

**Microsoft Online Tech Forum** 

微软在线技术峰会

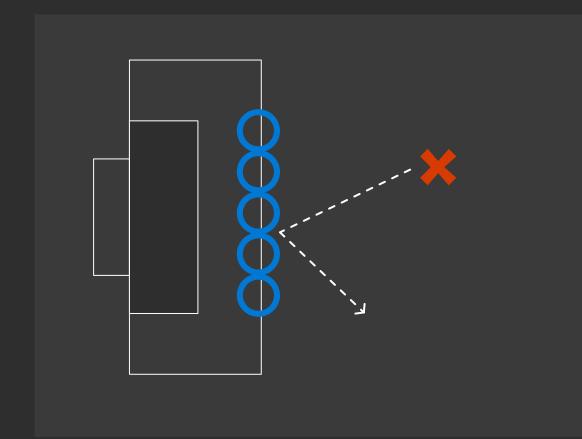
洞察威胁,全面保护 ——Microsoft Threat Protection 侦测调查的威力

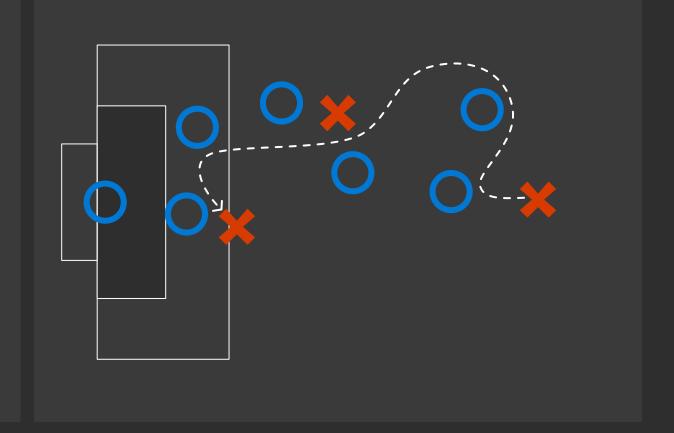
Holly Gong (龚祺莎)

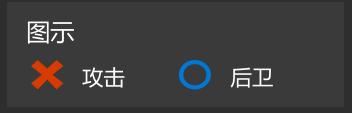
"防御者用列表思考。攻击者用图表思考。只要这一点是真的,攻击者就会赢。"

## 我们如何建立我们的防御

## 实际发生的情况







## 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。
- <u>Sodinokibi勒索病毒</u>: 在不到半年时间,该勒索病毒已非法获利数百万美元。
- <u>Globelmposter勒索病毒</u>: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"。
- <u>Stop勒索病毒</u>: 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。

Gandcrab (\/)\_(s \_\_ s)\_(\/)



Seller 424 posts Joined 12/18/17 (ID: 84324) Activity virology

Posted 18 hours ago

All the good things come to an end.

For the year of working with us, people have earned more than \$ 2 billion, we have become a nominal name in the field of the underground in the direction of crypto-fiber. Earnings with us per week averaged \$ 2,500,000.

Report post 45

We personally earned more than **150 million** dollars per year. We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet.

We were glad to work with you. But, as it is written above, all good things come to an end.

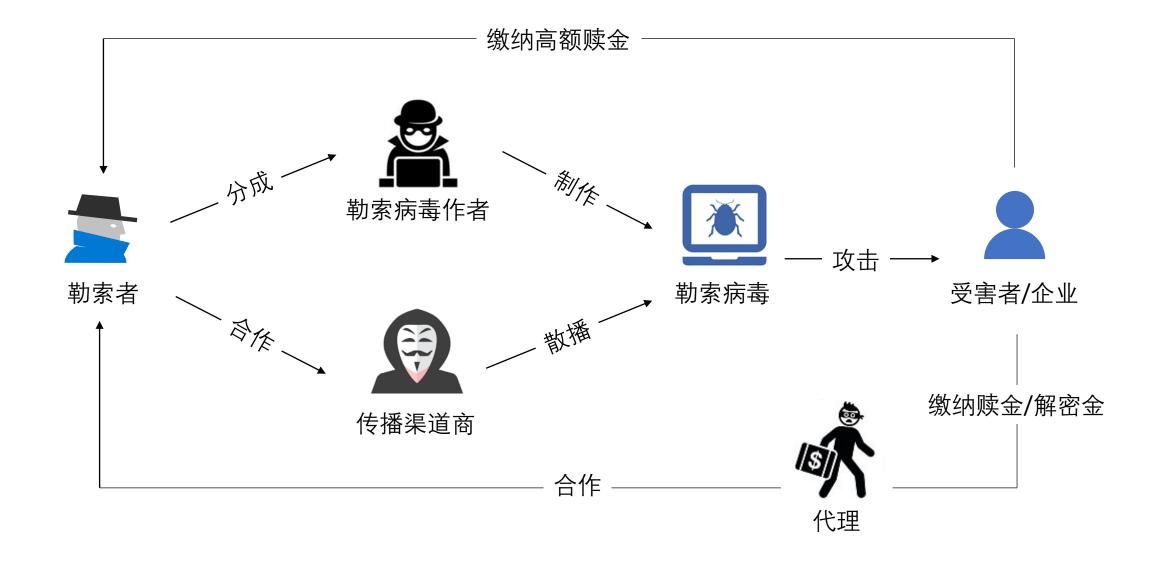
We are leaving for a well-deserved retirement. We have proven that by doing evil deeds, retribution does not come. We proved that in a year you can earn money for a lifetime. We have proved that it is possible to become number one not in our own words, but in recognition of other people.

In this regard, we:

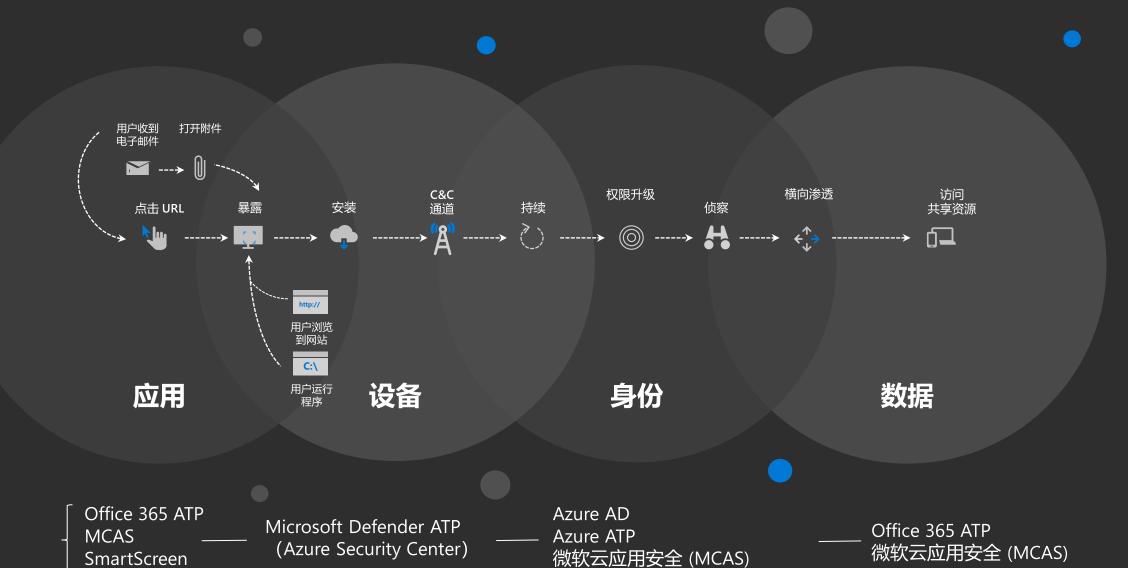
- 1. Stop the set of adverts;
- 2. We ask the adverts to suspend the flows;
- 3. Within 20 days from this date, we ask adverts to monetize their bots by any means;
- 4. Victims If you buy, now. Then your data no one will recover. Keys will be deleted.

That's all. The topic will be deleted in a month. Thank you all for the work.

# 勒索病毒产业链



## 攻击链条解析——跨越防御边界

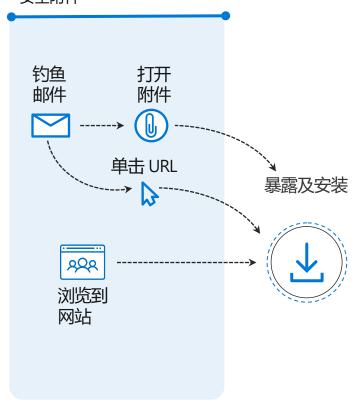


微软

# 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





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

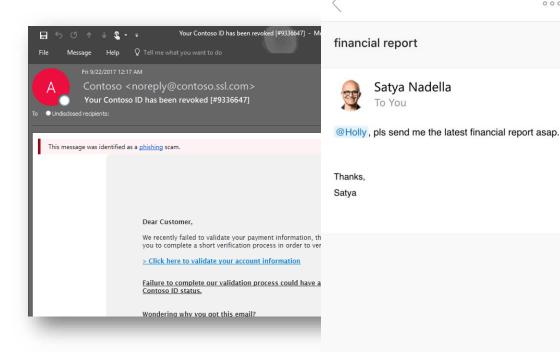


安全附件

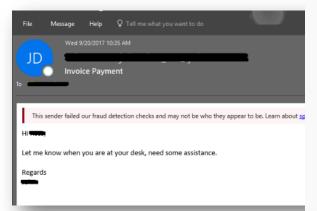
防范恶意附件

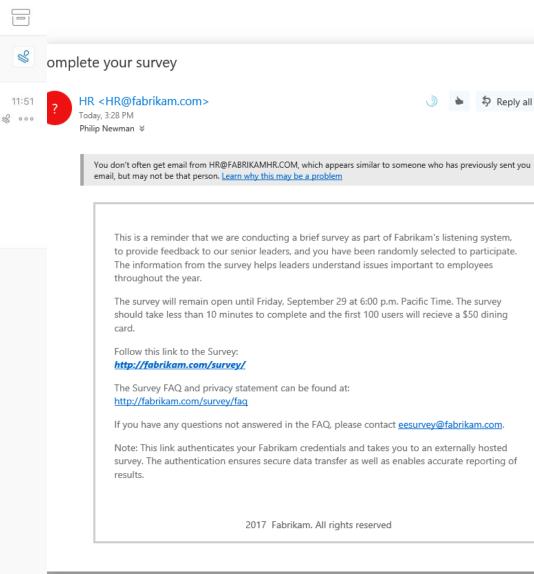


000



Reply to All





24

#### omplete your survey





This is a reminder that we are conducting a brief survey as part of Fabrikam's listening system, to provide feedback to our senior leaders, and you have been randomly selected to participate. The information from the survey helps leaders understand issues important to employees throughout the year.

The survey will remain open until Friday, September 29 at 6:00 p.m. Pacific Time. The survey should take less than 10 minutes to complete and the first 100 users will recieve a \$50 dining card.

Follow this link to the Survey:

#### http://fabrikam.com/survey/

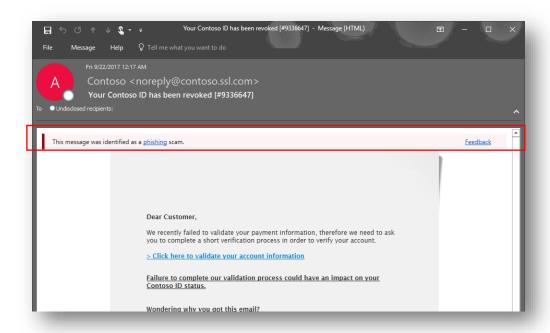
The Survey FAQ and privacy statement can be found at:

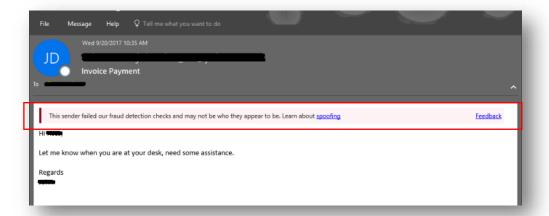
#### http://fabrikam.com/survey/faq

If you have any questions not answered in the FAQ, please contact eesurvey@fabrikam.com.

Note: This link authenticates your Fabrikam credentials and takes you to an externally hosted survey. The authentication ensures secure data transfer as well as enables accurate reporting of results.

2017 Fabrikam. All rights reserved





#### Complete your survey



#### HR <HR@fabrikam.com>

Today, 3:28 PM Philip Newman ♥







You don't often get email from HR@FABRIKAMHR.COM, which appears similar to someone who has previously sent you email, but may not be that person. Learn why this may be a problem

This is a reminder that we are conducting a brief survey as part of Fabrikam's listening system, to provide feedback to our senior leaders, and you have been randomly selected to participate. The information from the survey helps leaders understand issues important to employees throughout the year.

The survey will remain open until Friday, September 29 at 6:00 p.m. Pacific Time. The survey should take less than 10 minutes to complete and the first 100 users will recieve a \$50 dining card.

Follow this link to the Survey:

#### http://fabrikam.com/survey/

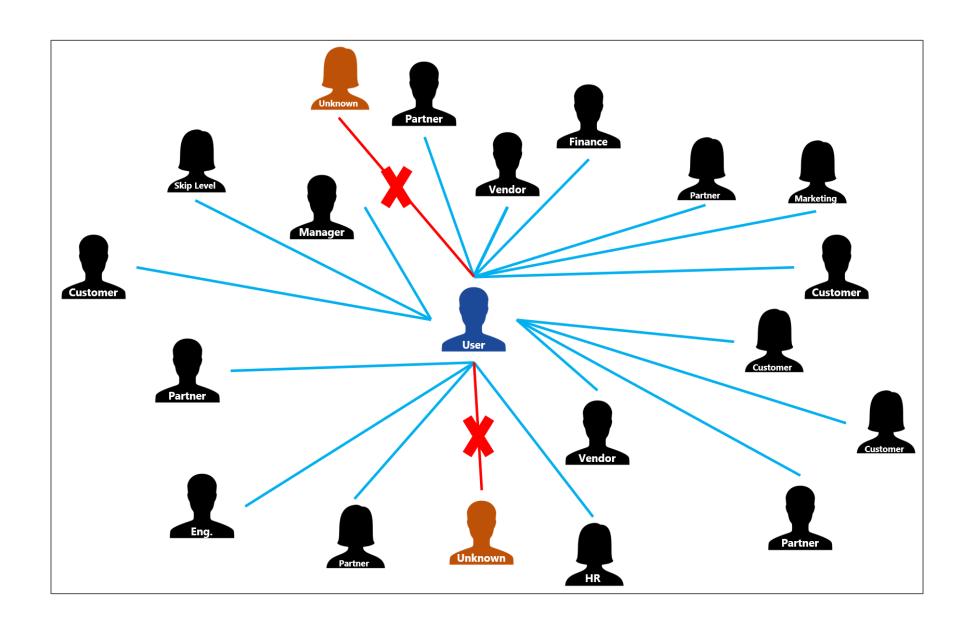
The Survey FAQ and privacy statement can be found at:

http://fabrikam.com/survey/faq

If you have any questions not answered in the FAQ, please contact eesurvey@fabrikam.com.

Note: This link authenticates your Fabrikam credentials and takes you to an externally hosted survey. The authentication ensures secure data transfer as well as enables accurate reporting of results.

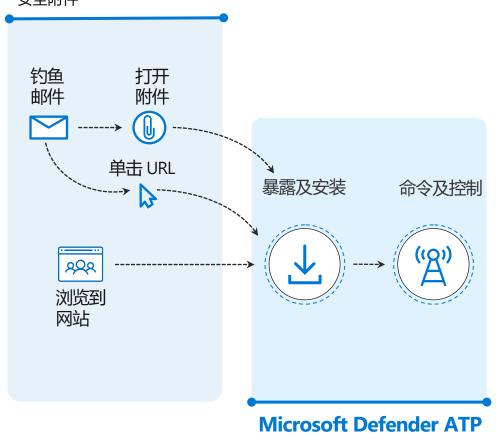
2017 Fabrikam. All rights reserved



## 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



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?

Post-Breach

#### **Endpoint Detection and Response (EDR)**

**Detect** security incidents at the endpoint, **Investigate** security incidents, **Contain** the incident, Remediate endpoints

#### **Endpoint Protection Platform (EPP)**

Device control
Firewall
Anti-Malware
Application Sandboxing
Vulnerability assessment
Application control
Enterprise mobility management (EMM)
Memory protection
Behavioral monitoring of application code
Full-disk and file encryption
Endpoint data loss prevention (DLP)

Windows Defender Advanced Threat Protection

TREND

Symantec

McAfee

Windows Defender

Advanced Threat Protection

COUNTRINE

CROWDSTRIKE

SentinelOne

Cybereason

**Antivirus** 

## EPP and EDR Leader

Figure 1. Magic Quadrant for Endpoint Protection Platforms



#### FORRESTER RESEARCH

#### THE FORRESTER WAVE™

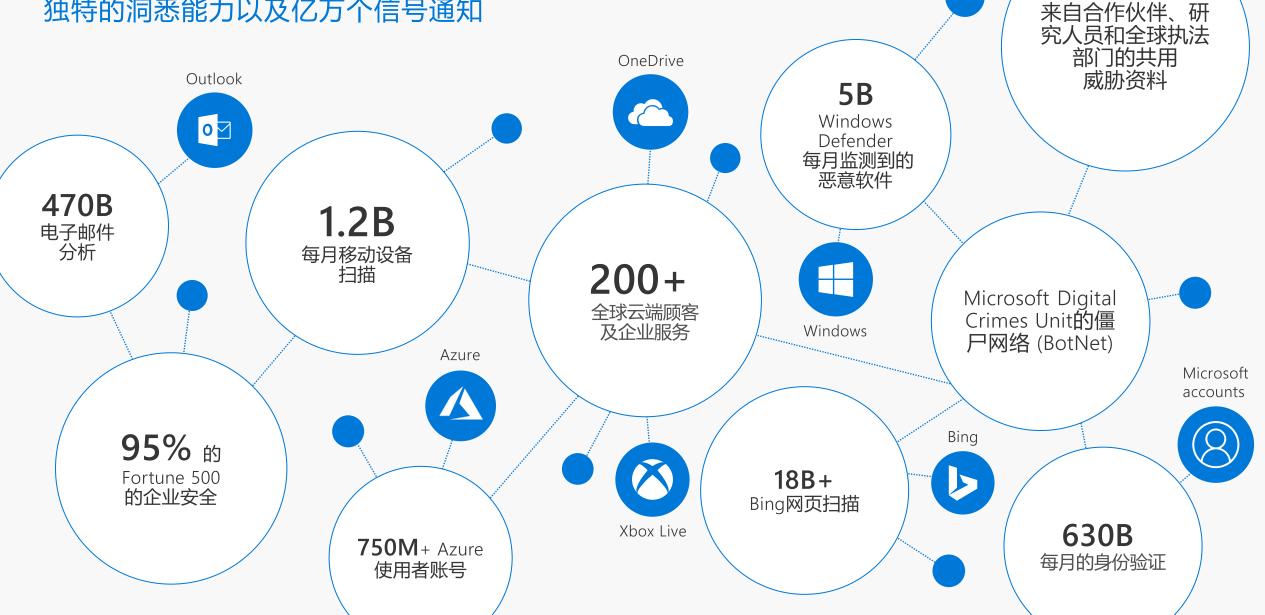
Enterprise Detection And Response

Q1 2020

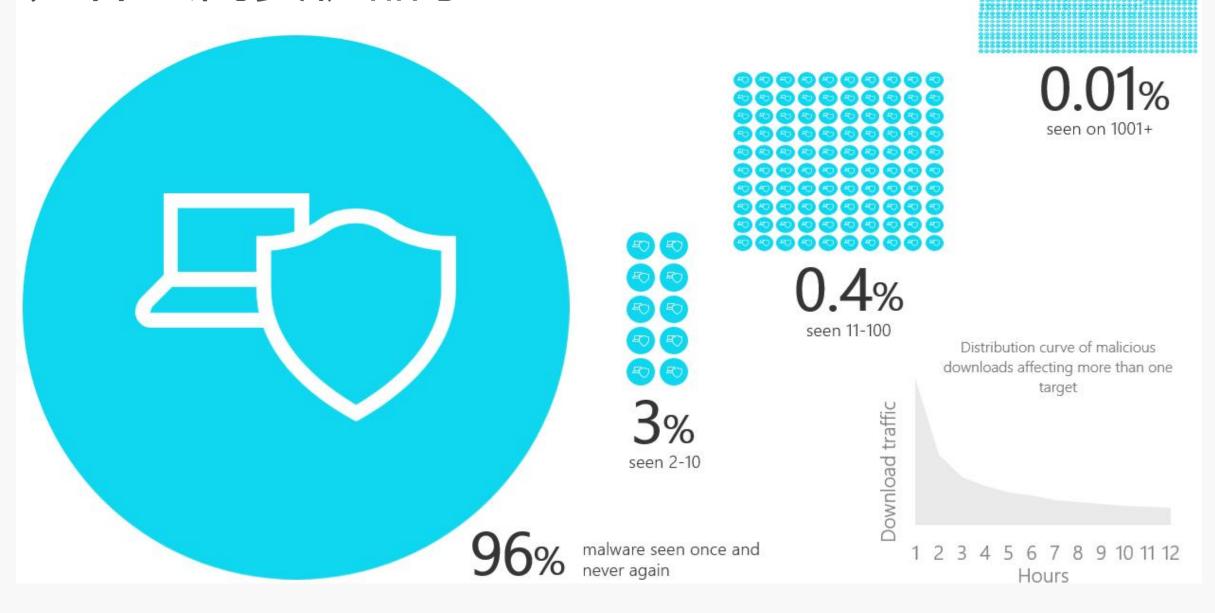


# Microsoft 智能安全图谱

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?



# Microsoft Defender ATP 机器学习层级架构

LOCAL ML MODELS, BEHAVIOR-BASED DETECTION ALGORITHMS, GENERICS AND HEURISTICS

milliseconds

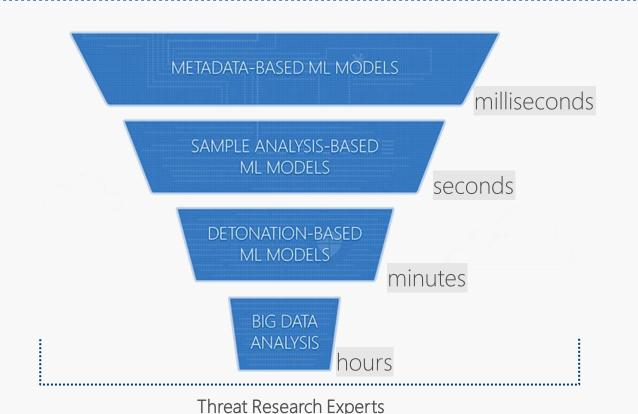
Client – 大部分的恶意软件会被高精准的 Windows Defender AV通过本地的机器学习模 型, 启发法及行为数据分析, 得以成功拦截











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







Sample - 可疑文件的副本将上传以通过multiclass及深度神经网络等规则讲行评估判断



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



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



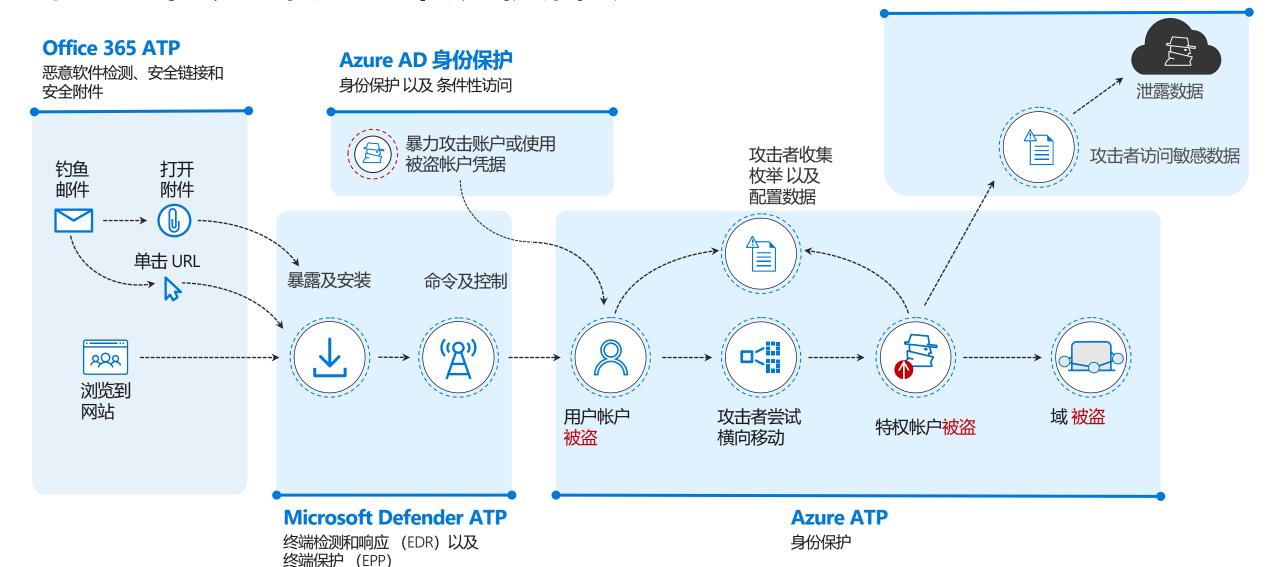


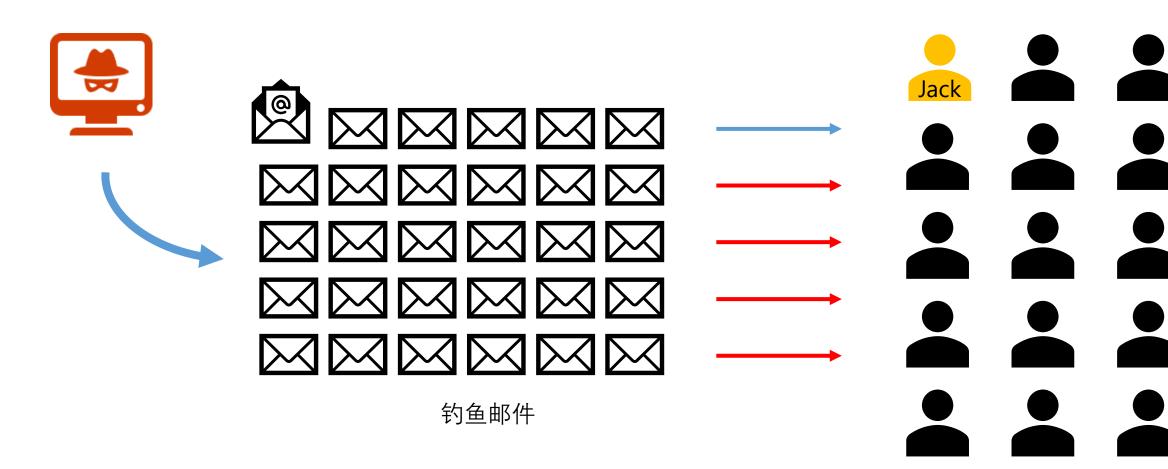
## Demo - MDATP

## 在整个攻击链条中提供保护

#### 微软云应用安全 (MCAS)

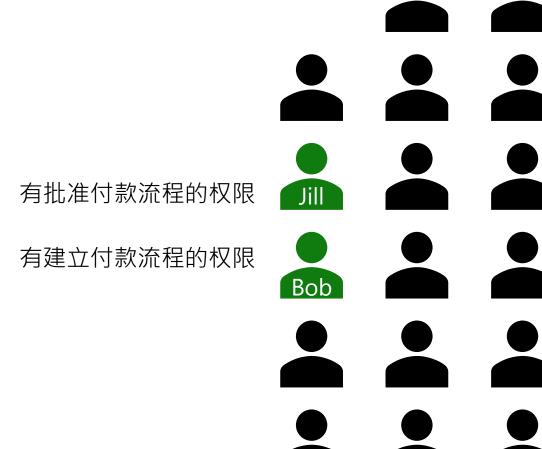
扩展对其他云应用的保护及条件性访问

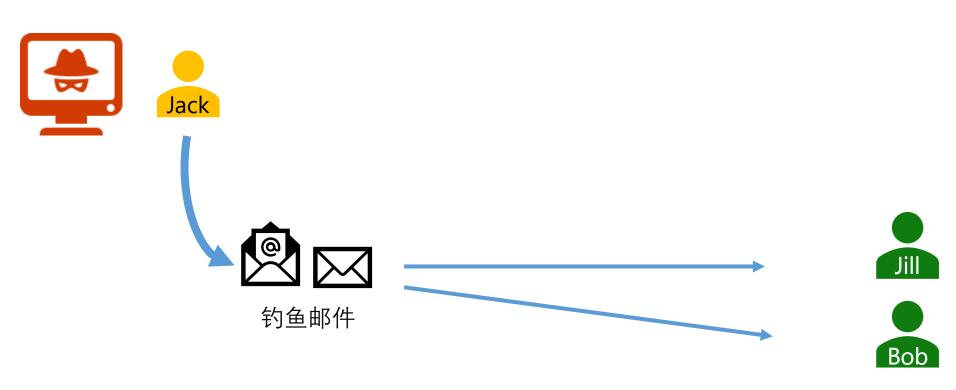


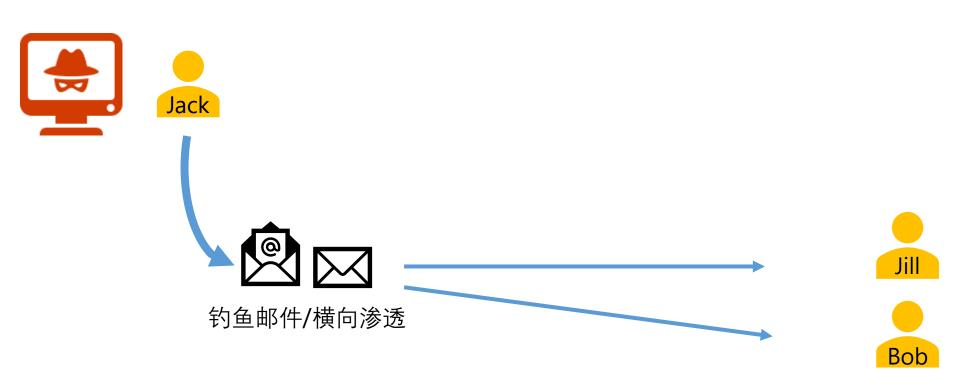










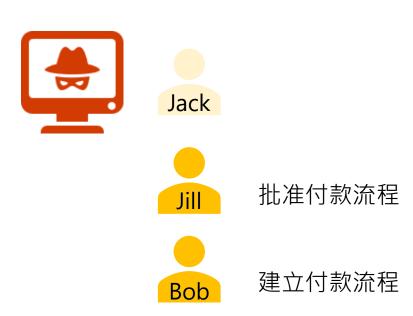












### AZURE ATP 具有广泛的可疑活动检测范围

异常资源访问

帐户枚举

净会话枚举

DNS 枚举

SAM-R 枚举

异常身份验证请求

异常资源访问

传递票证

传递哈希

过桥哈希

恶意服务创建

骨架密钥恶意软件

黄金票证

远程执行

恶意复制请求

敏感组的异常修改



侦察

凭据被盗



异常工作时间

使用 NTLM、Kerberos 或 LDAP 的暴力攻击

纯文本身份验证中公开的敏感帐户

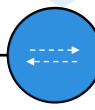
在纯文本身份验证中公开的服务帐户

蜜罐帐户可疑活动

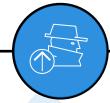
异常协议实现

恶意数据保护私人信息 (DPAPI) 请求

异常 VPN



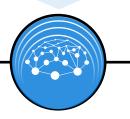
横向渗透



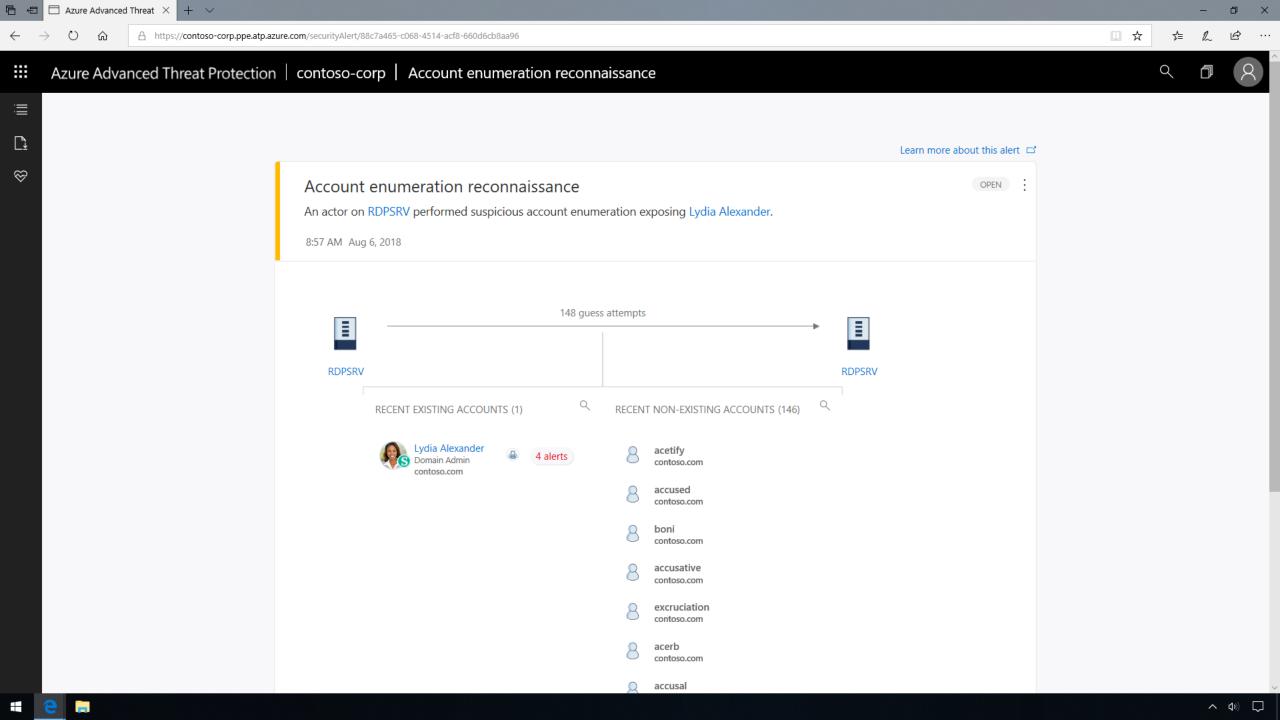
权限升级

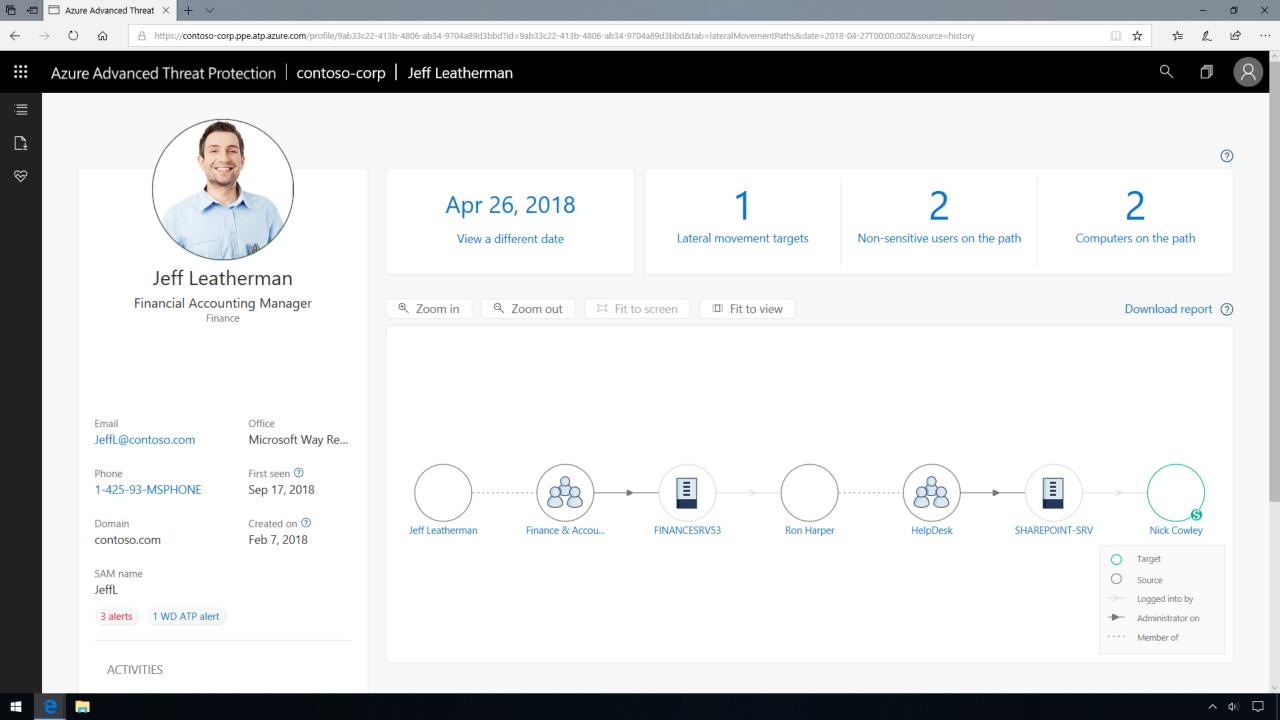
MS14-068 漏洞 (伪造 PAC)

MS11-013 漏洞 (银色 PAC)

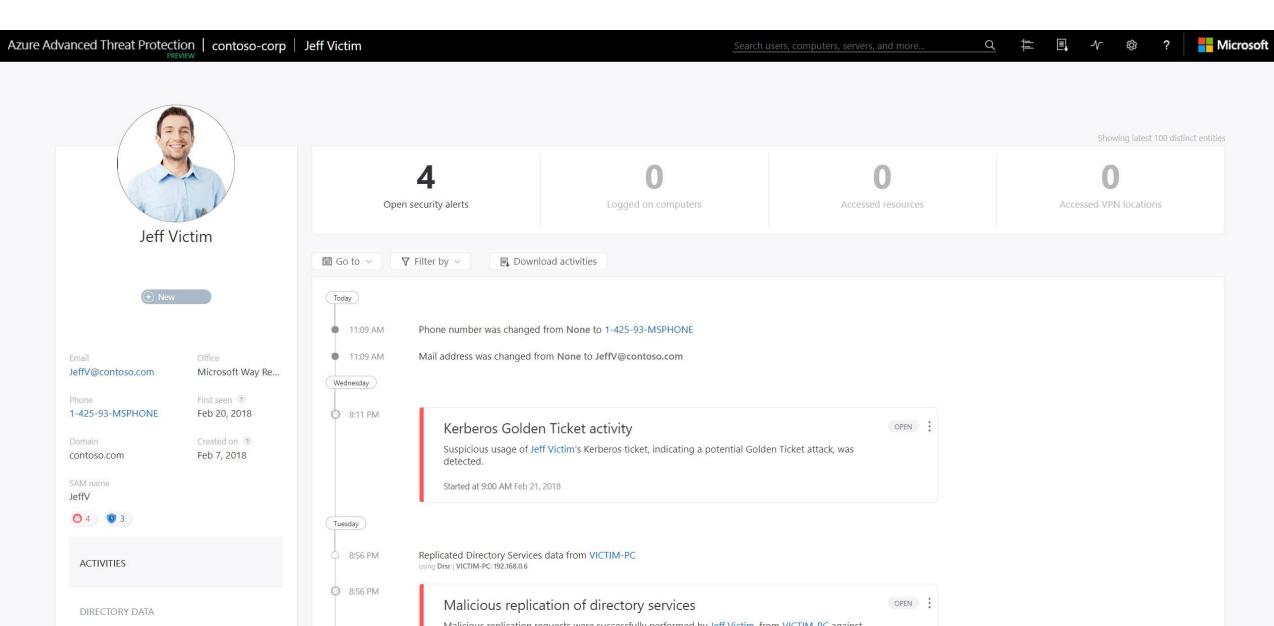


域的掌控

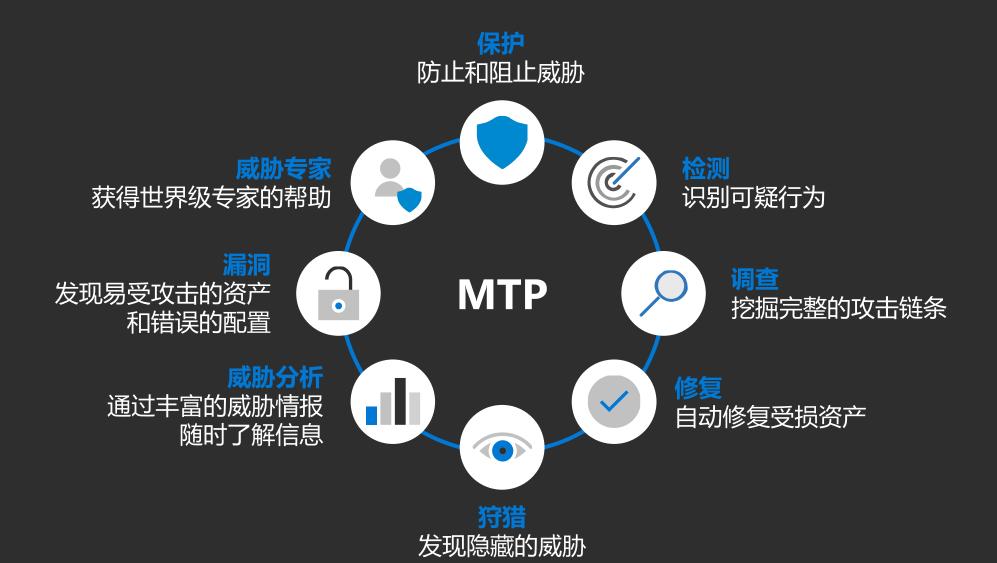




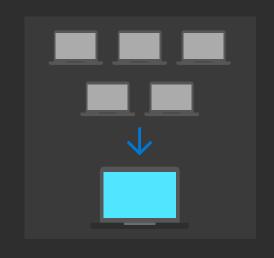
## Azure Advanced Threat Protection profile timeline



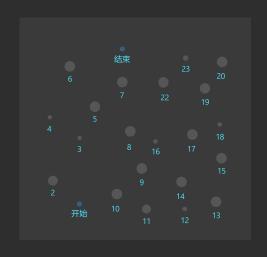
## MTP提供全方位的防御和保护



## 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

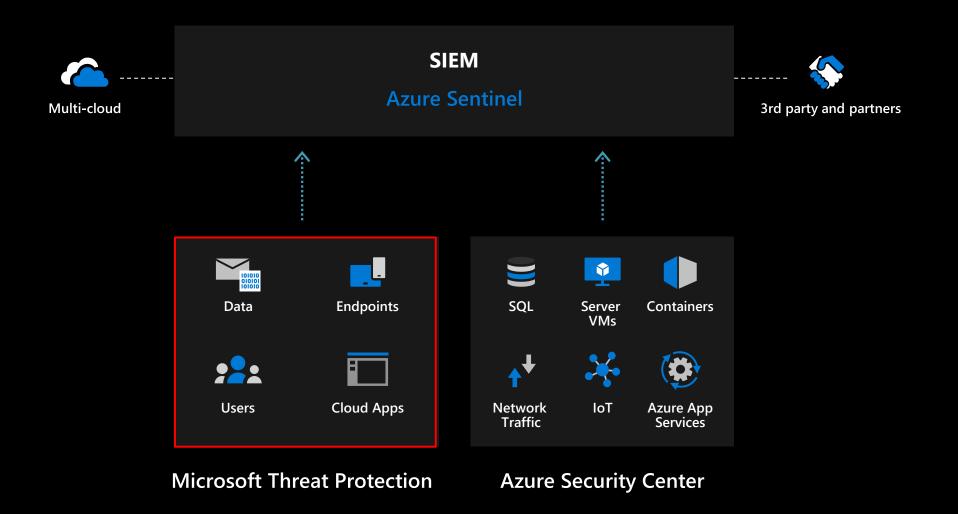
### 2.3 billion

endpoint vulnerabilities discovered daily



## Demo - MTP

## Gain insights across your enterprise



Gartner. Licensed for Distribution

### 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



As of October 2019

COMPLETENESS OF VISION

#### 统一端点管理象限领导者





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