
- How are others Evolving Security with the Cloud?



Industry trends

Cloud solutions are generally trusted by most companies

Traditional cybersecurity vendors are struggling

Identity is a key battleground with intense competition from Okta and others

Cloud solution providers are investing heavily in security and looking to seek market dominance



Talent Shortages Exacerbate Cyber Risk

- **1.5 million** unfilled cybersecurity professionals by 2020
- Burnout amongst cybersecurity professionals is extremely high



GDPR gets its teeth

- British Airways faces **\$183 million** fine
- Marriott faces **\$123 million** fine

Notable data breaches, incidents, and attacker techniques, tactics, and procedures (TTPs)

2019 Verizon Data Breach Report

- **52%** of breaches featured hacking
- **33%** included social attacks
- Errors were causal events in **21%** of breaches
- **32%** of breaches involved phishing
- **29%** of breaches involved use of stolen credentials
- **56%** of breaches took months or longer to discover

Microsoft Security Intelligence Report

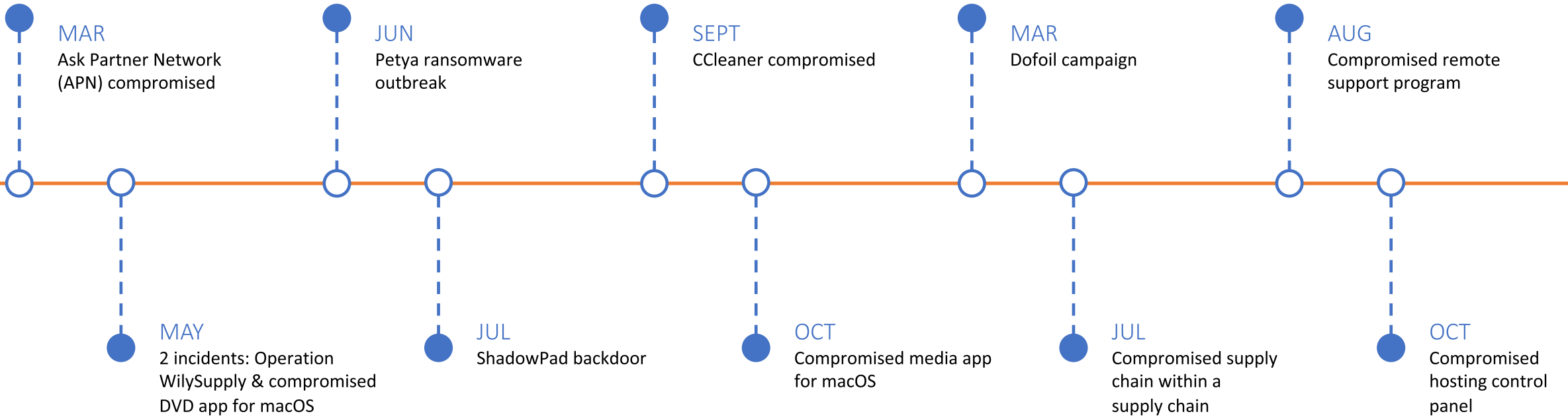
- Cloud weaponization scenarios on the rise
- Cryptocurrency mining on the rise
- Software supply chains at risk
- Phishing continues to be the preferred attack vector

Source: <https://www.microsoft.com/securityinsights/>

Timeline of supply chain attacks

2017

2018



Common attacks against cloud resources



Exposed endpoints



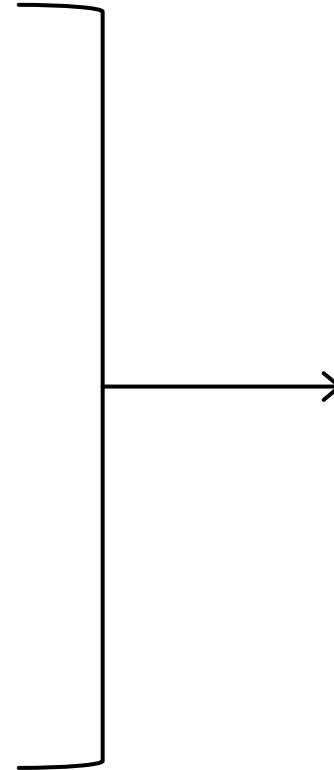
Weak passwords



Exposed and/or stolen credentials



Improper handling/storage of data



Root cause

Misconfiguration

First American Corporation

850 million files, dating back 16 years, available to view online without authentication

Password spray
attacks against
cloud services

```
PS C:\Tools> Get-GlobalAddressList -UserName
[*] First trying to log directly into OWA to
[*] Using https://mail.[REDACTED].com/owa/au
[*] Logging into OWA...
[*] OWA Login appears to be successful.
[*] Retrieving OWA Canary...
[*] Successfully retrieved the X-OWA-CANARY c
OFTCmX0.
[*] Retrieving AddressListId from GetPeopleFi
[*] Global Address List Id of 5775714f-98e2-4
[*] Now utilizing FindPeople to retrieve Glob
[*] Now cleaning up the list...
AndresG@[REDACTED].com
BamaS@[REDACTED].com
CaptainV@[REDACTED].com
CarlT@[REDACTED].com
itadmin@[REDACTED].com
vladi@[REDACTED].com
[*] A total of 6 email addresses were retriev
PS C:\Tools>
```

Ransomware continues to wreak havoc

- City of Riviera Beach, Florida



IRANIAN HACKERS LAUNCH A NEW US-TARGETED CAMPAIGN AS TENSIONS MOUNT



Nation-states

- Global conflicts and disputes have the potential to accelerate cyber attacks and espionage
- MSTIC Holmium Activity Alert
 - aka APT 33

Attackers Continue to Evolve Techniques

```
DTt = Format(Date, "Lon" & "g D" & "ate")
End Function
Function co()
coo = "MsgBox (""Your Interest to Date is "" & int now & "".""")": co = Cells
End Function
Function SediR()
fbb = False
remmi = "If (pFeatureLayer.FeatureClass.ShapeType = esriGeometryPolygon) Then
misR = 19
tre1 = ""
For u = 1 To 4
```

VBA crafted to evade ML classification engines

The intelligent, connected cloud introduces both opportunity and risk

81%

of hacking breaches leverage stolen/ weak passwords

Verizon 2017 Data Breach Investigation Report

1,181

cloud apps in the avg. large enterprise, 61% is shadow IT.

Microsoft 2018

90%

of the world's data has been created in the last two years

IBM Marketing Cloud, "10 Key Marketing Trends For 2017"

TECHNOLOGY HAS CHANGED THE WAY WE DO BUSINESS.
PROTECTING COMPANY ASSETS REQUIRES A NEW APPROACH.

A person is standing in a server room, looking at a laptop. The room is filled with rows of server racks, with blue and yellow cables visible. The lighting is dim, with some light coming from the server racks.

Complexity is the enemy of intelligent security

70

from

35

Security products

Security vendors

Is the average for companies
with over 1,000 employees

[Nick McQuire, VP Enterprise Research CCS Insight.](#)

\$1.37_M

On average that an organization
spends annually
in time wasted responding to
erroneous malware alerts

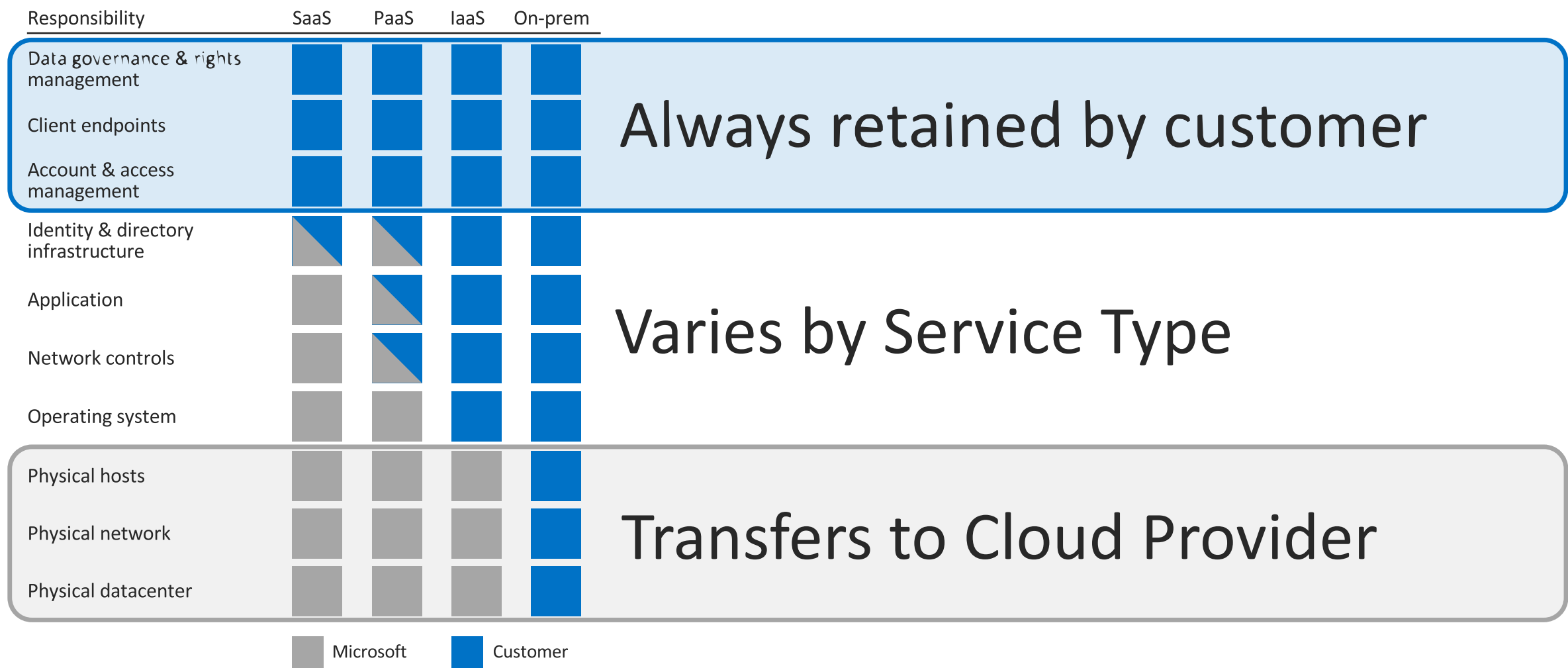
["The Cost of Insecure Endpoints" Ponemon Institute©
Research Report, June 2017](#)

1.87_M

Global cybersecurity workforce
shortage by 2022

[Global Information Security Workforce Study 2017](#)

Cloud Redefines Security Responsibilities



Always retained by customer

Varies by Service Type

Transfers to Cloud Provider

The 'best-of-breed' model is broken


Complex and expensive integration

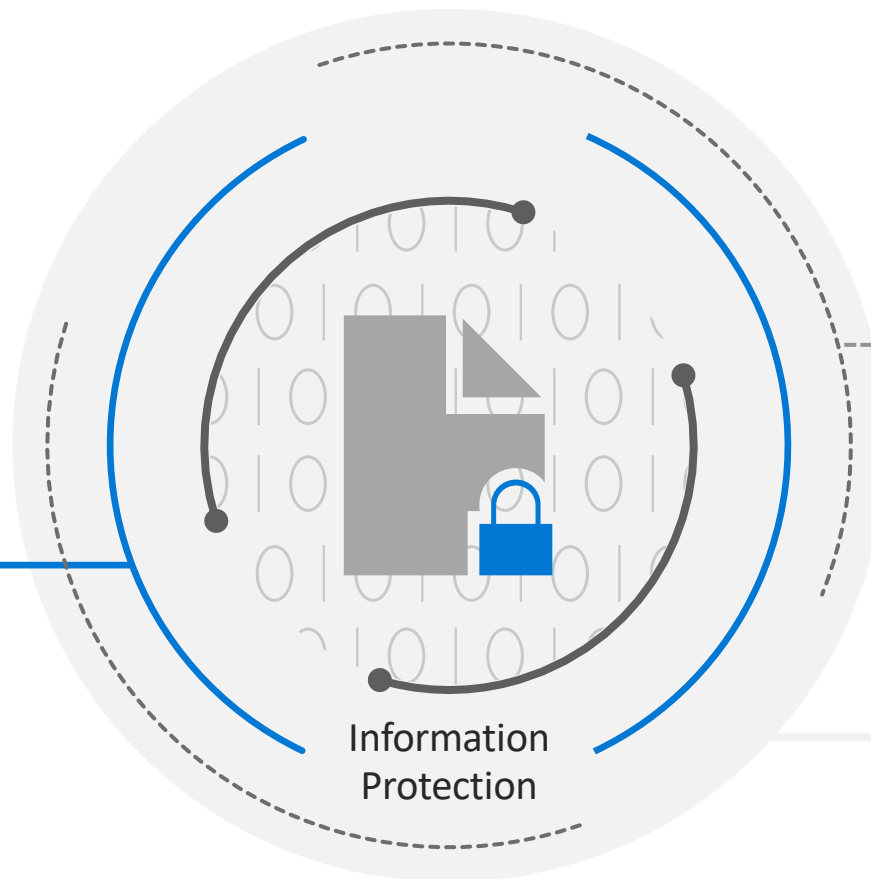
Constant training on new tools


Too many alerts to handle

Gaps in visibility



 Identity & Access Management



Threat Protection 

Security Management 



Data is your most important company asset



Correlate threat information and automatically respond



Optimize with security insights and configuration tools

Intelligent security for the modern workplace



Identity & Access Management

Secure identities to reach zero trust



Threat Protection

Help stop damaging attacks with integrated and automated security



Information Protection

Protect sensitive information anywhere it lives



Security Management

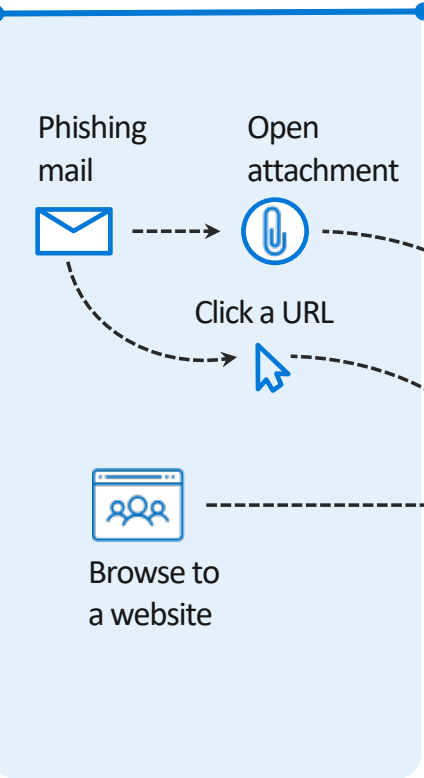
Strengthen your security posture with insights and guidance

Holistic security across your digital landscape

Protection across the attack kill chain

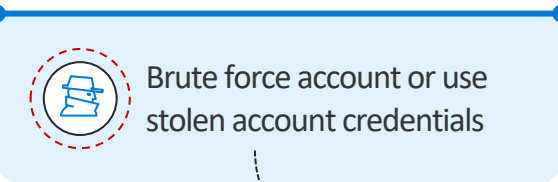
Office 365 ATP

Malware detection, safe links, and safe attachments



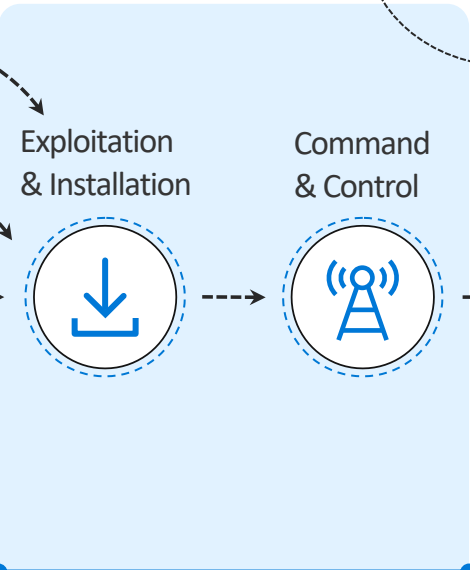
Azure AD Identity Protection

Identity protection & conditional access



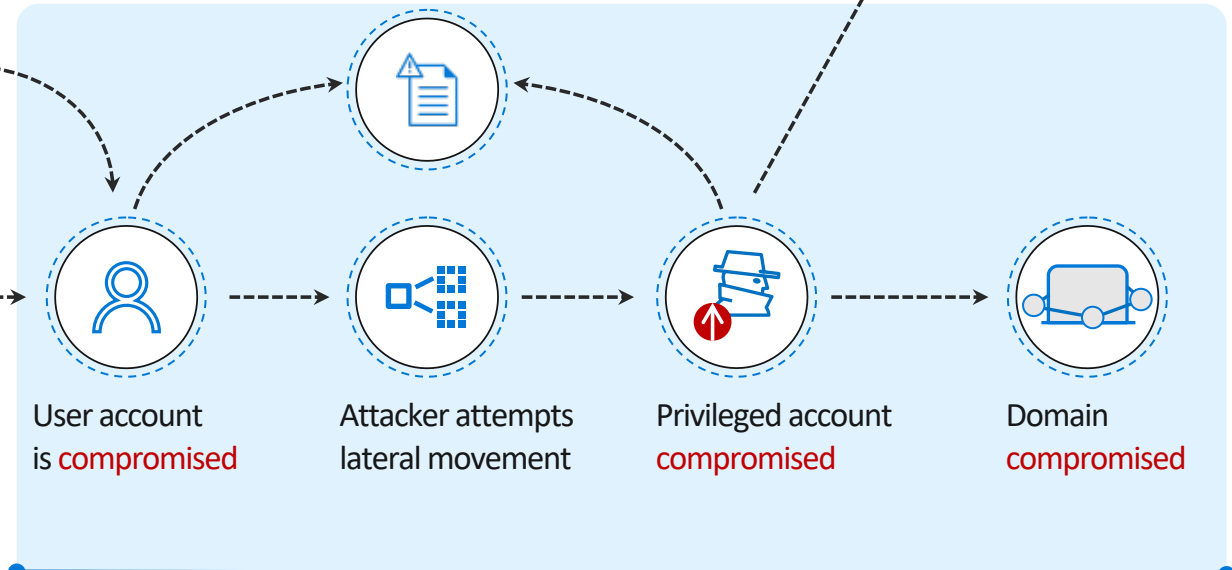
Microsoft Defender ATP

Endpoint Detection and Response (EDR) & End-point Protection (EPP)



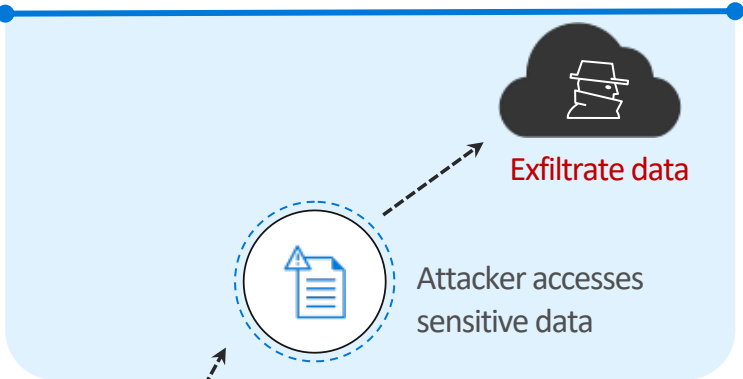
Azure ATP

Identity protection



Microsoft Cloud App Security

Extends protection & conditional access to other cloud apps



Azure Sentinel

SIEM + SOAR

Session takeaways

- **Phishing** continues to be the primary method for gaining a foothold by attackers
- A significant portion of attacks involve the **use of compromised credentials**, or successful **attacks against weak passwords**
- Breaches continue to **take months to identify**
- **Lack of trained and qualified security professionals** requires a strategy shift
- Subscribe to and regularly read the **MSFT Security Blog** and **MSFT threat intel**
- **Best of Breed** model is broken – must shift to cloud platform solutions.

Thank You!!!



CYBER SECURITY
Security solutions through collaboration.™ **SUMMIT**

#cybersummitmn

October 28-30, 2019 | Minneapolis Convention Center