



**Microsoft Online Tech Forum**

**微软在线技术峰会**

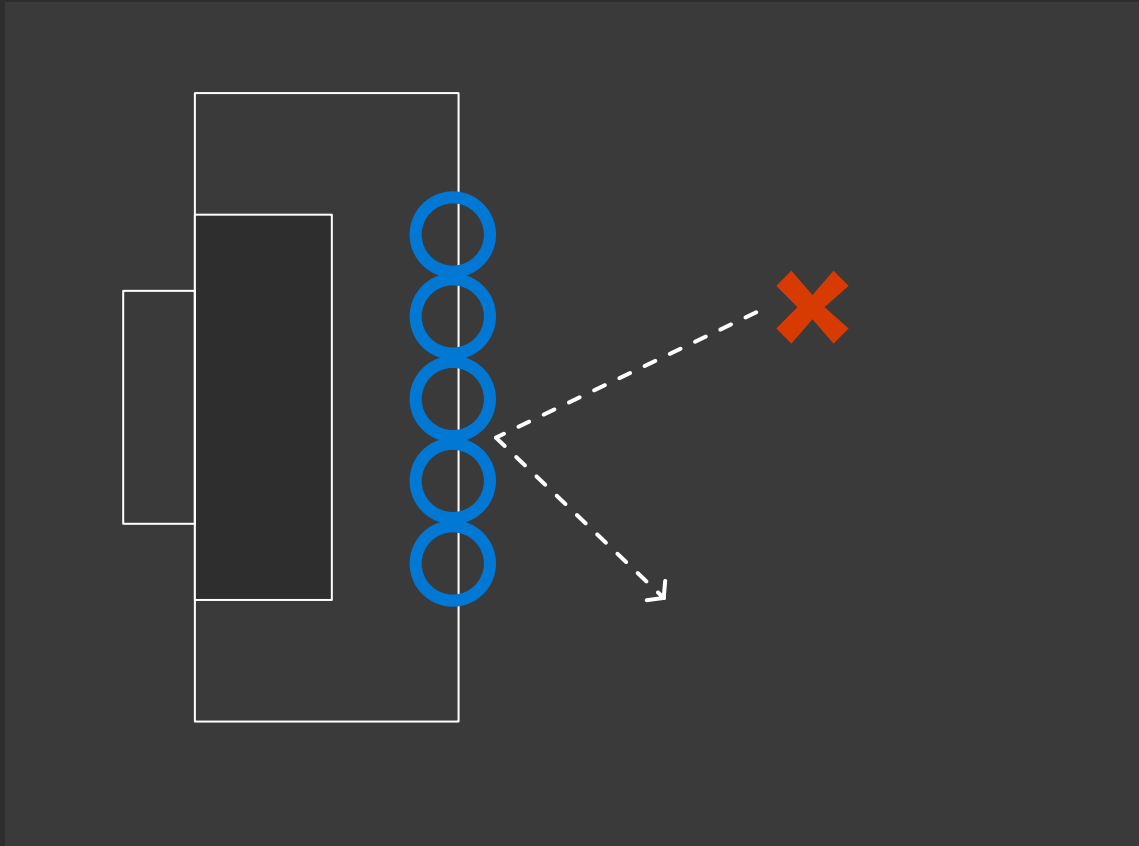
**洞察威胁，全面保护 ——Microsoft  
Threat Protection 侦测调查的威力**

Holly Gong (龚祺莎)

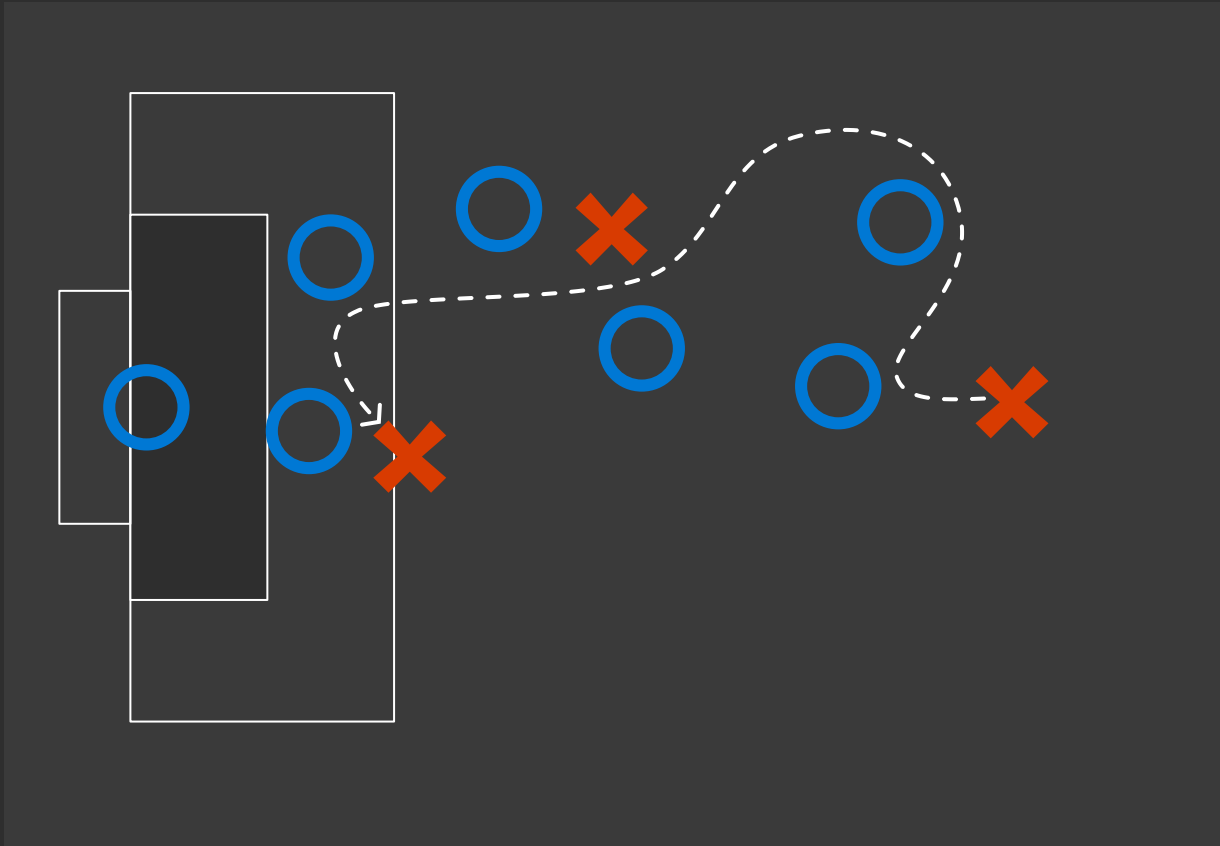
“防御者用列表思考。攻击者用图表思考。  
只要这一点是真的，攻击者就会赢。”

---

# 我们如何建立我们的防御



# 实际发生的情况



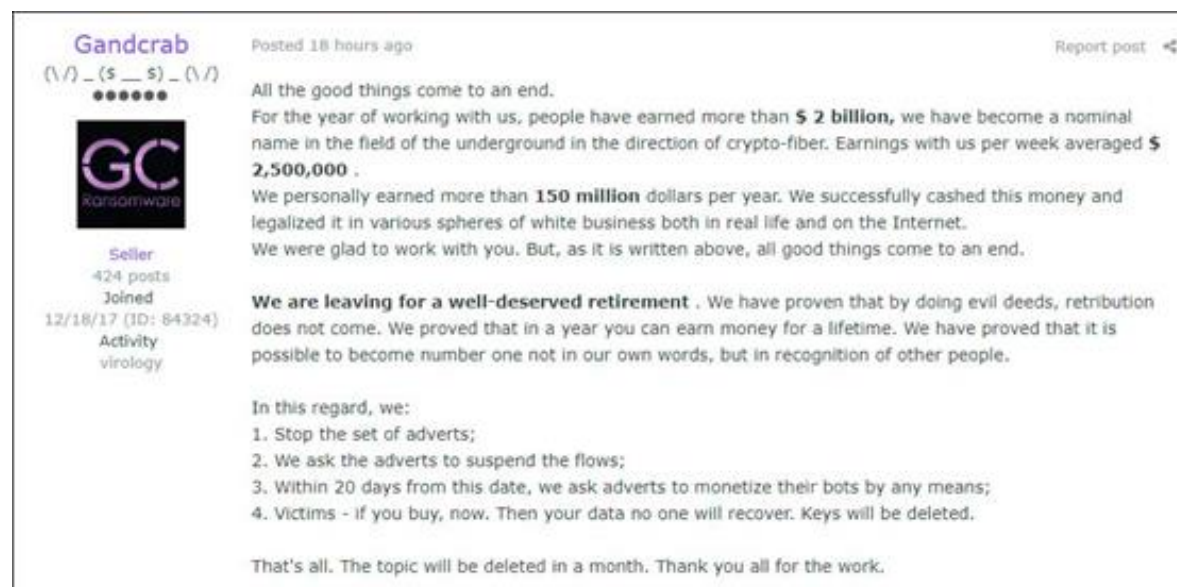
图示

× 攻击

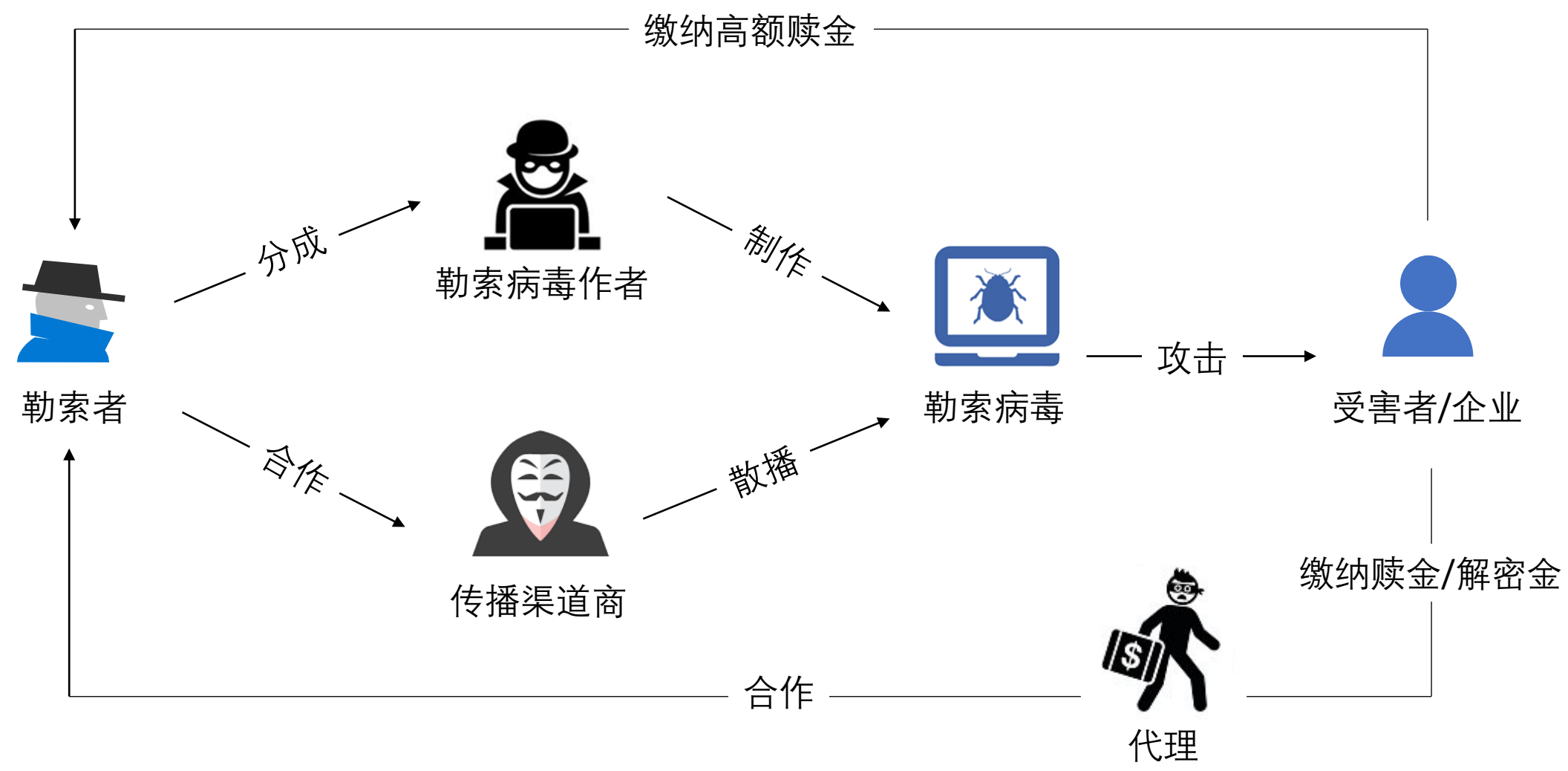
○ 后卫

# 2019年 – 年度五大勒索病毒家族

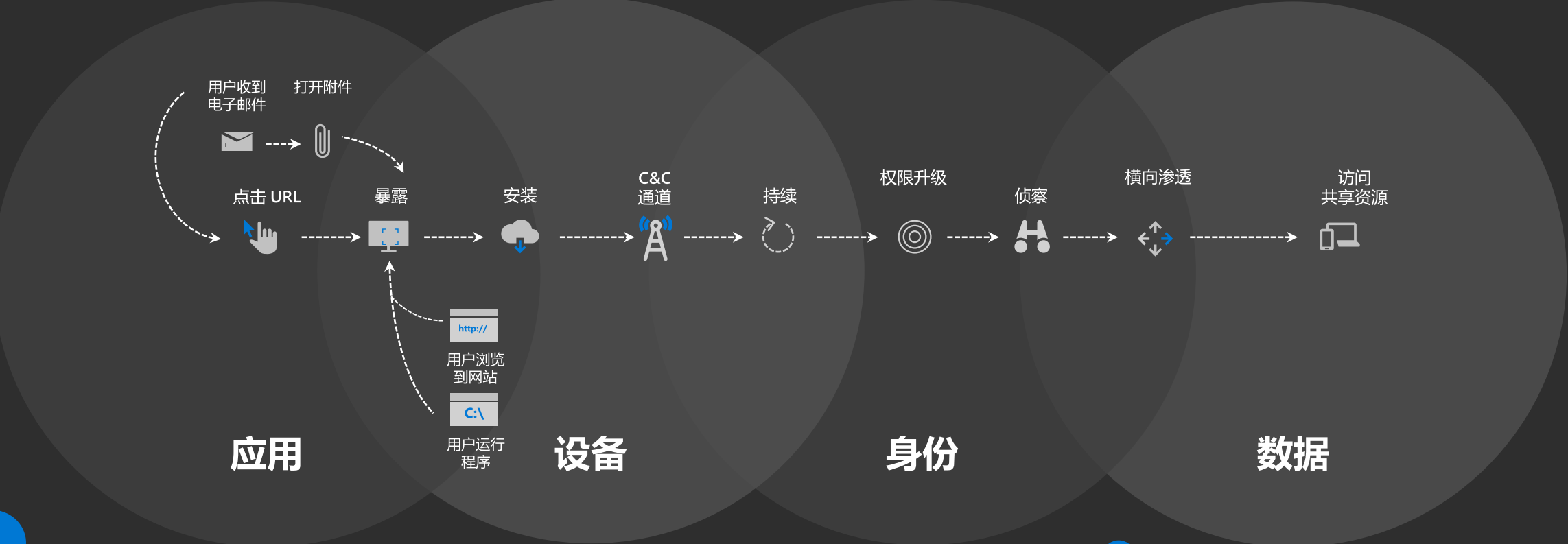
- **GandCrab勒索病毒**: 2018年GandCrab首次出现，之后经过5次版本迭代，波及罗马尼亚、巴西、印度等数十国家地区，全球累计超过150万用户受到感染。还被国内安全团队称为“侠盗病毒”，因为他们后期的版本中避开了战火中的叙利亚地区。
- **Sodinokibi勒索病毒**: 在不到半年时间，该勒索病毒已非法获利数百万美元。
- **Globelmposter勒索病毒**: 该勒索病毒又称“十二生肖”病毒，会以“十二生肖英文名+4444”的文件后缀，对文件进行加密。而Globelmposter自2017年5月首发至今，已经历八个版本迭代，并且后缀也从“十二生肖”，变身希腊“十二主神”。
- **Stop勒索病毒**: 走薄利多销的敛财路线，解密赎金需要980美元，并且72小时联系软件作者还可享五折优惠。该病毒主要利用木马站点，通过伪装成软件破解工具或捆绑在激活软件进行传播，用户中招率奇高。
- **Phobos勒索病毒**: 与Dharma病毒（又名CrySis）属于同一组织，并且该病毒在运行过程中会进行自复制，和在注册表添加自启动项，如果没有把系统残留的病毒体清理干净，很可能会遭遇二次加密。



# 勒索病毒产业链



# 攻击链条解析——跨越防御边界



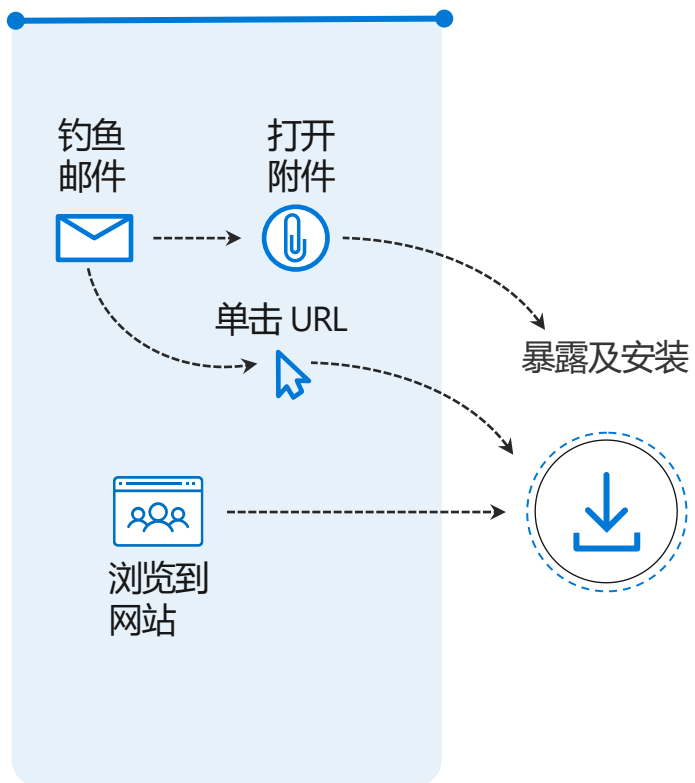
微软

- Office 365 ATP  
MCAS  
SmartScreen
- Microsoft Defender ATP  
(Azure Security Center)
- Azure AD  
Azure ATP  
微软云应用安全 (MCAS)
- Office 365 ATP  
微软云应用安全 (MCAS)

# 攻击链条解析

## Office 365 ATP

恶意软件检测、安全链接和  
安全附件



# 防范各种复杂的邮件威胁



## 安全链接

在点击时提供  
恶意网页侦测功能



## 智能防欺诈

对于仿发件人姓名，域名，  
等的欺诈邮件进行识别提醒

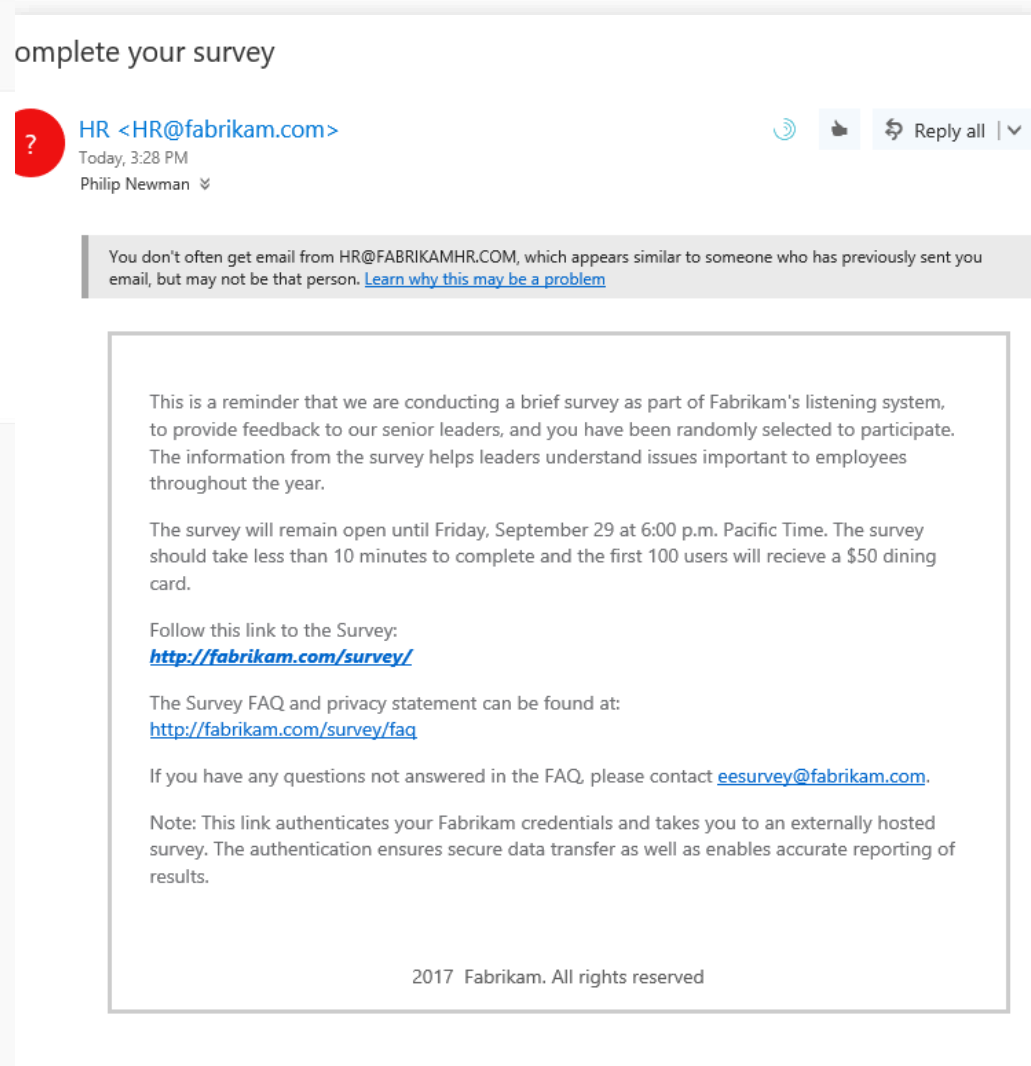
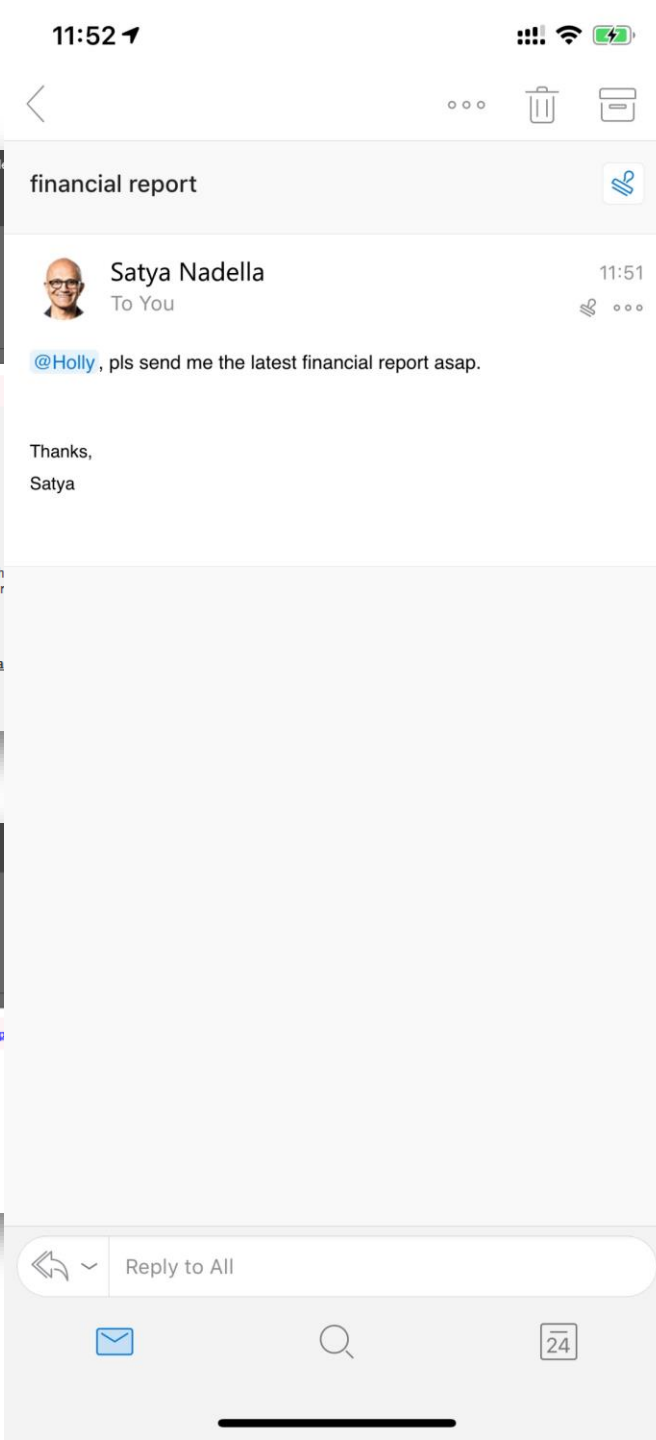
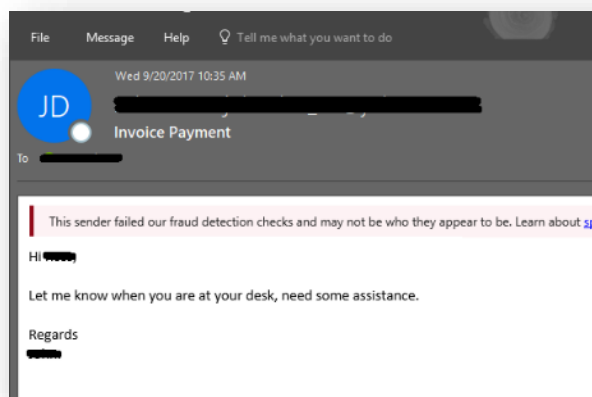
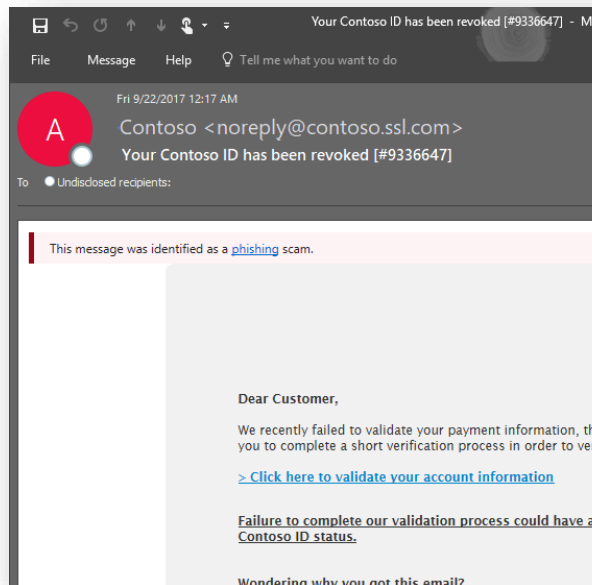


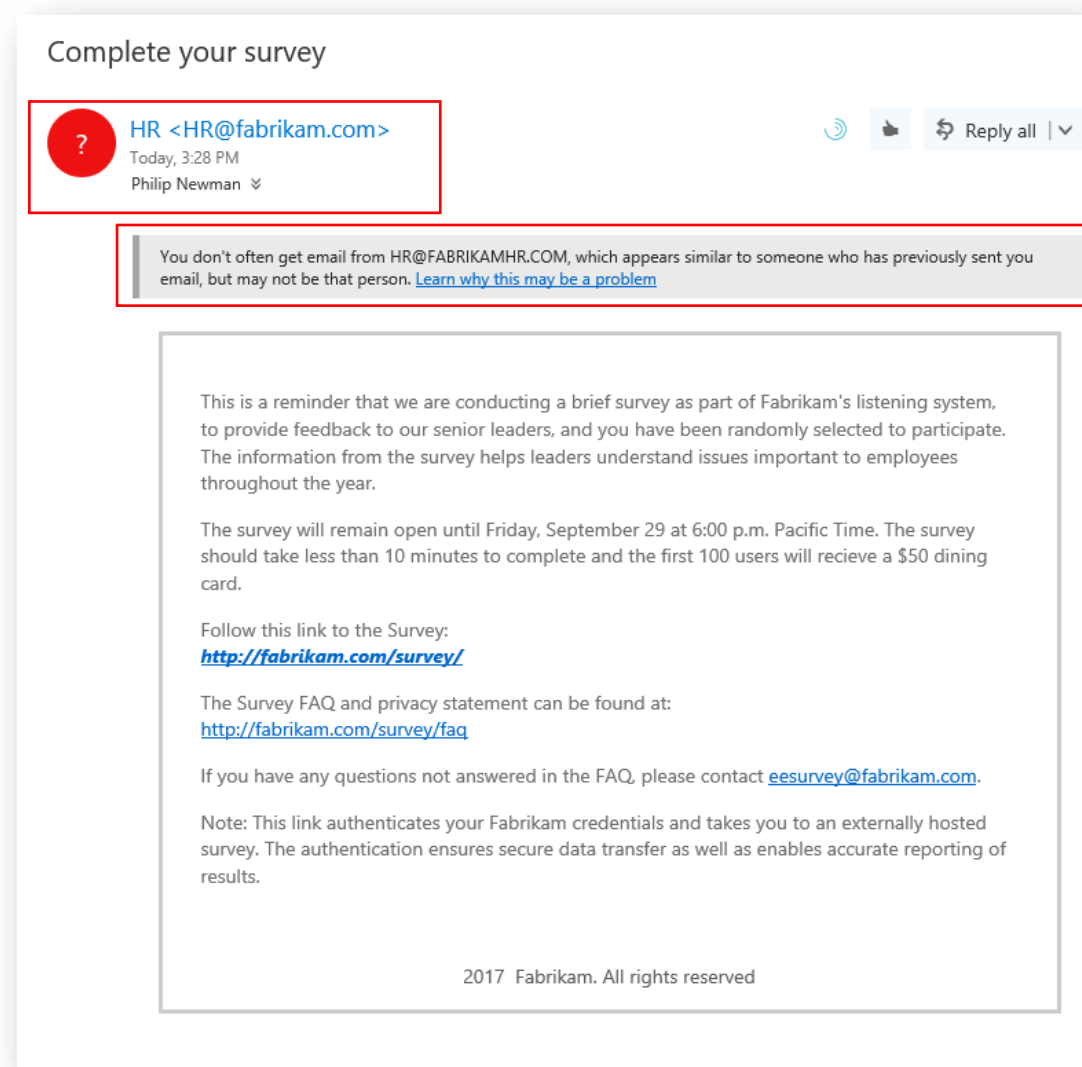
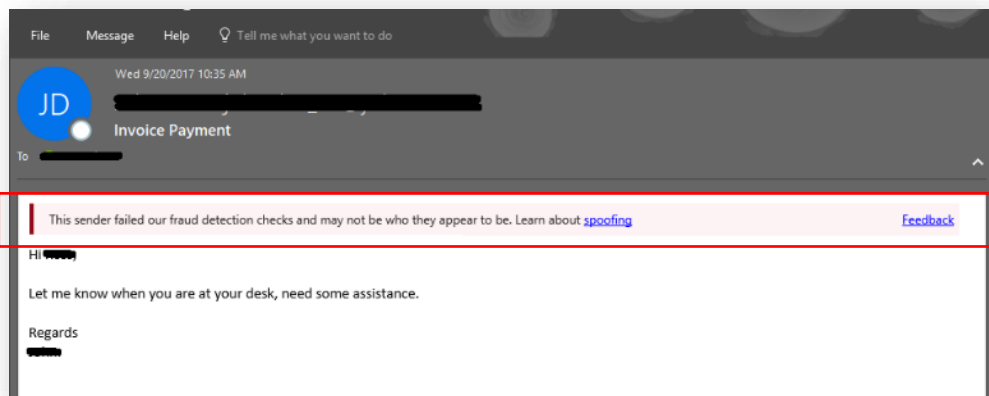
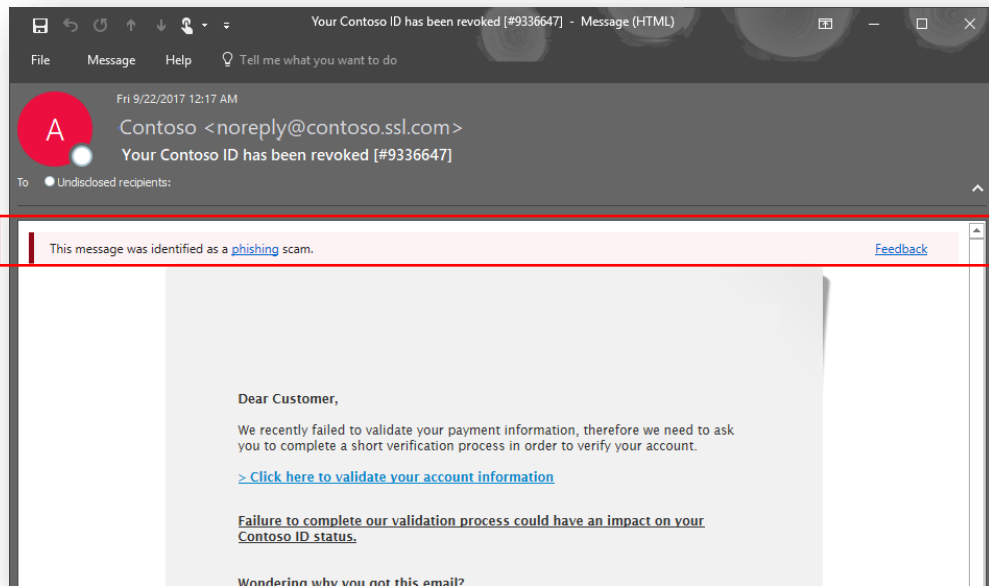
## 安全附件

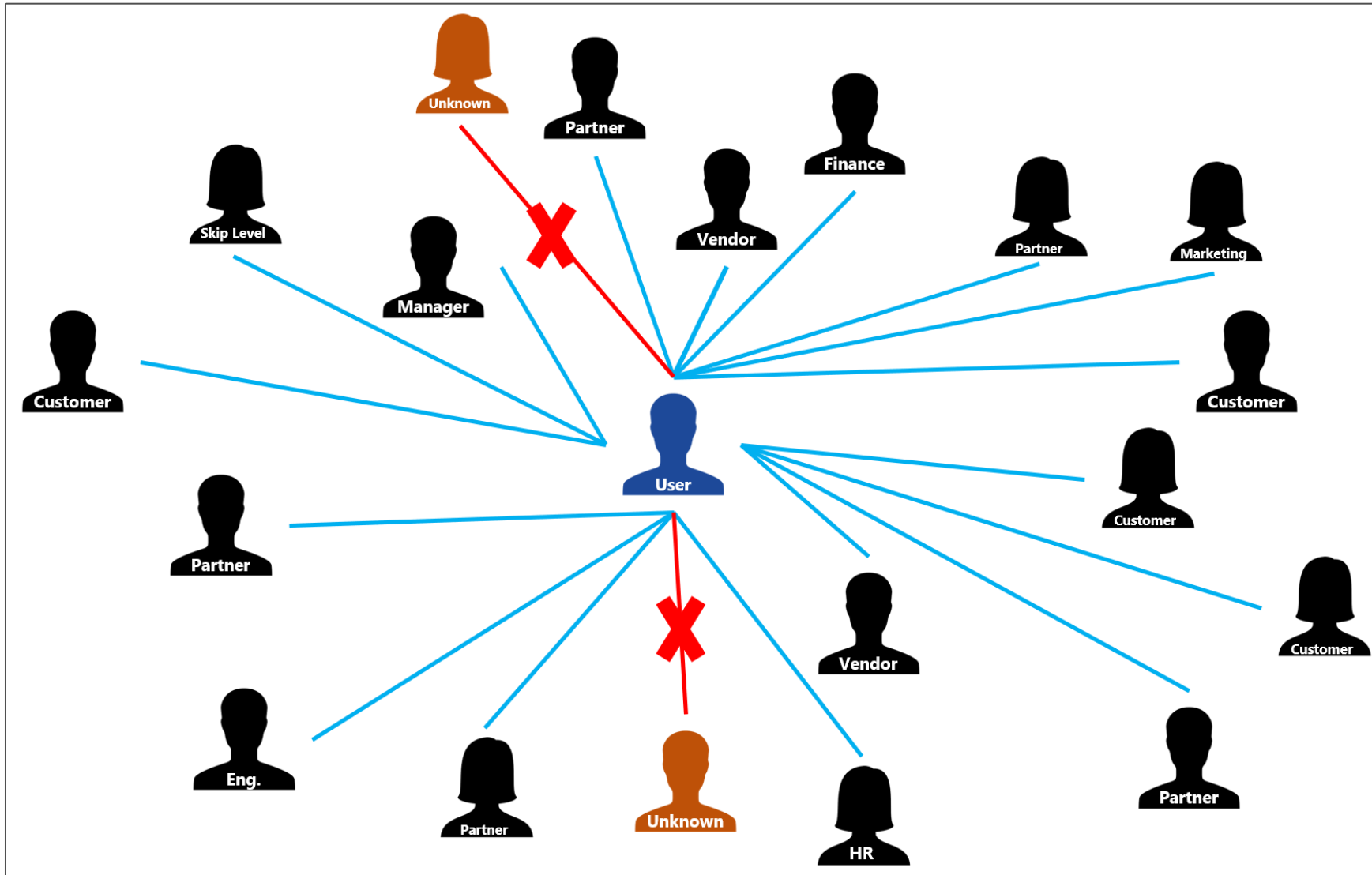
防范恶意附件

多种功能，最高的安全保障





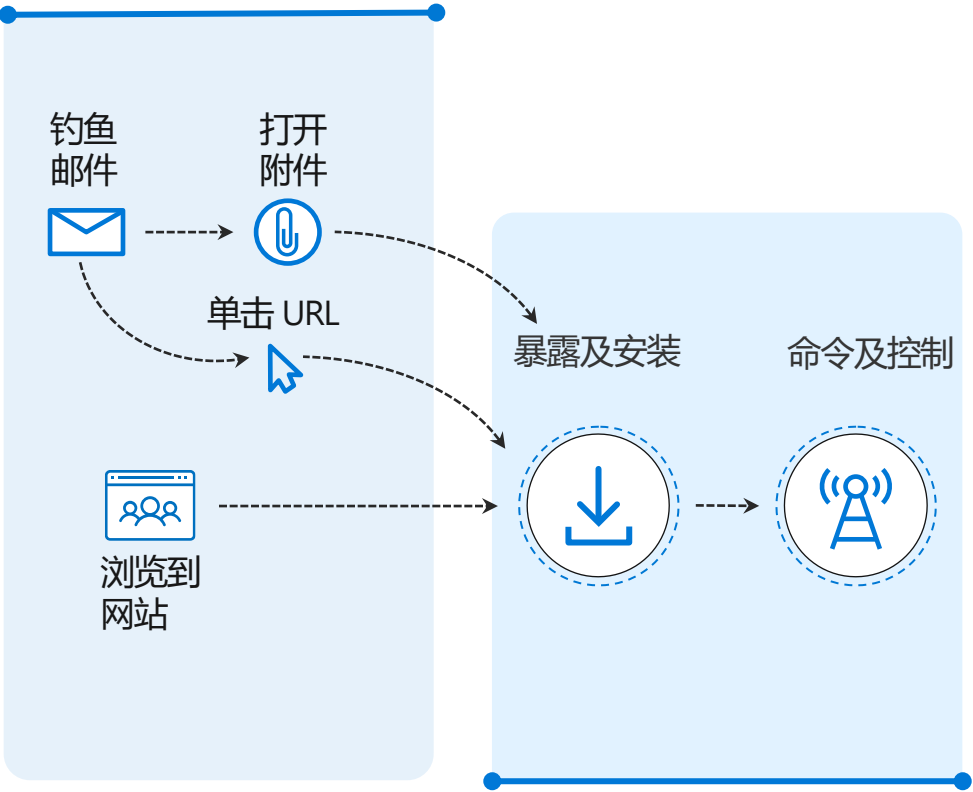




# 在整个攻击链条中提供保护

## Office 365 ATP

恶意软件检测、安全链接和安全附件

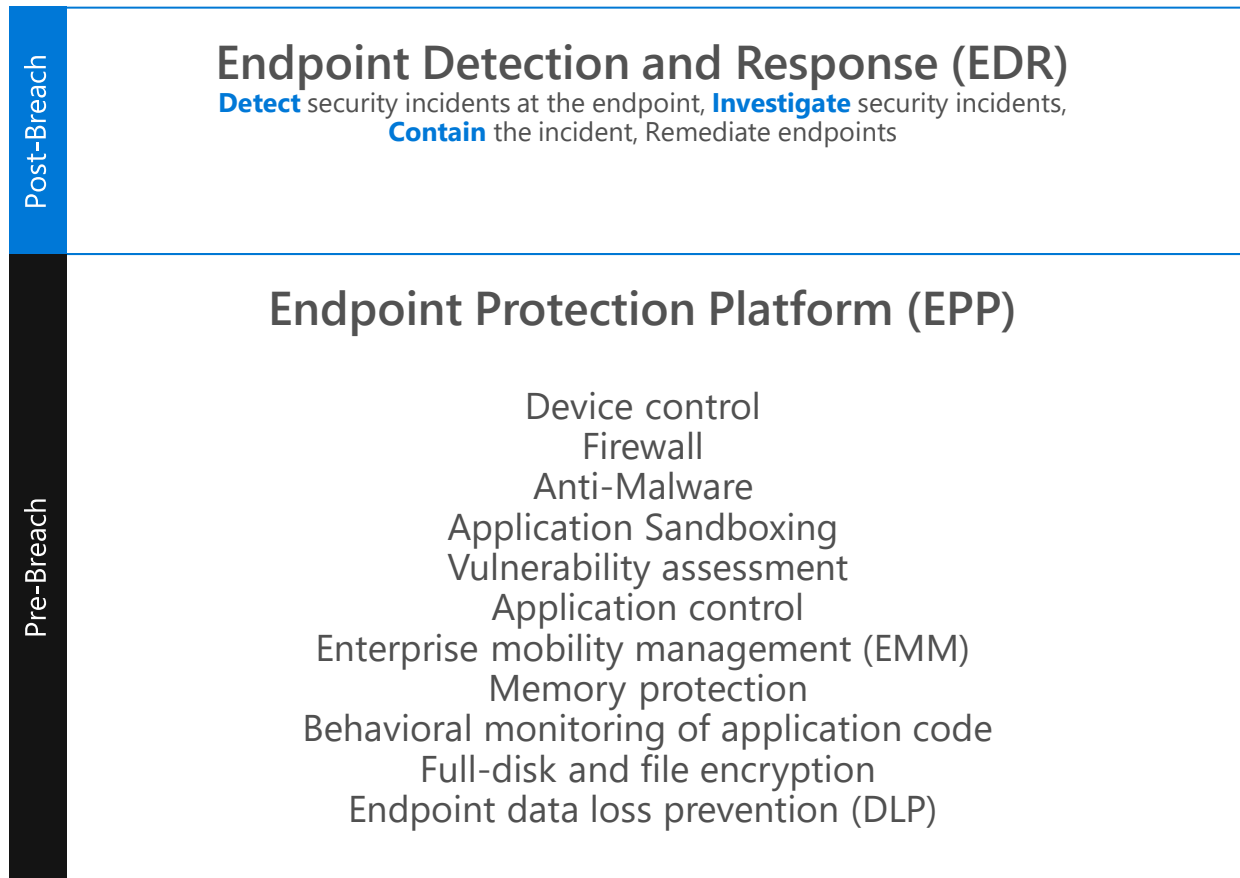


## Microsoft Defender ATP

终端检测和响应 (EDR) 以及  
终端保护 (EPP)

# Microsoft Defender Advanced Threat Protection

How it fits in the endpoint security stack?



# EPP and EDR Leader

Figure 1. Magic Quadrant for Endpoint Protection Platforms



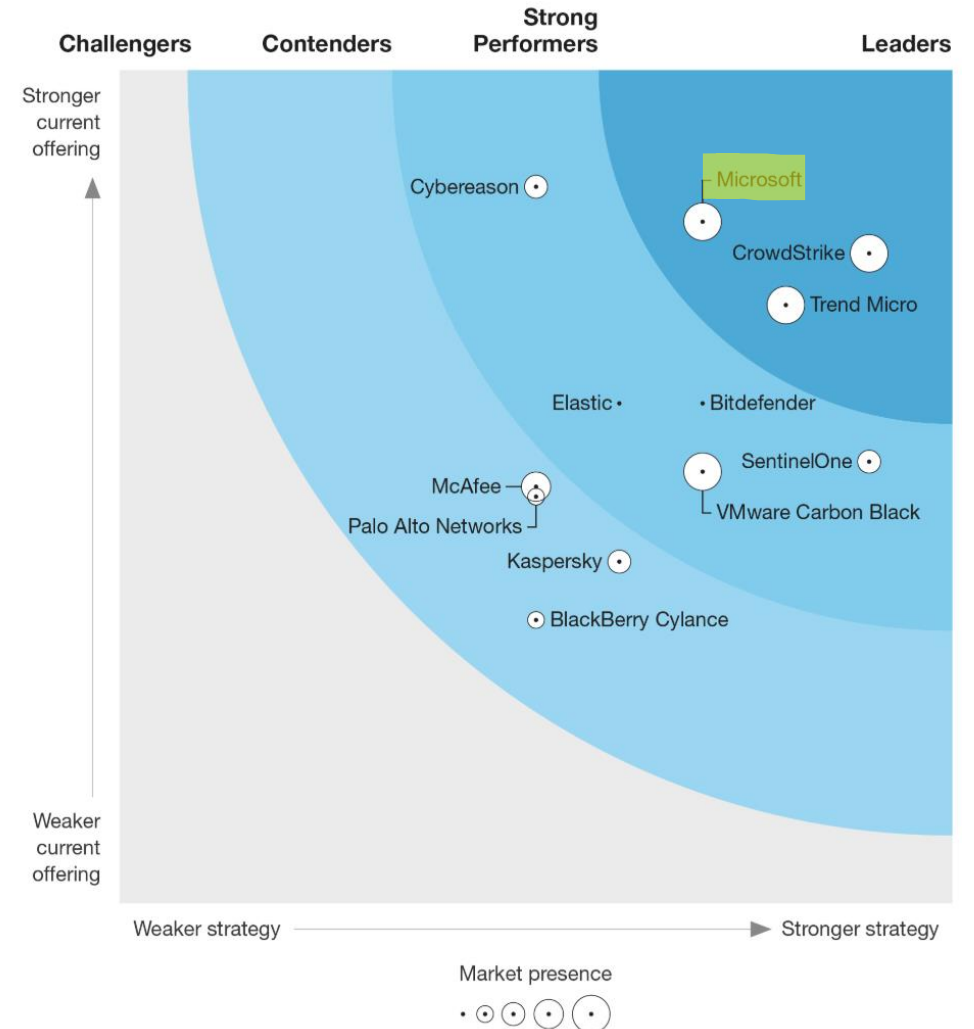
Source: Gartner (August 2019)

FORRESTER RESEARCH

## THE FORRESTER WAVE™

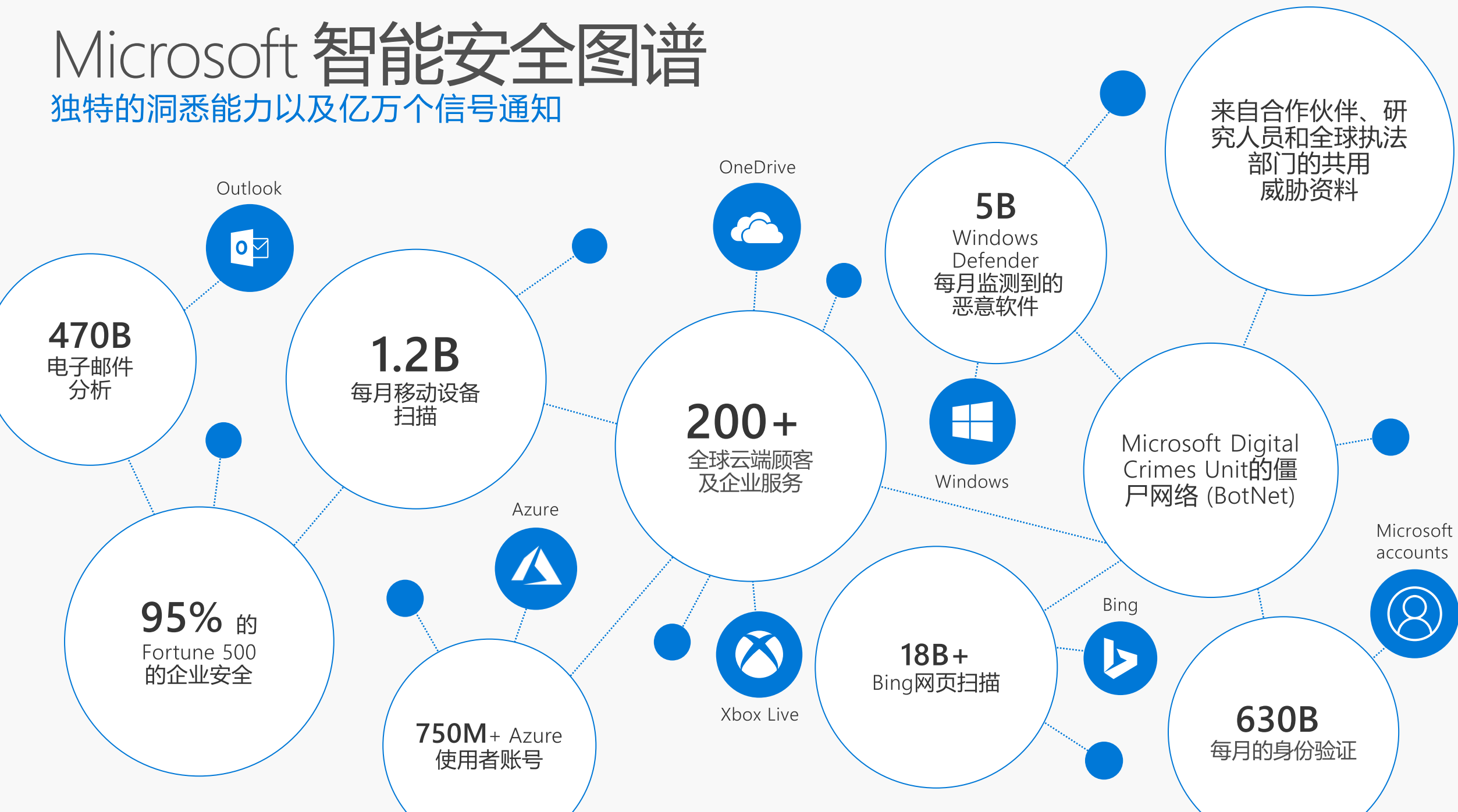
Enterprise Detection And Response

Q1 2020

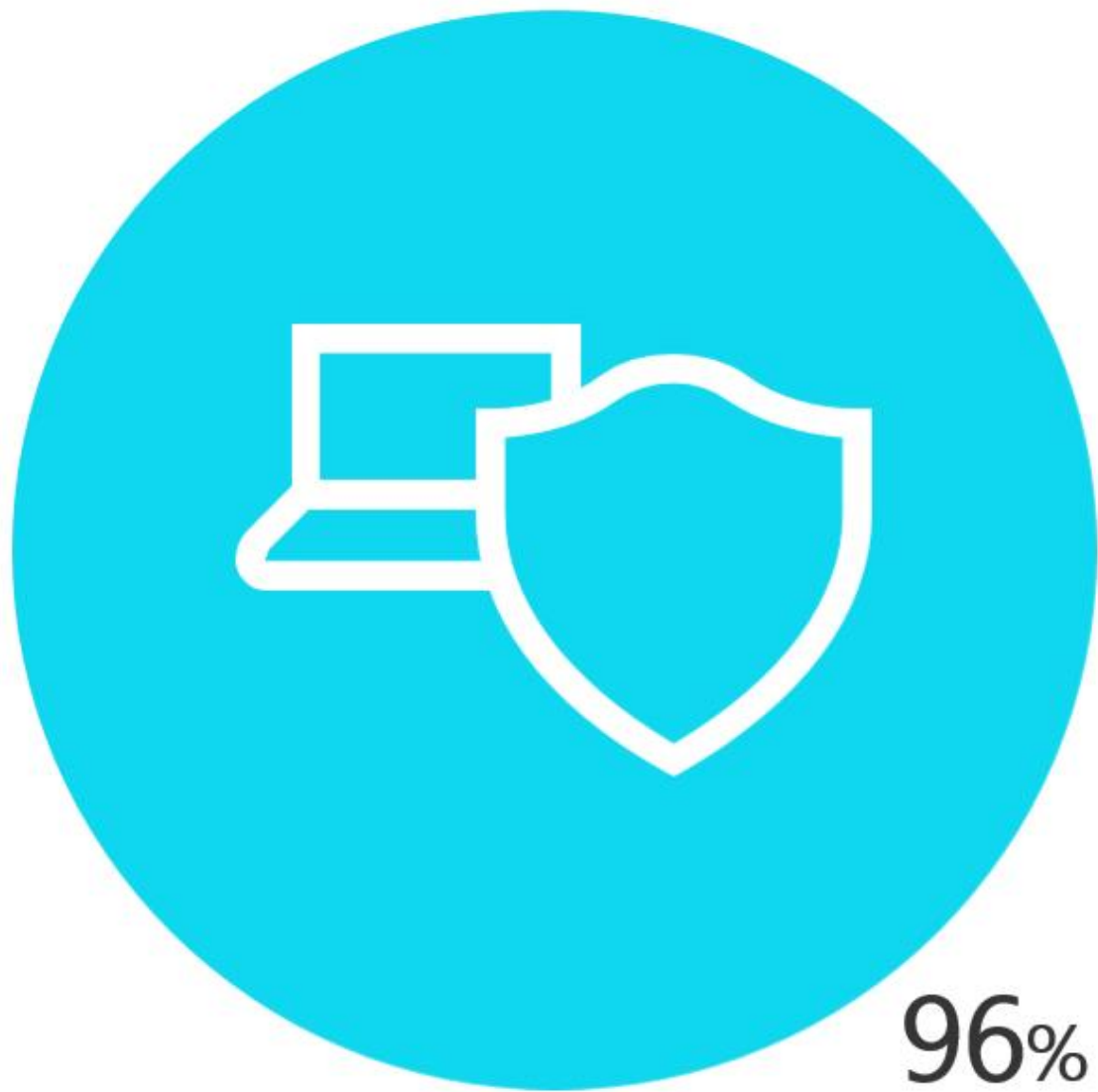


# Microsoft 智能安全图谱

独特的洞悉能力以及亿万个信号通知



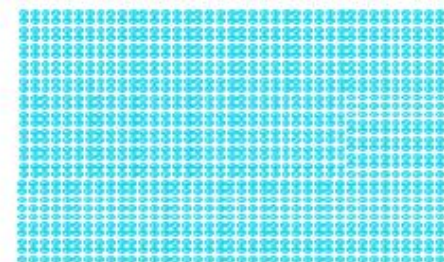
# 为什么需要机器学习?



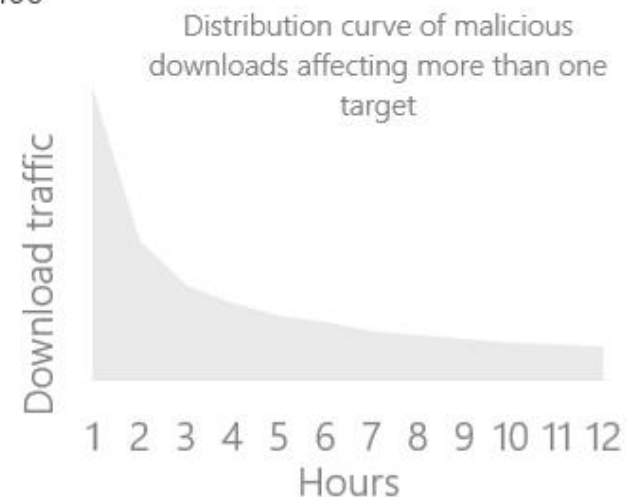
3%  
seen 2-10



0.4%  
seen 11-100



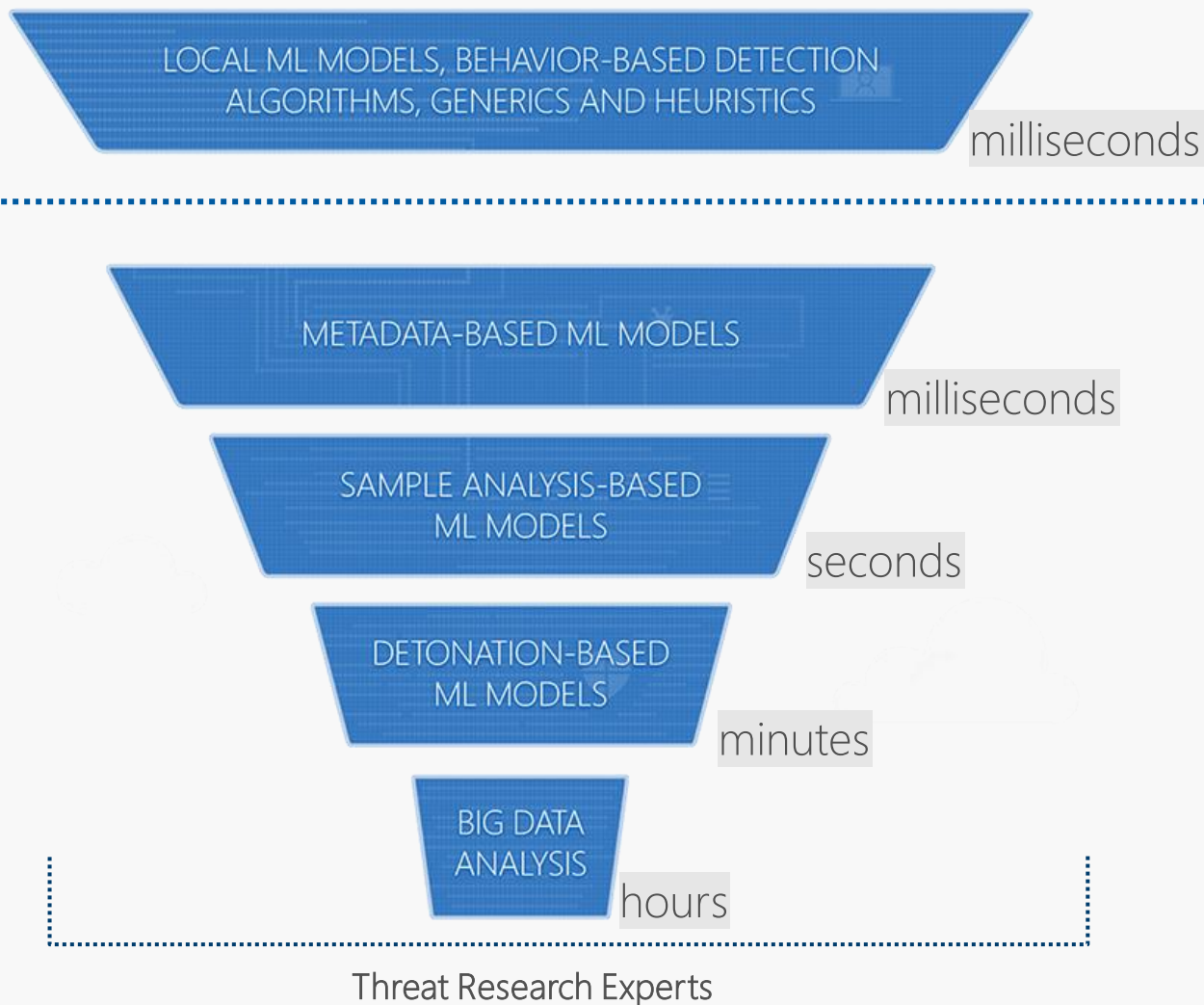
0.01%  
seen on 1001+





# Microsoft Defender ATP 机器学习层级架构

本地  
云端



**Client** – 大部分的恶意软件会被高精度的 Windows Defender AV 通过本地的机器学习模型、启发法及行为数据分析，得以成功拦截

Pro E3 E5

**Cloud metadata** – 借以云端机器学习规则来评估 Windows Defender AV 客户端发送的 metadata，鉴别可疑信号

Pro E3 E5

**Sample** – 可疑文件的副本将上传以通过 multi-class 及深度神经网络等规则进行评估判断

E5

**Detonation** – 可疑文件将在沙盒中执行，并通过 multi-class 及深度神经网络等机器学习技术对其进行动态分析

E5

**Big data** – 用机器学习模型和高级规则分析及关联全球 Microsoft 智能安全图谱的数据，自动化识别恶意攻击

E5

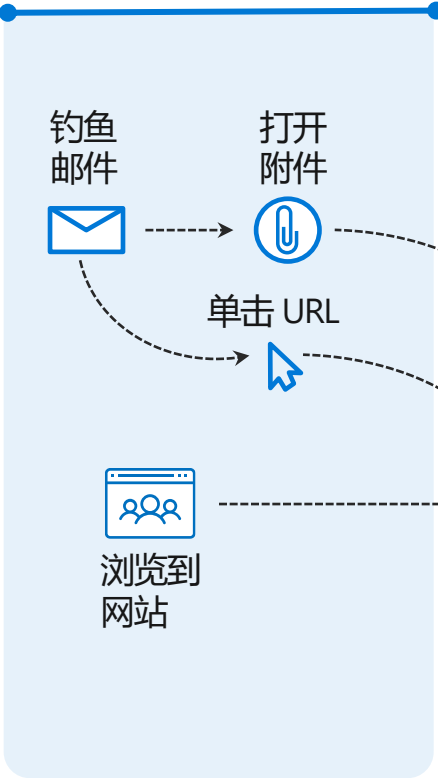


# Demo - MDATP

# 在整个攻击链条中提供保护

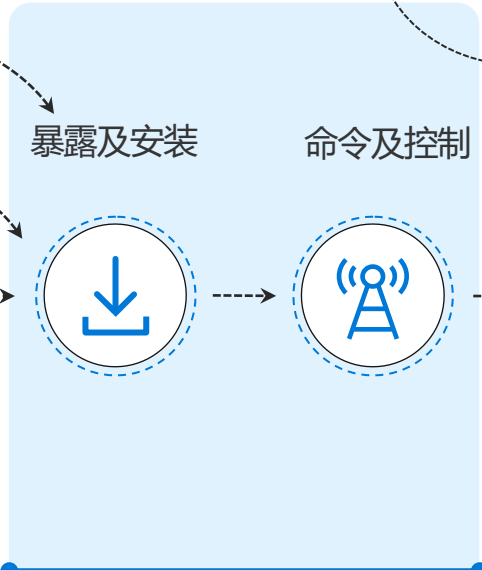
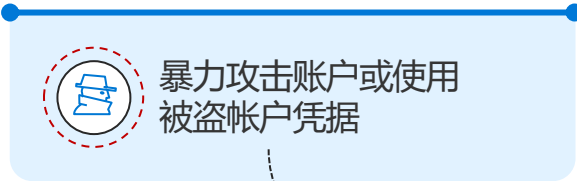
## Office 365 ATP

恶意软件检测、安全链接和安全附件



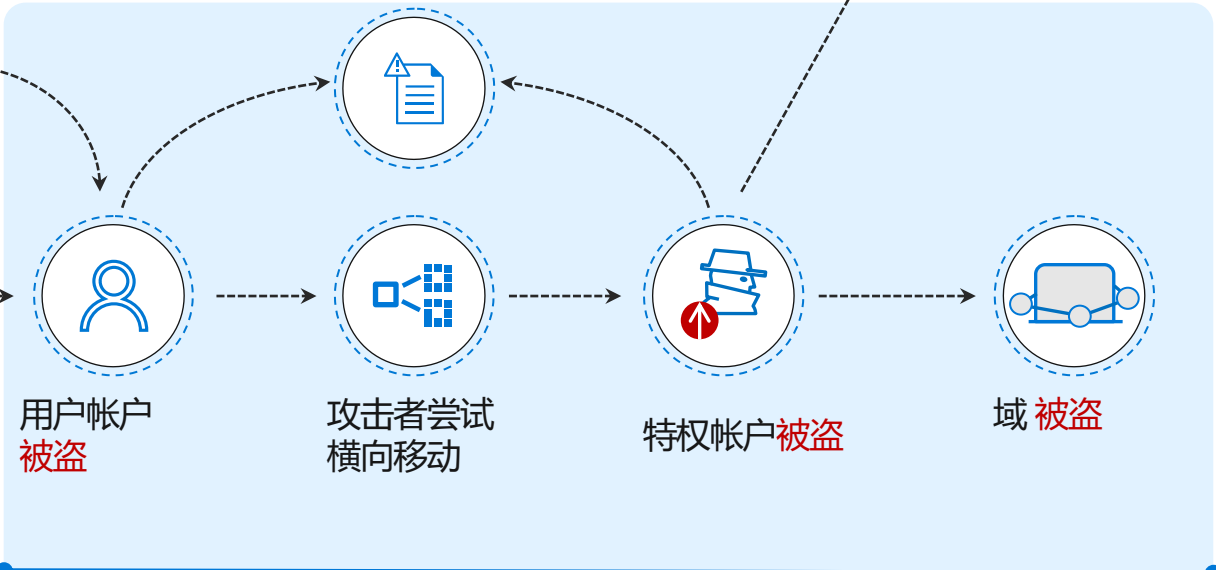
## Azure AD 身份保护

身份保护以及 条件性访问



## Microsoft Defender ATP

终端检测和响应 (EDR) 以及终端保护 (EPP)

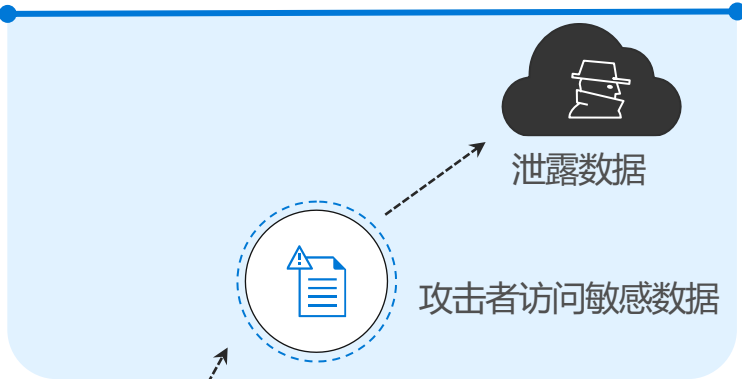


## Azure ATP

身份保护

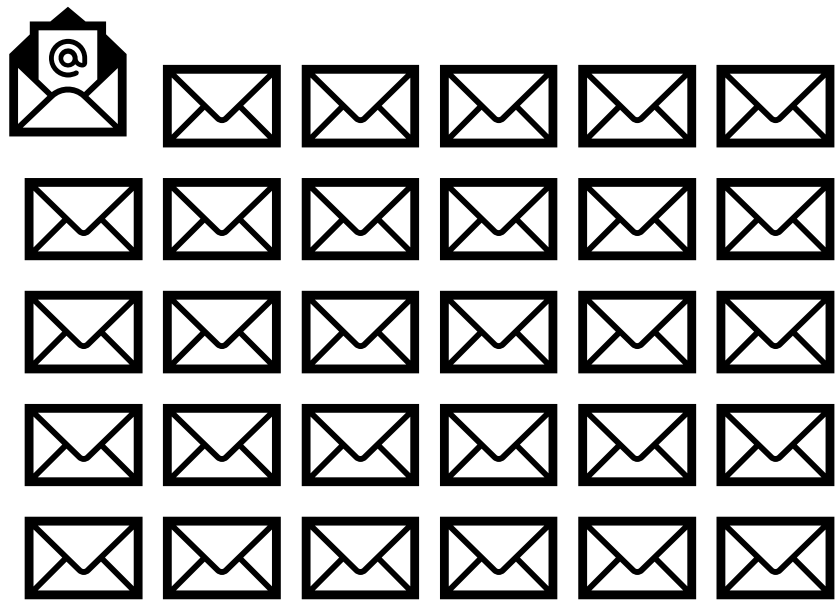
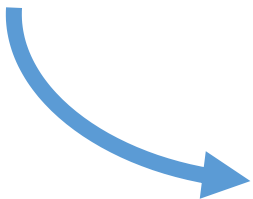
## 微软云应用安全 (MCAS)

扩展对其他云应用的保护及条件性访问

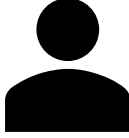
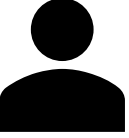
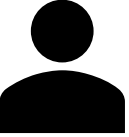


# 攻击内幕—— 电信诈骗

攻击者



钓鱼邮件



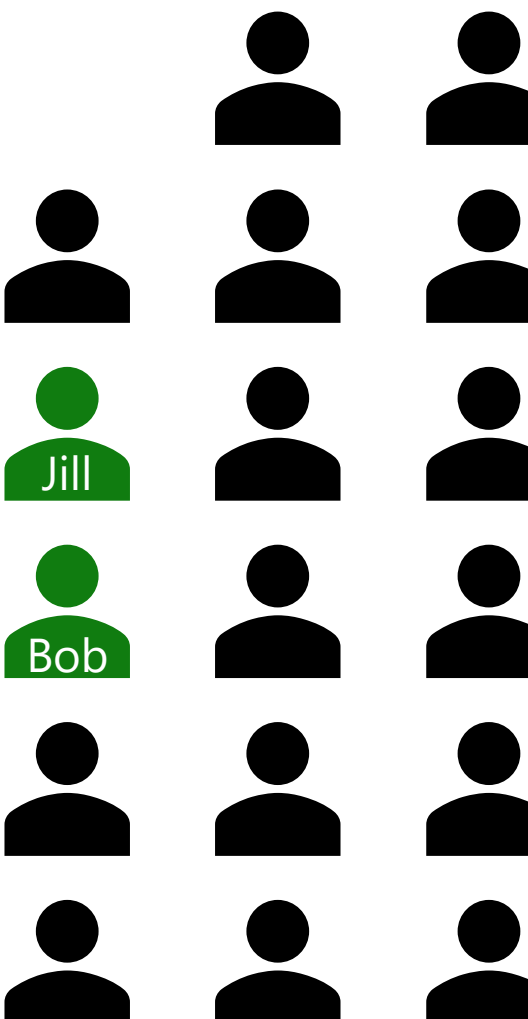
# 攻击内幕—— 电信诈骗

攻击者



有批准付款流程的权限

有建立付款流程的权限



# 攻击内幕—— 电信诈骗

攻击者



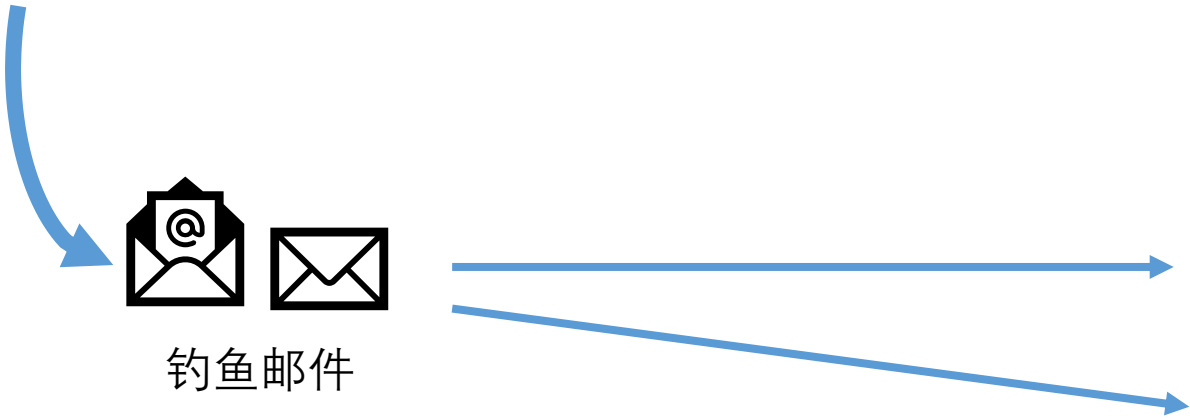
Jack



钓鱼邮件

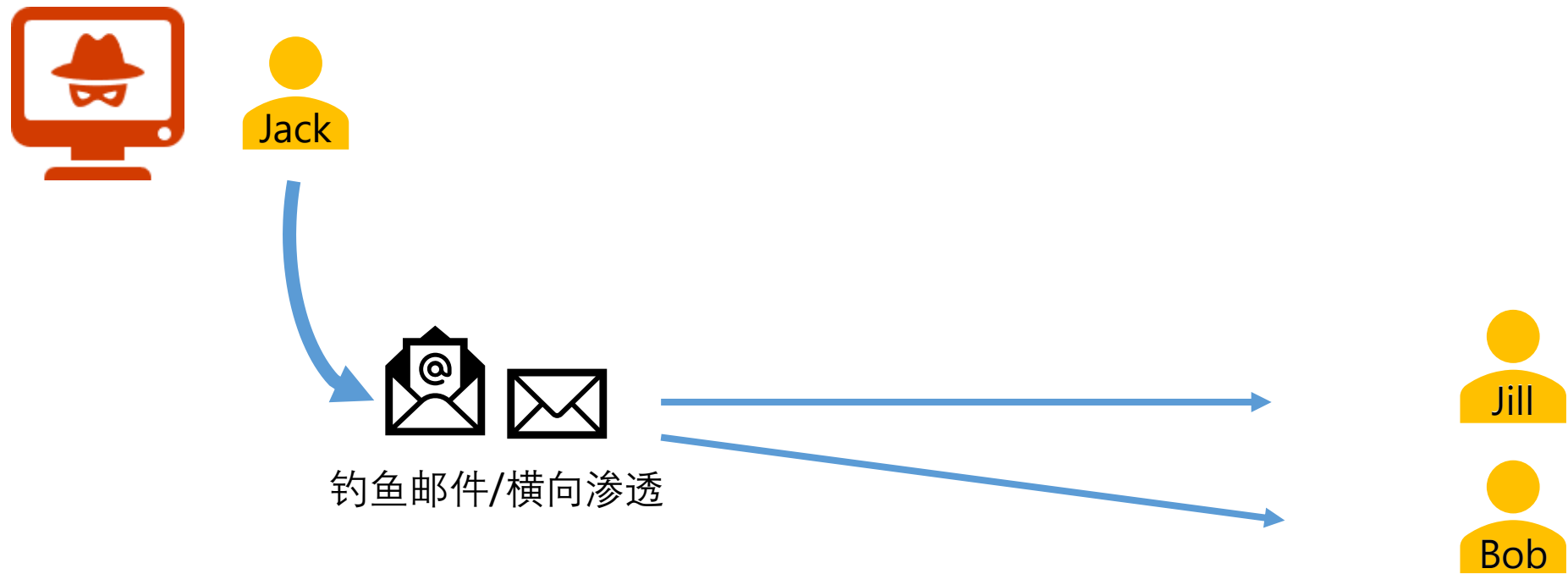
Jill

Bob



# 攻击内幕—— 电信诈骗

攻击者



# 攻击内幕—— 电信诈骗

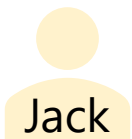
攻击者





# 攻击内幕—— 电信诈骗

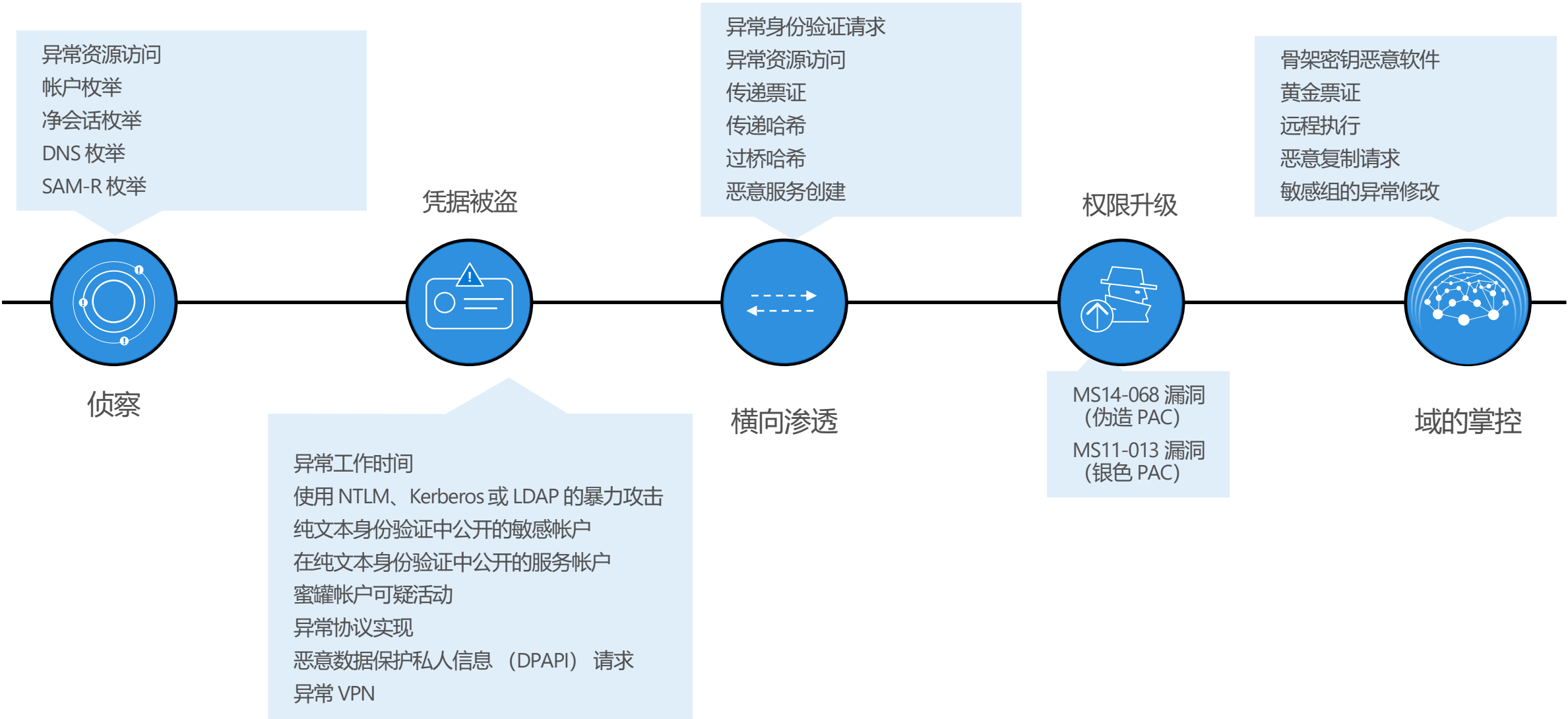
攻击者

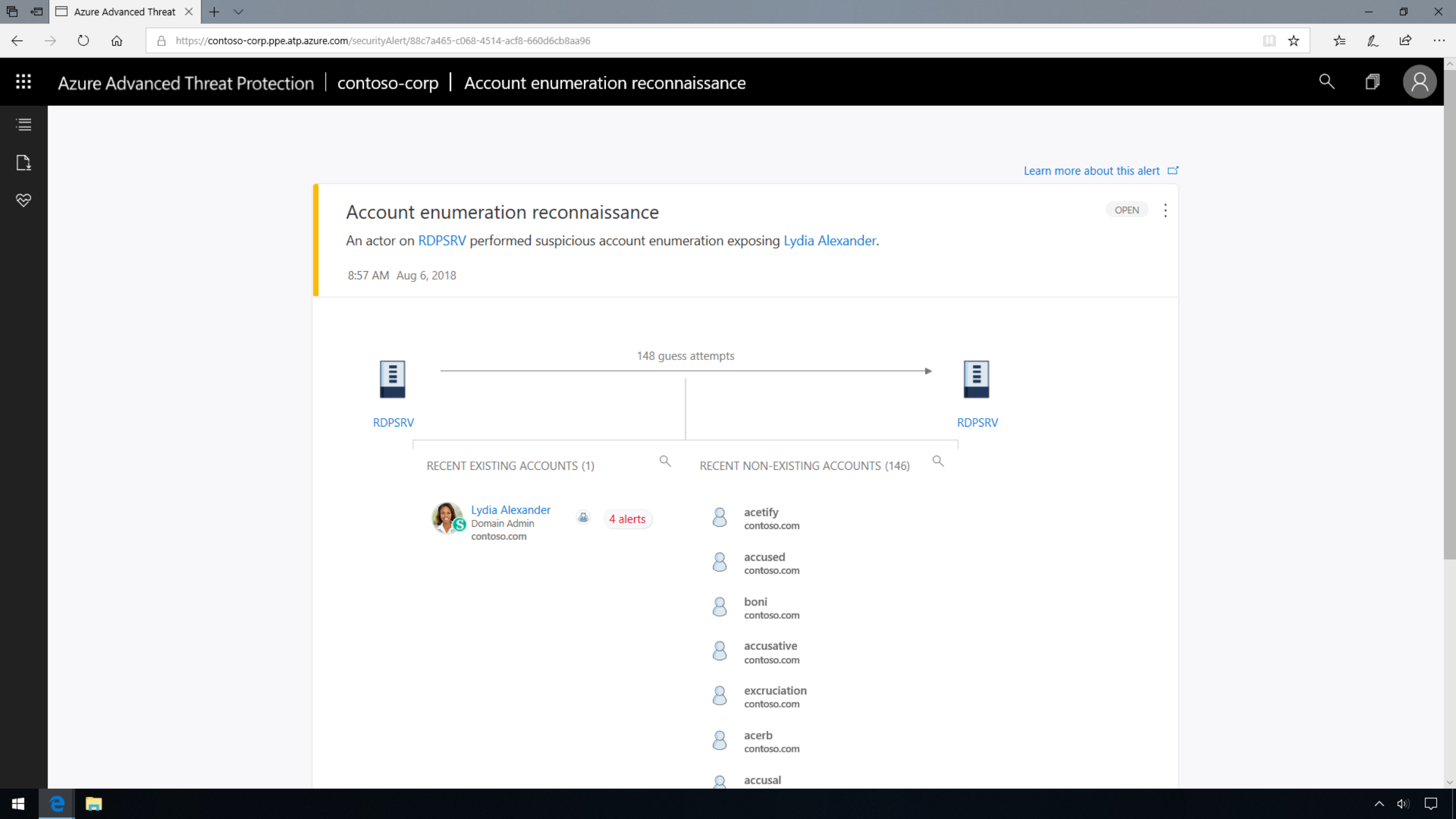


批准付款流程

建立付款流程

# AZURE ATP 具有广泛的可疑活动检测范围





[Learn more about this alert](#)

## Account enumeration reconnaissance

OPEN


An actor on **RDPSRV** performed suspicious account enumeration exposing **Lydia Alexander**.

8:57 AM Aug 6, 2018




### RECENT EXISTING ACCOUNTS (1)








### RECENT NON-EXISTING ACCOUNTS (146)

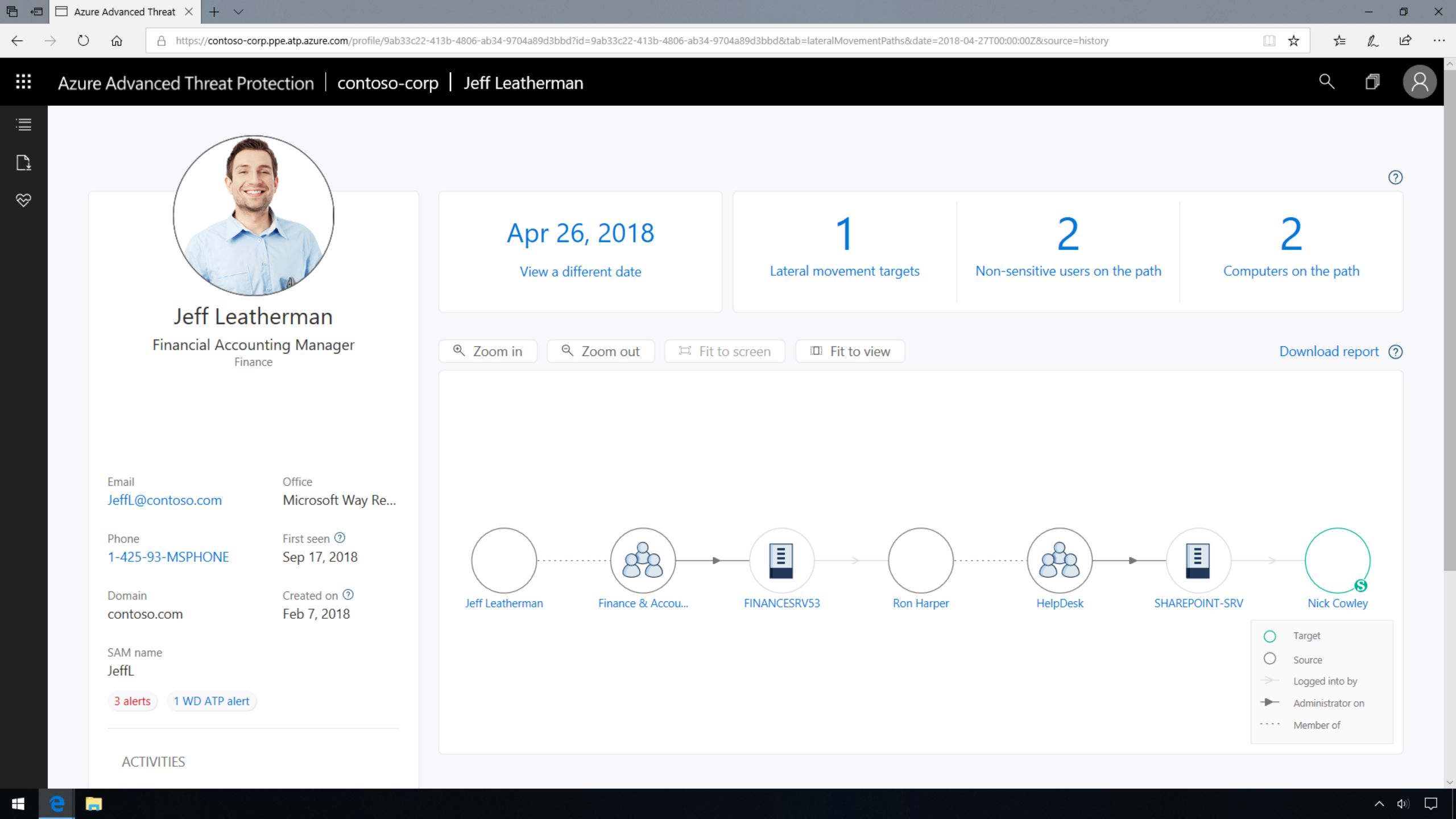


**Lydia Alexander**  
Domain Admin  
contoso.com



4 alerts

-  acetify  
contoso.com
-  accused  
contoso.com
-  boni  
contoso.com
-  accusative  
contoso.com
-  excruciation  
contoso.com
-  acerb  
contoso.com
-  accusal



# Azure Advanced Threat Protection profile timeline



Jeff Victim

 New

Email  
JeffV@contoso.com

Office  
Microsoft Way Re...

Phone  
1-425-93-MSPHONE

First seen   
Feb 20, 2018

Domain  
contoso.com

Created on   
Feb 7, 2018

SAM name  
JeffV

4 3

## ACTIVITIES

## DIRECTORY DATA

4

Open security alerts

O

Logged on computers

0

### Accessed resources

0

Accessed VPN locations

Showing latest 100 distinct entities

Go to ▾

Filter by

 Download activities

Today

11:09 AM

Phone number was changed from **None** to **1-425-93-MSPHONE**

11:09 AM

Mail address was changed from None to JeffV@contoso.com

Wednesday

8:11 PM

## Kerberos Golden Ticket activity

Suspicious usage of **Jeff Victim**'s Kerberos ticket, indicating a potential Golden Ticket attack, was detected.

Started at 9:00 AM Feb 21, 2018

OPEN

Tuesday

8:56 PM

Replicated Directory Services data from VICTIM-PC  
using Dsr | VICTIM-PC: 192.168.0.6

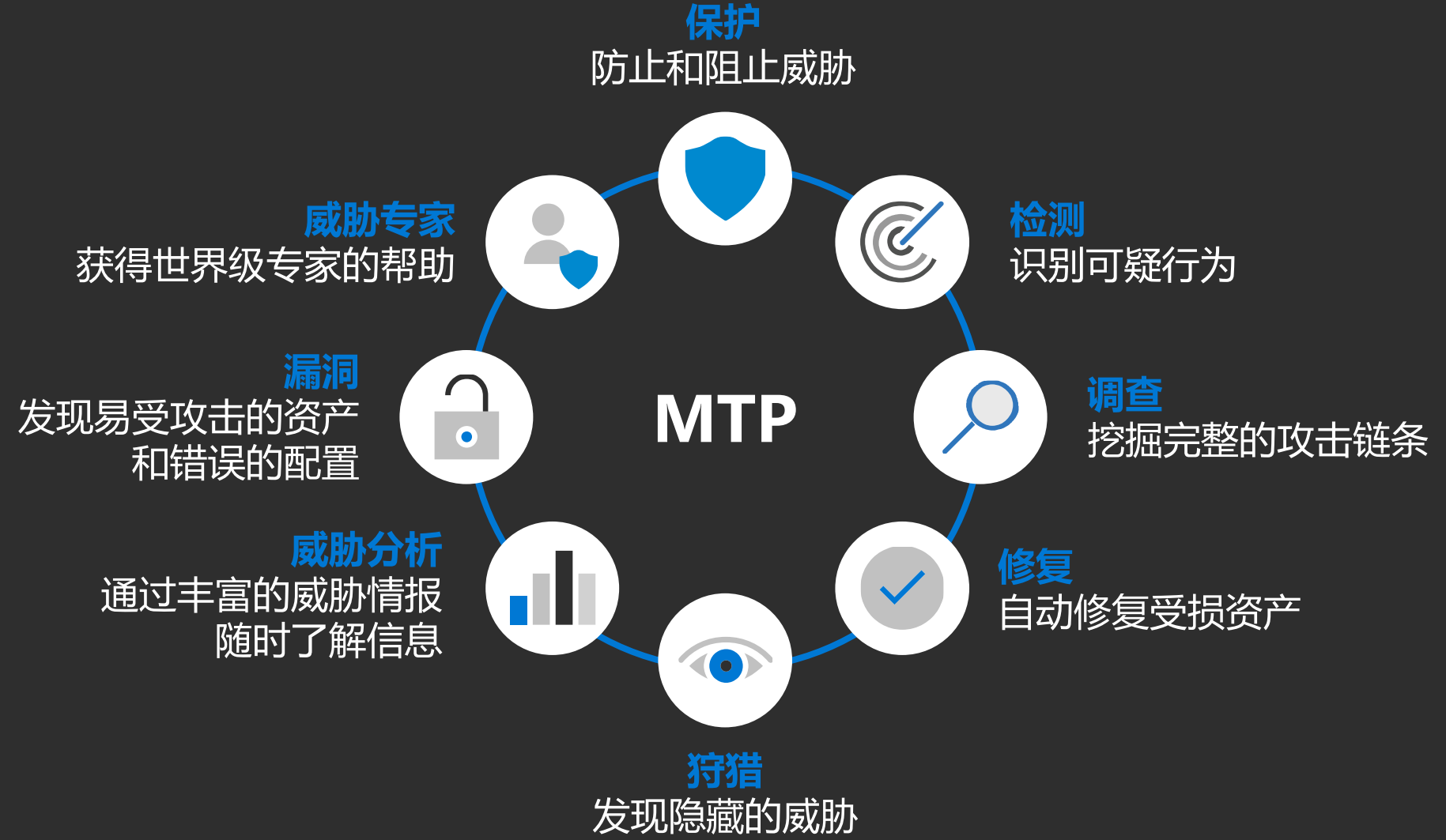
8:56 PM

## Malicious replication of directory services

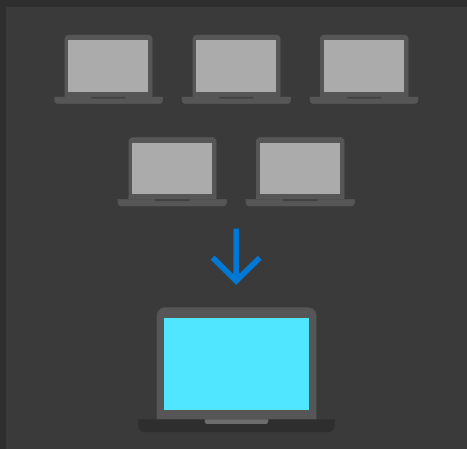
Malicious replication requests were successfully performed by [Jeff Victim](#) from [VICTIM BC](#) against

OPEN

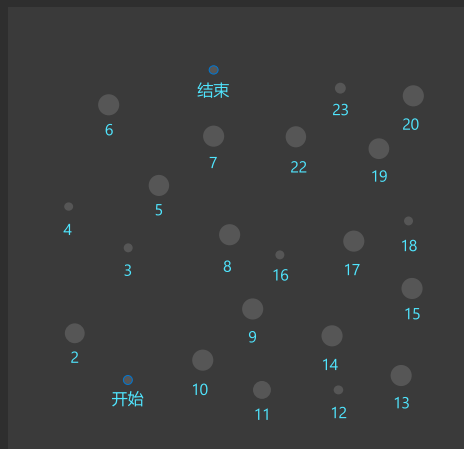
# MTP提供全方位的防御和保护



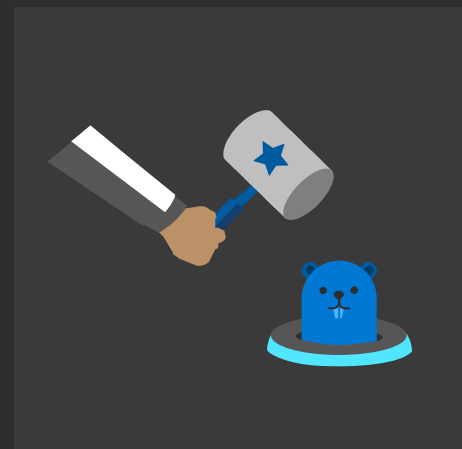
# 安全工具需要应对这些挑战



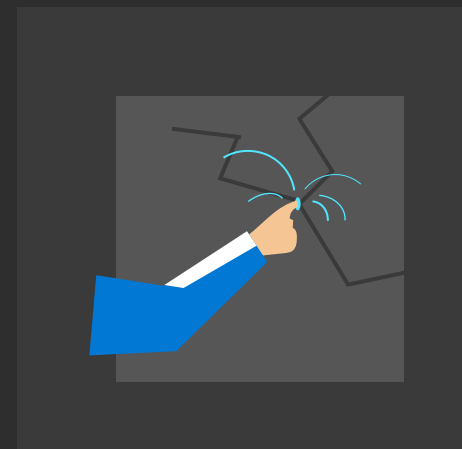
多个 to 单个管理界面



警报 to 事件



各个边界 to 协调防御



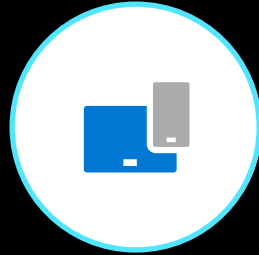
保护 to 预防

# Make sense of unparalleled signal



Users

Azure ATP



Endpoints

Microsoft Defender ATP



Cloud Apps

Microsoft Cloud  
App Security



Data

Office 365 ATP

**12 billion**

cloud activities  
inspected, monitored  
and controlled in 2019

**11 billion**

malicious and  
suspicious messages  
blocked in 2019

**300 billion**

user activities profiled  
and analyzed in 2019

**2.3 billion**

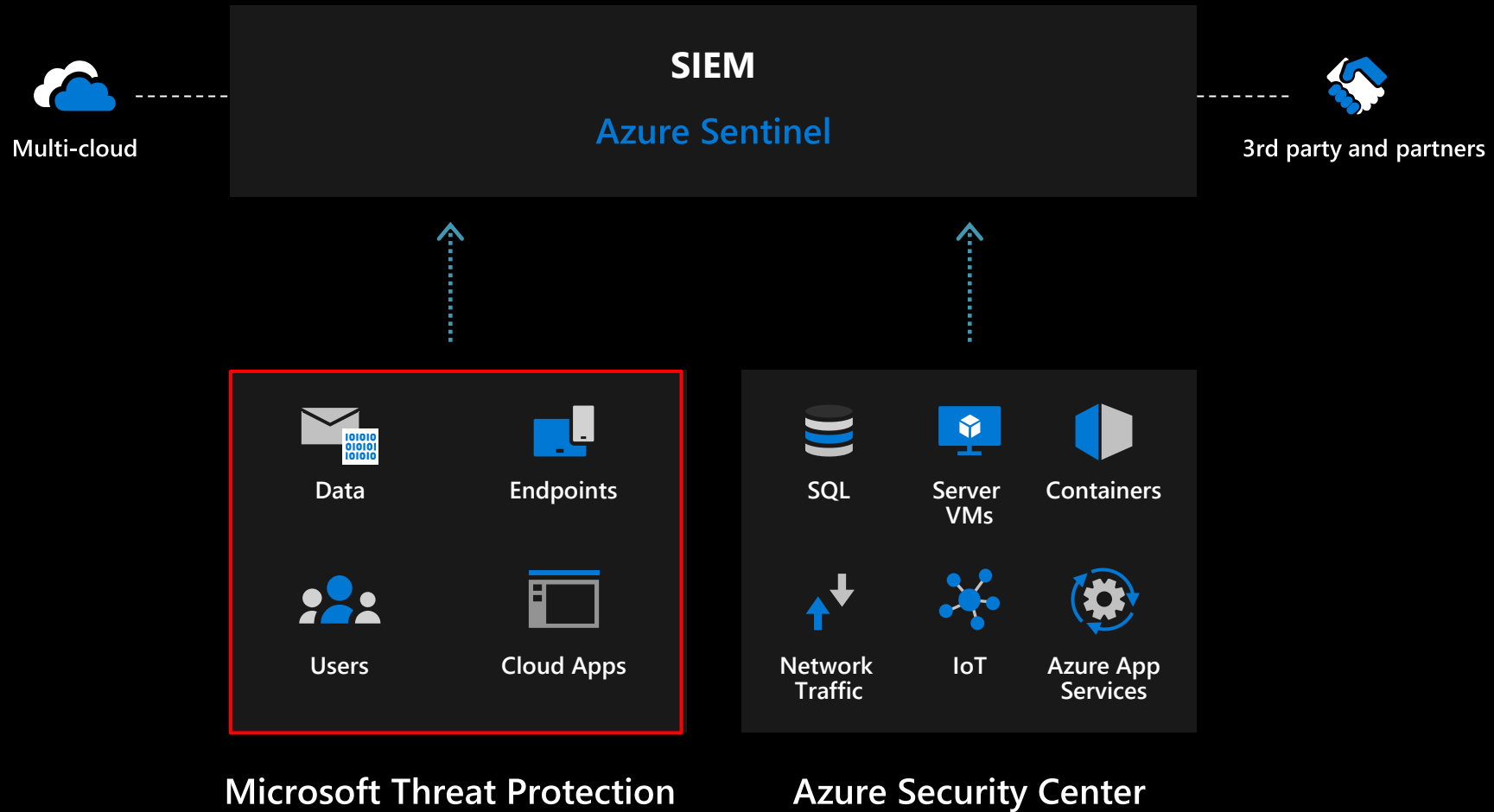
endpoint vulnerabilities  
discovered daily





# Demo - MTP

# Gain insights across your enterprise



## SWOT: Microsoft, Security Products and Features, Worldwide

Published 18 December 2018 - ID G00371388 - 31 min read

By Analysts Sid Deshpande, Deborah Kish

Microsoft is now a security vendor. Technology product managers at security services providers can use this document to identify opportunities to reshape their product roadmaps and integrations based on Microsoft's changed approach to security.

[SWOT: Microsoft, Security Products and Features, Worldwide](#)

## 终端保护平台象限领导者

Figure 1. Magic Quadrant for Endpoint Protection Platforms



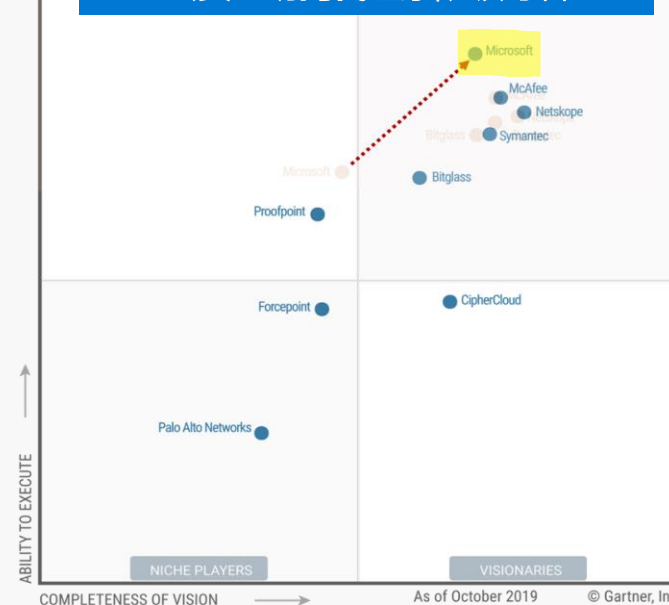
[Gartner names Microsoft a Leader in 2019 Endpoint Protection Platforms Magic Quadrant](#) / (Full report)

## 访问管理象限领导者

Figure 1. Magic Quadrant for Access Management



## 云安全访问代理象限领导者



## 统一端点管理象限领导者

Figure 1. Magic Quadrant for Unified Endpoint Management



F-Secure	SAFE 17	TOP PRODUCT	6	6	6
kaspersky	Internet Security 19.0	TOP PRODUCT	5	6	6
Microsoft	Windows Defender 4.18	TOP PRODUCT	6	6	6
Norton	Norton Security 22.17	TOP PRODUCT	5	6	6
TREND MICRO	Internet Security 15.0	TOP PRODUCT	6	5.5	6
VIPRE	VIPRE AdvancedSecurity 11.0	TOP PRODUCT	5.5	6	6

Microsoft Defender gets full score in AV-Test  
仅有四个产品获得全满分