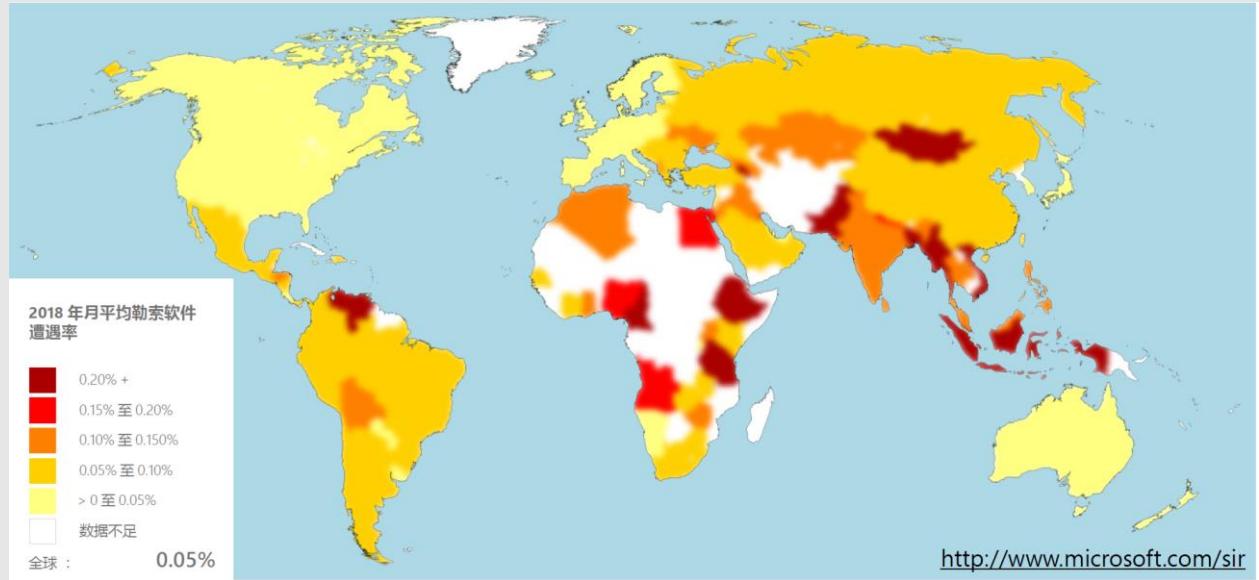




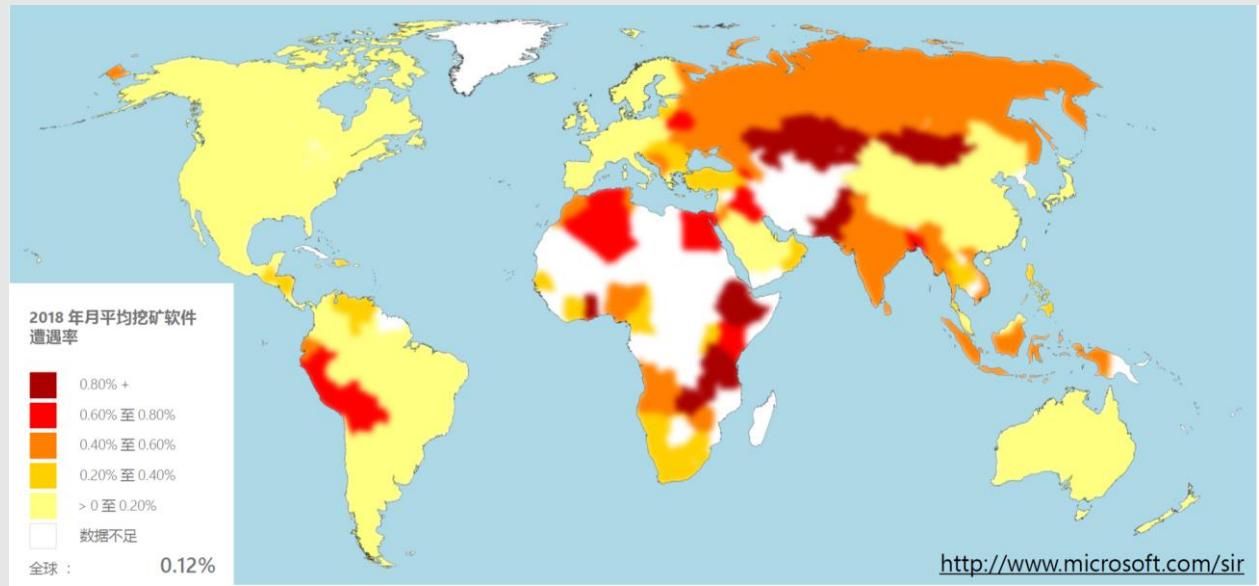
Microsoft Security

Yi Liang
China OCP PTS
yiliang@microsoft.com

攻击手段的演变



VS



November 14

2019

Showing All Countries
Show Attacks

Large Unusual Combined

Large attacks on United States, United Kingdom, China, + 5 others

Color Attacks By

Type Source Port
 Duration Dest. Port

- TCP Connection
- Volumetric
- Fragmentation
- Application

Size (Bandwidth, in Gbps)

25 5 1

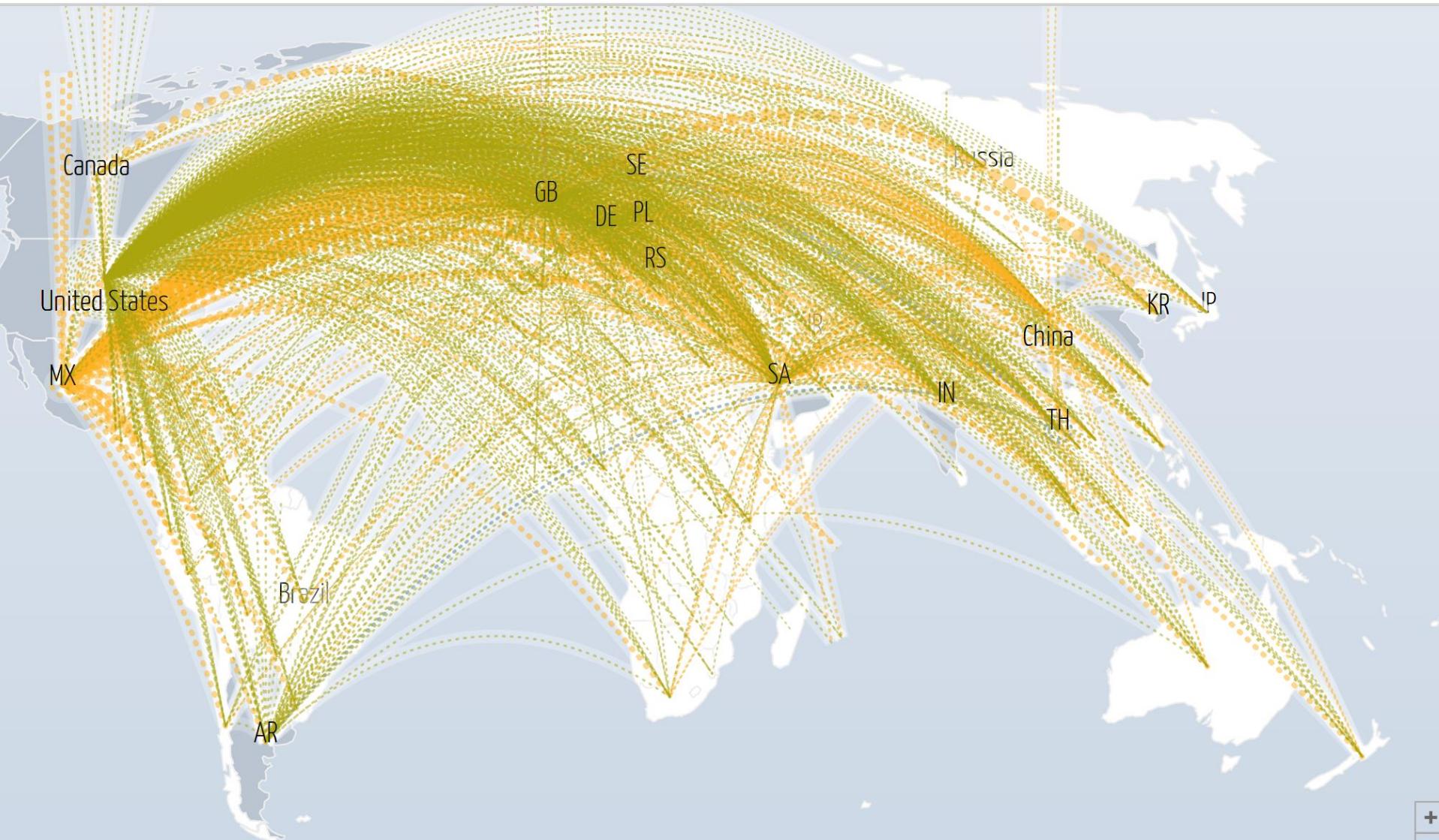
Shape (source + destination)

between two countries

internal

either source or dest. unknown

[Get Embed Code](#)



Attack Bandwidth (All Countries), Gbps Dates are shown in GMT Data shown represents the top ~.1% of reported attacks. Graph below is capped at 10k Gbps

Presented by Jigsaw



一份完整的
的个人身份
数据

撞库即
服务的
每月订
阅费

勒索软件
即服务
的每月
订阅费

资金转移
(钱骡)

42亿
客户记录遭到泄露¹

99 天
从泄露到被检测²

1700万美元
安全漏洞导致的平均损失³



每个企业平均5000人

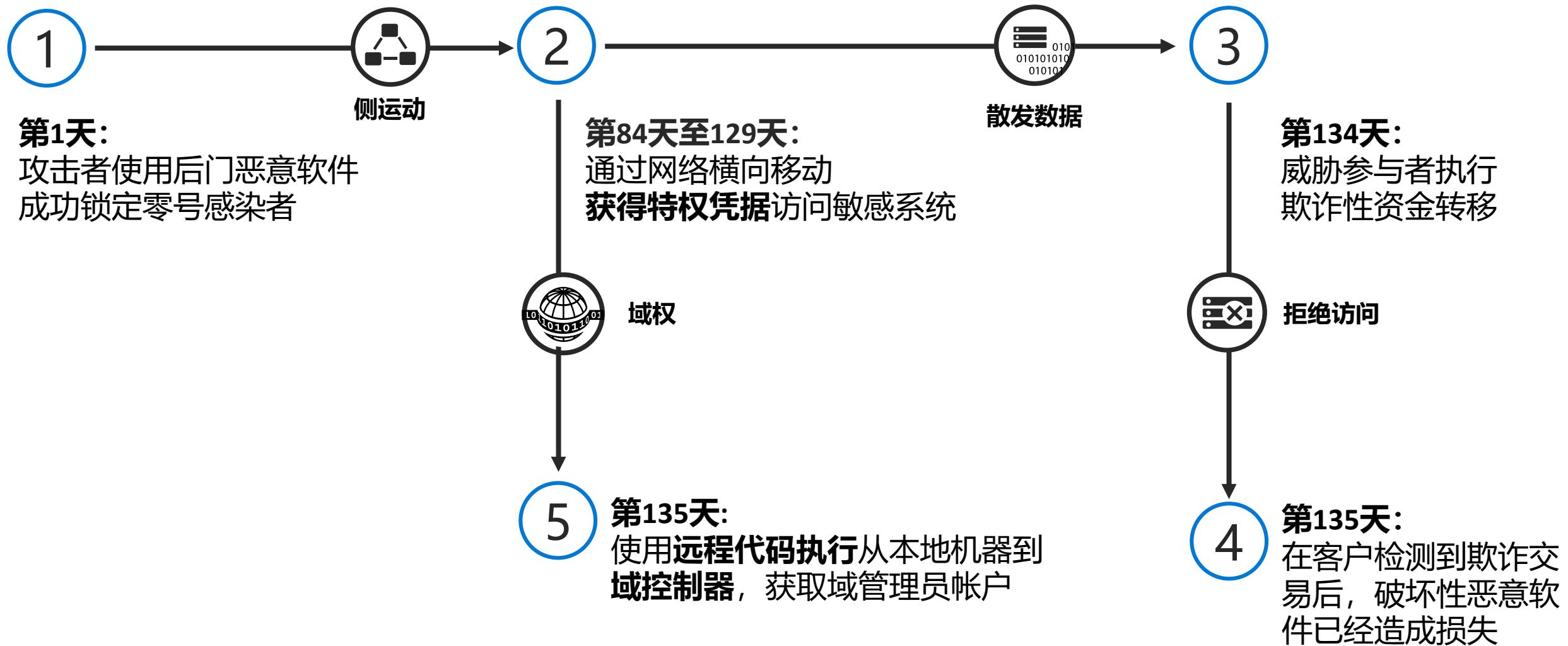
3,400美元
安全漏洞导致的人均损失

¹Source: <https://pages.riskbasedsecurity.com/hubfs/Reports/2016%20Year%20End%20Data%20Breach%20QuickView%20Report.pdf> Date: 2017

²Source: <https://www.fireeye.com/blog/threat-research/2017/03/m-trends-2017.html> Date: March 2017

³Source: Cyber crime--a risk you can manage: Information management and governance to protect business innovation business white paper Date: November 2016 Microsoft Document: Office 365 Security and Compliance Infographic, CDOC EBC Presentation

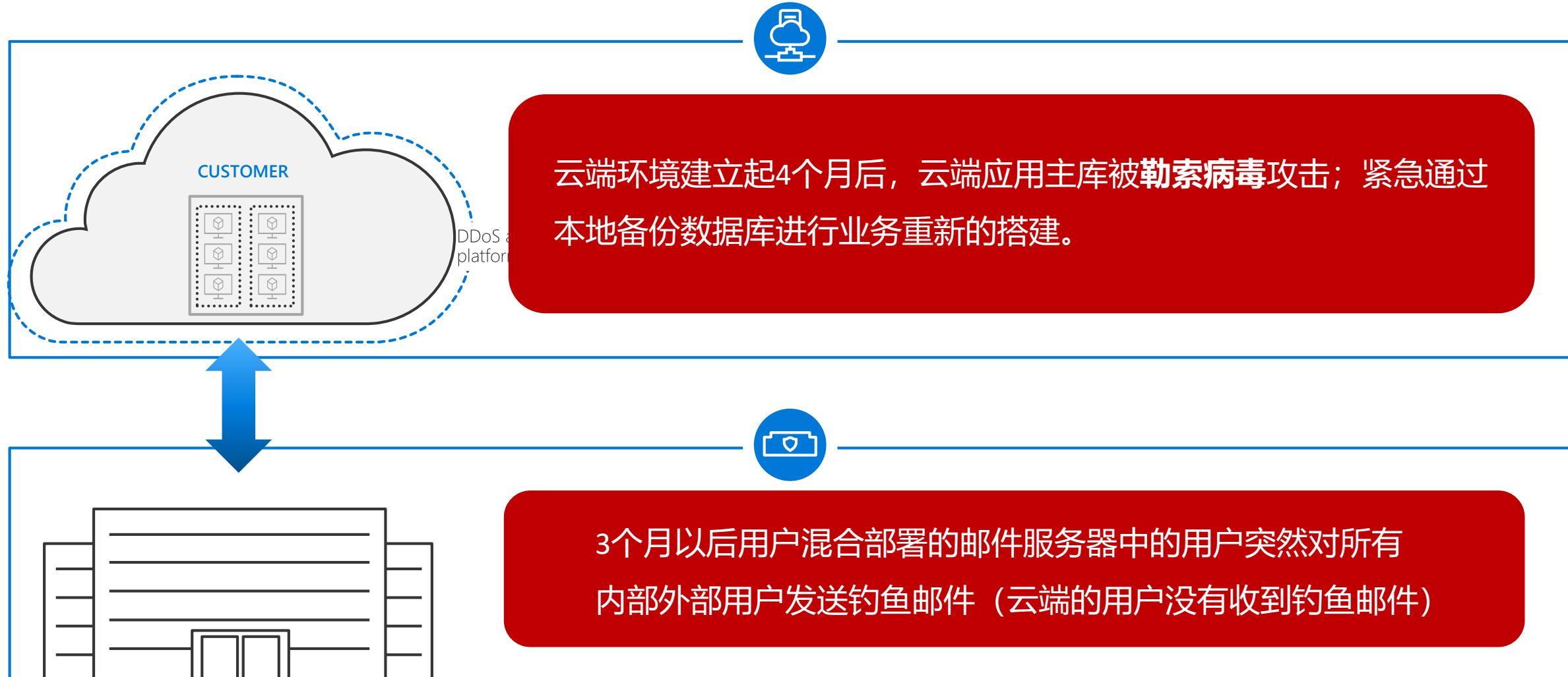
攻击时间表



Customer Real Case



Customer Real Case



跨运营、技术和合作伙伴关系
提供无与伦比的安全性

仅网络安全方面
10亿美元年度投资

3500€全球安全专家

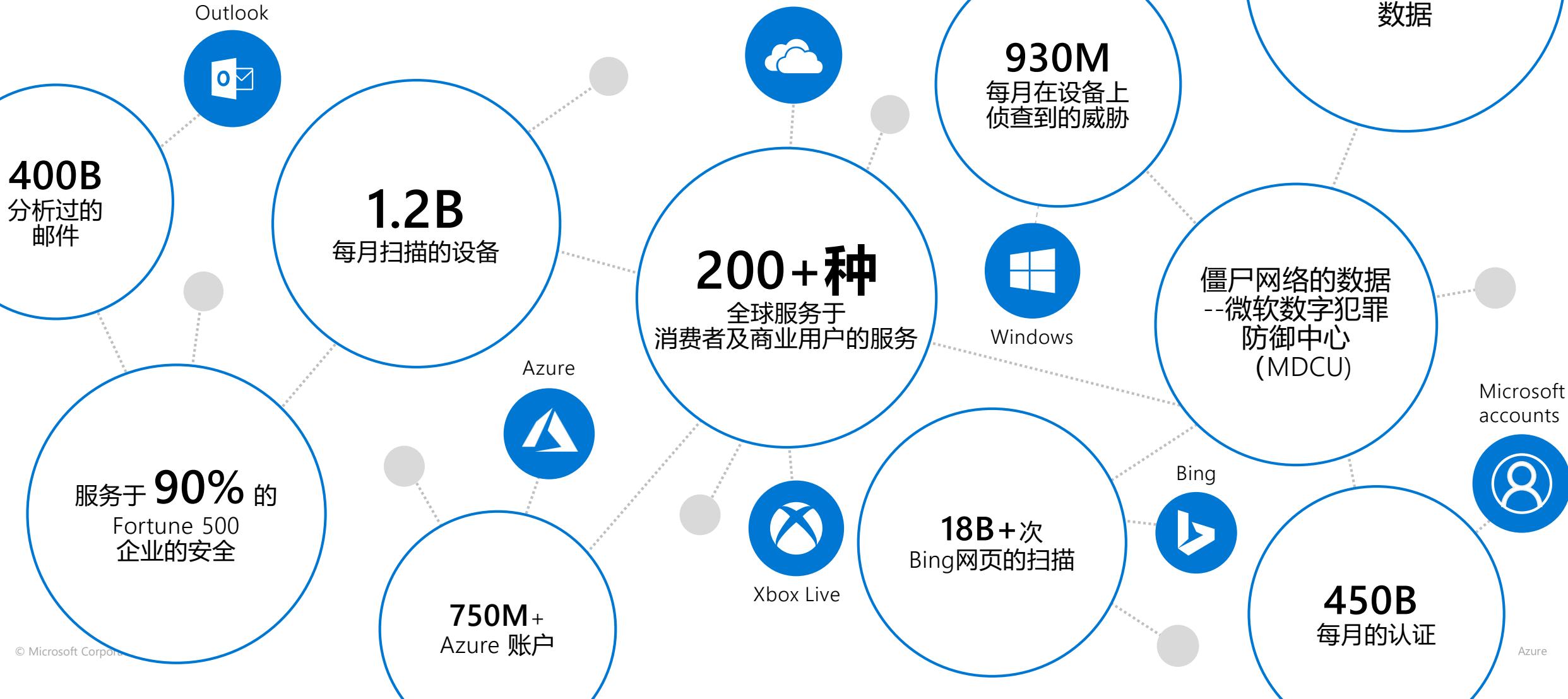
万亿各种信号,获得独特的智能

操作
安全的基础和智能



微软智能安全图

通过数万亿的信号提供的独特的见解





Collecting cybersecurity data across Microsoft's global sensors



每月扫描350 +
的邮件
每日跟踪
600,000发送垃
圾邮件的地址



超过2.5亿
全球
Windows
Defender
用户



保护全球数百万
消费者
删除全世界每年
数十亿恶意软件



数百万的电脑
受到微软企业级
防病毒解决方案
的保护



超过4.2亿
活动用户



每月有来自7亿
计算机的报告
自2005年来超过
四百亿次执行操
作



每月扫描
180亿+
网页



1 billion 个人及
企业消费者
200+ 云服务

微软威胁情报系统

威胁数据源和分析工具



基于安全感知和端点数据构建的下一代分析

按IoC (indicators of compromise) 汇编的下一代威胁情报

通过大数据和机器学习驱动，增强的关联性



This is your security team.

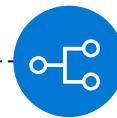
Azure提供全面的安全服务



身份认证&管理



数据保护



网络安全



威胁防护



安全管理

Azure Active Directory

Encryption
(Disks, Storage, SQL)

VNET, VPN, NSG

Azure Sentinel

Multi-Factor
Authentication

Azure Key Vault

Application Gateway
(WAF), Azure Firewall

Microsoft Antimalware
for Azure

Azure Log Analytics

Role Based Access
Control

Confidential
Computing

DDoS Protection
Standard

Threat Protection

Azure Security Center

Azure Active Directory
(Identity Protection)

Information
Protection

ExpressRoute

+ Partner Solutions

Azure 安全中心



加强安全防御系统

云安全状态管理

安全分数

策略和合规性



防范威胁

本地
服务器

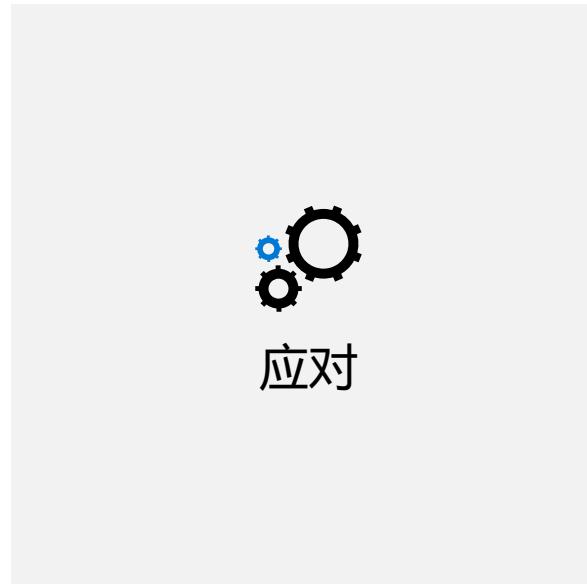
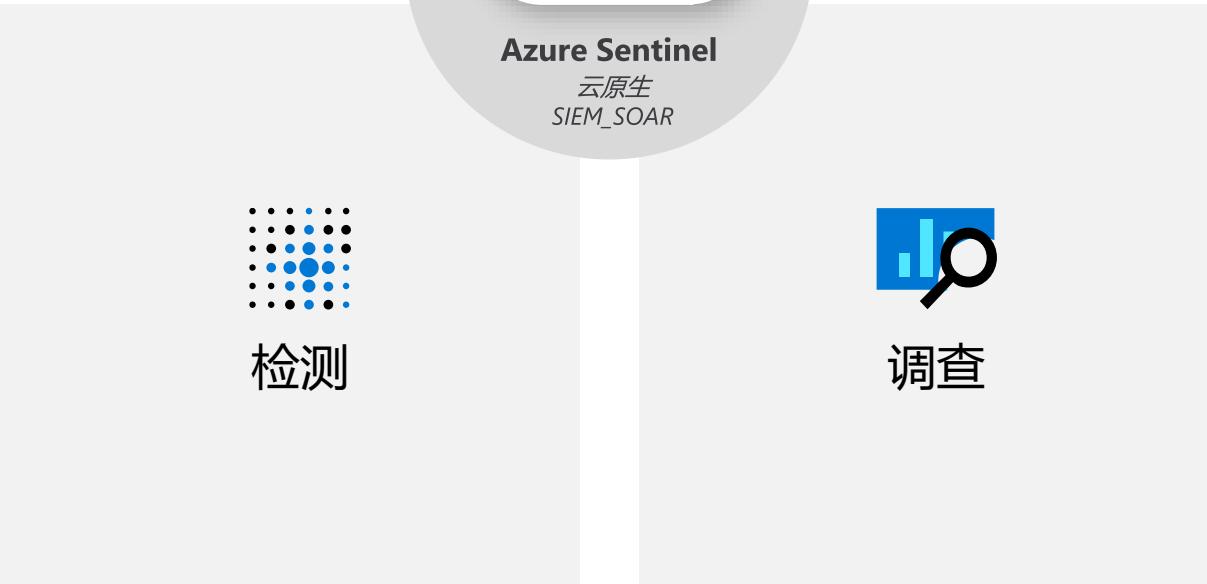
云原生工作负载

数据库
及存储



更快地获得安全

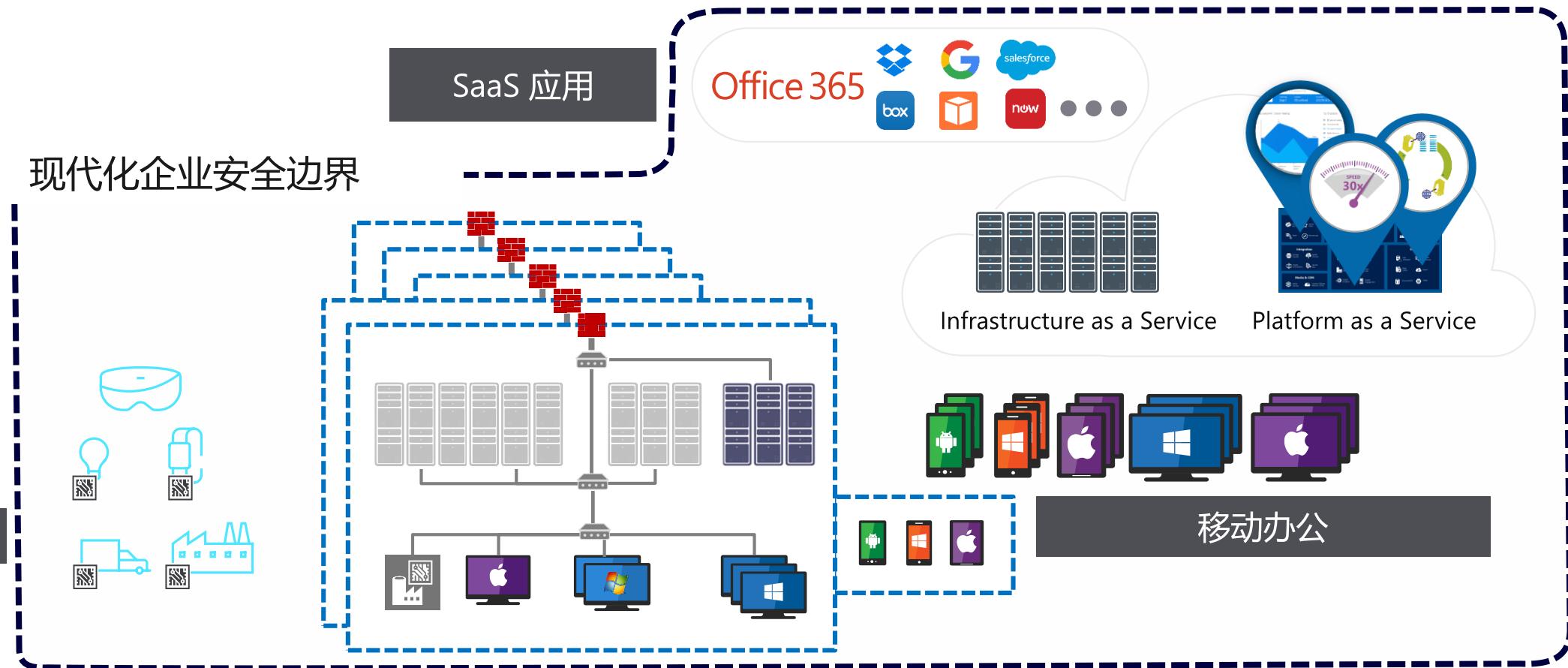
Azure Sentinel



企业一直在不断地变化

需要一个紧跟企业变化的**身份边界**

公有云的技术



如何定义企业安全边界?



Users

101010
010101
101010

Data leaks

customers



Apps



Stolen credentials



Data

Business partners



Lost device



Compromised identity

Employees



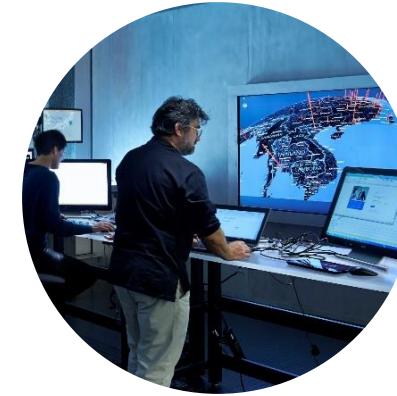
Devices



身份认证驱动安全



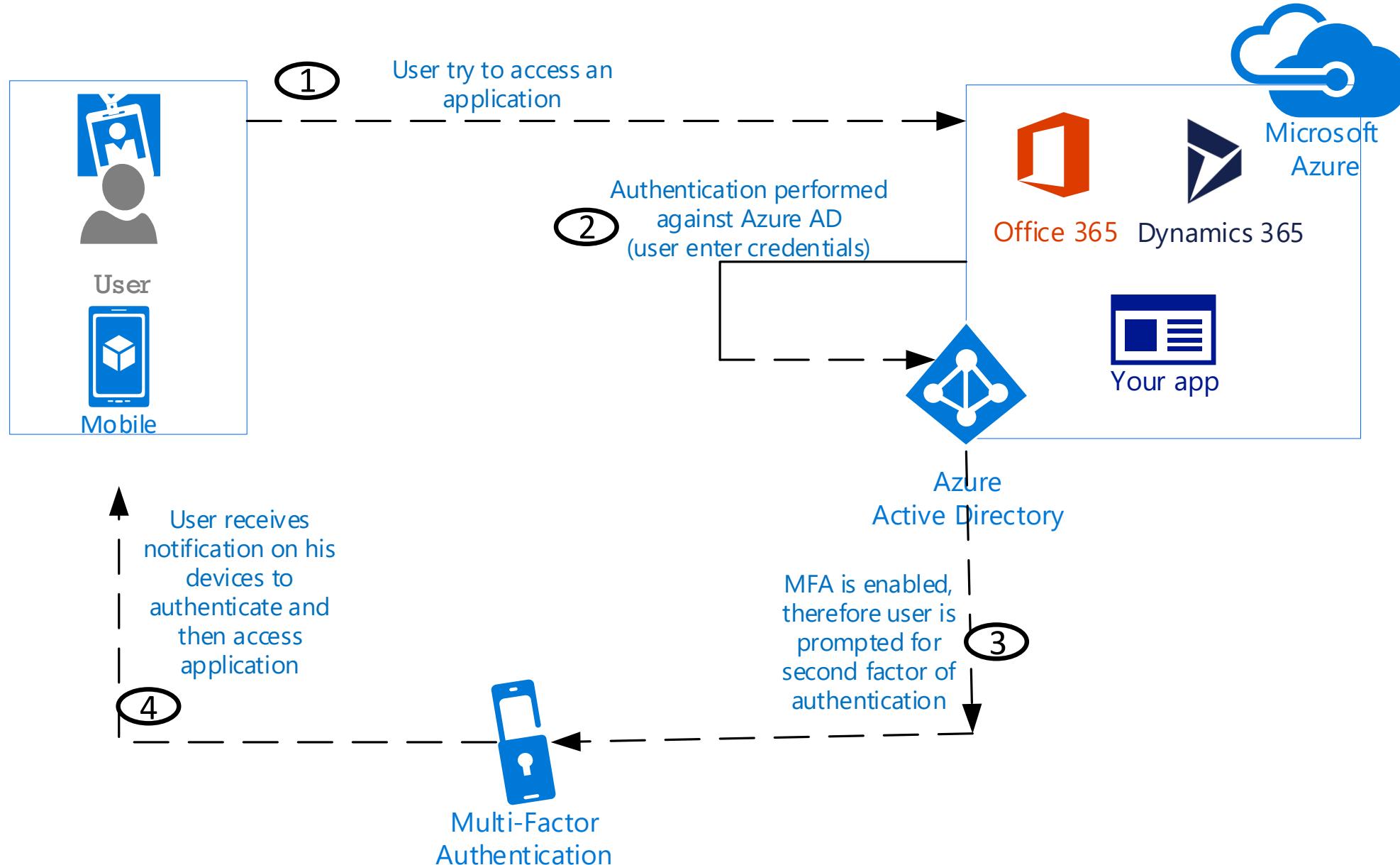
移动设备管理



威胁监测及防护

Microsoft 企业级移动+ 安全性

Azure 活动目录 & 多因子认证



单点登录

身份认证是新的安全面板



Q&A

我就是家小公司，别人为什么要攻击我？



- 每一台服务器和每一份数据在黑市上都是明码标价的，多少算力多少钱，什么样的数据什么样的价格。
- 别人攻击你并不是针对你，降维打击，不关心被攻击的企业是什么，企业用AI，攻击者也用AI。
- 攻击者也有Marketplace，丰富的攻击工具供购买以及按订阅的模式付费使用。我们有IaaS, PaaS, SaaS, 他们有RaaS。

用了云端的产品，不应该是云厂商来保证安全吗？



攻击有来自外部的攻击（端口扫描），也有来自内部的攻击（员工凭据泄露），企业需要有一套更先进的企业防护边界，保证任何可疑行为可以被监控到。

需要根据企业业务特性，制定自定义的行为告警模型

我已经用了第三方杀毒软件为什么还要用你们的？



- Palo Alto, 赛门特克, 杀毒软件都是被动防御的方式, 如何进行主动防御, 再没有被攻击的时候就能检测到异常和潜在威胁
- 在多云场景下, 通过Azure Sentinel可以应用一套统一的监控逻辑, 对可疑行为进行监控报警。

做安全的产出是什么？怎么给领导汇报？

The screenshot displays the Microsoft Security Center - Overview dashboard. On the left, a navigation sidebar lists categories such as Home, Security Center - Overview, General, Policy & Compliance, Resource Security Hygiene, Threat Protection, Automation & Orchestration, and Advanced Cloud Defense. The main content area is divided into several sections:

- Subscriptions**: Shows Subscription coverage (7 total, 1 covered standard, 6 covered free, 0 not covered), 278 covered resources, Overall compliance (13%), Least compliant subscriptions (Contoso IT - demo, Contoso IT - Retail - Prod), and a chart of Policy compliance over time.
- Resource security hygiene**: Features a Secure score of 607 of 1.3K, 46 active recommendations, and a pie chart showing 607 SCORE across Compute & apps, Data & storage, Networking, and Identity & access.
- Threat protection**: Shows Security alerts by severity (High: 0, Medium: 21, Low: 1) and 22 total attacked resources.
- Resource health monitoring**: Displays secure scores for Compute & apps (152), Data & storage (69), Networking (56), and Identity & access (1).
- Highest secure score impact recommendations**: Lists three items: Enable MFA for accounts with write permissions (+40), Remediate endpoint protection health (-40), and Remediate vulnerabilities in container images (+35).

Key Metrics from the Dashboard:

- Subscription coverage:** 7 total, 1 covered standard, 6 covered free, 0 not covered.
- Overall compliance:** 13%.
- Secure score:** 607 of 1.3K.
- Active recommendations:** 46.
- Threat protection:** 22 total attacked resources.
- Resource health monitoring:** Compute & apps (152), Data & storage (69), Networking (56), Identity & access (1).
- Highest secure score impact recommendations:**
 - Enable MFA for accounts with write permissions (+40)
 - Remediate endpoint protection health (-40)
 - Remediate vulnerabilities in container images (+35)

- 微软提供不同维度的安全分数(从合规, 从云端环境评测等), 能够量化实施团队的贡献