Microsoft

Microsoft Online Tech Forum

云平台安全响应机制

陈健宁 陈彬彬
微软全球技术支持中心

内容安排

1 云平台安全和应急响应

2 云平台安全响应利器和最佳实践

Microsoft

云平台安全和应急响应

更廉价的攻击

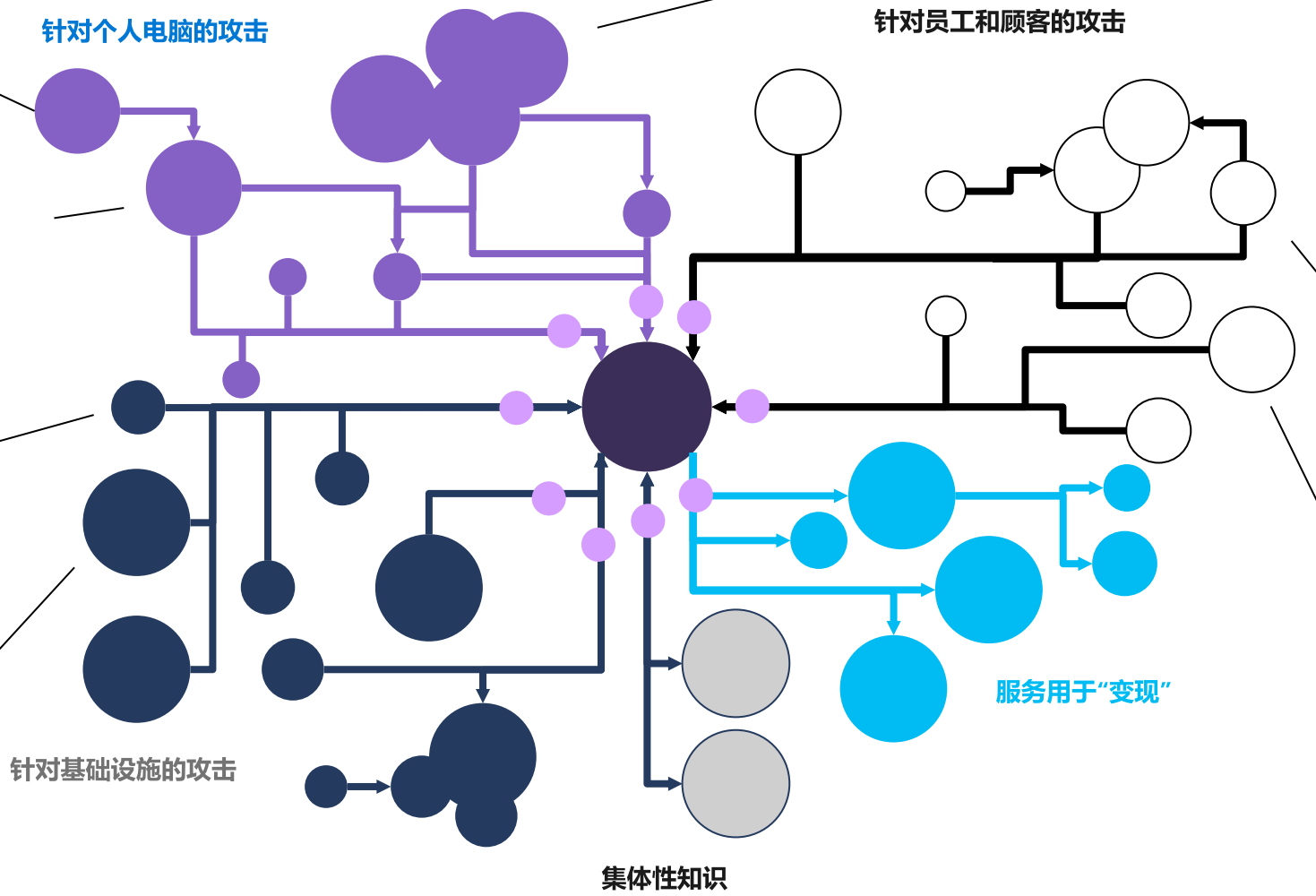
勒索软件:
预付$66 或者30% 的盈利

0days 价格从$5,000
到 $350,000

负载(受控设备)
平均价格区间
- **PC** - $0.13 到 $0.89
- **移动端** - $0.82 到 $2.78

拒绝服务 (DOS)
平均价格
每天: $102.05
每周: $327.00
每月: $766.67

用于遮掩IP地理位置的**代理**
服务价格
100,000个最低每周$100

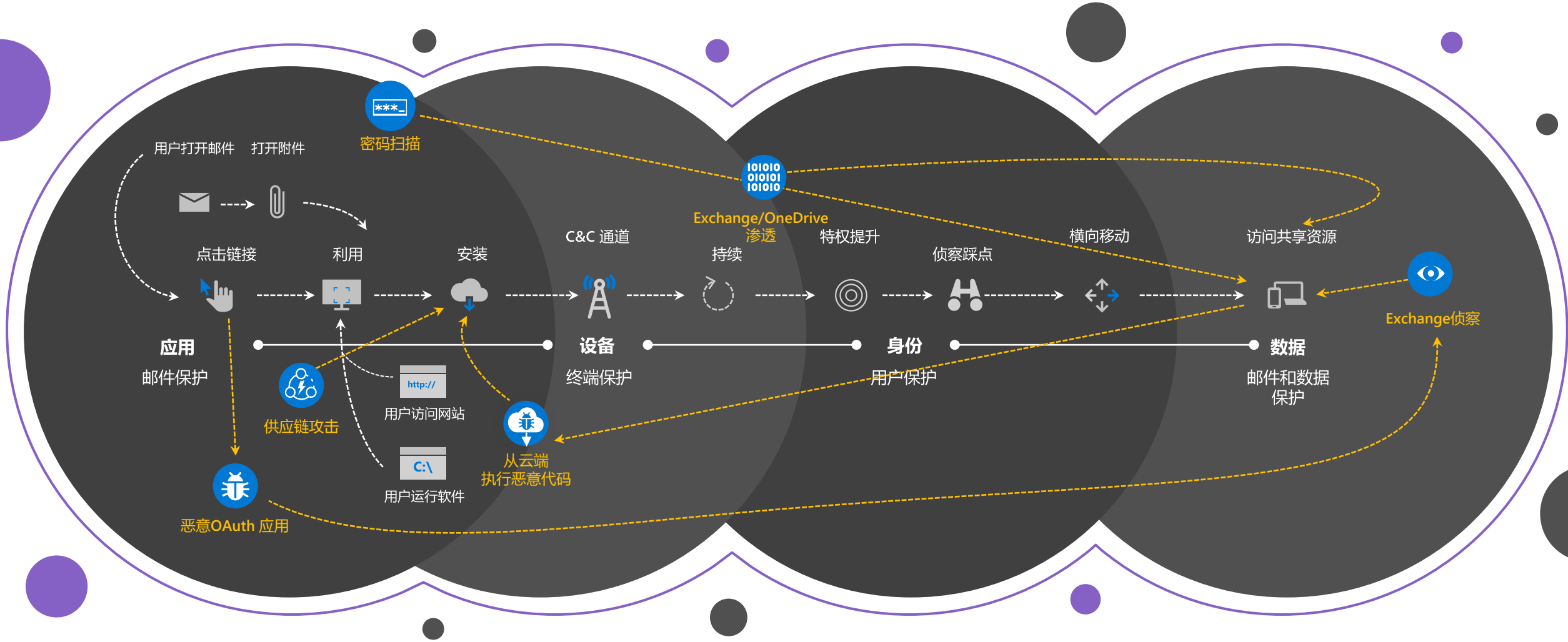


鱼叉式钓鱼
每成功一个账号收取
$100 到 $1,000 不等

破解的账号
最低4亿只需$150
平均 $0.97每千个.

现代化攻击链在不断演进

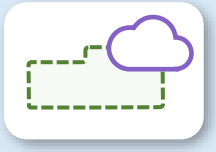
综合性攻击被完全用于云端或影响混合环境



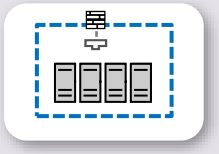
共享责任和策略要点

责任	SaaS	PaaS	IaaS	On-prem
信息和数据	用户	用户	用户	用户
设备 (移动终端和个人电脑)	用户	用户	用户	用户
账户和身份	用户	用户	用户	用户
身份和域基础设施	用户	用户	用户	用户
应用	微软	用户	用户	用户
网络控制	微软	用户	用户	用户
操作系统	微软	微软	用户	用户
物理主机	微软	微软	微软	用户
物理网络	微软	微软	微软	用户
物理数据中心	微软	微软	微软	用户

微软　用户



建立现代化的边界

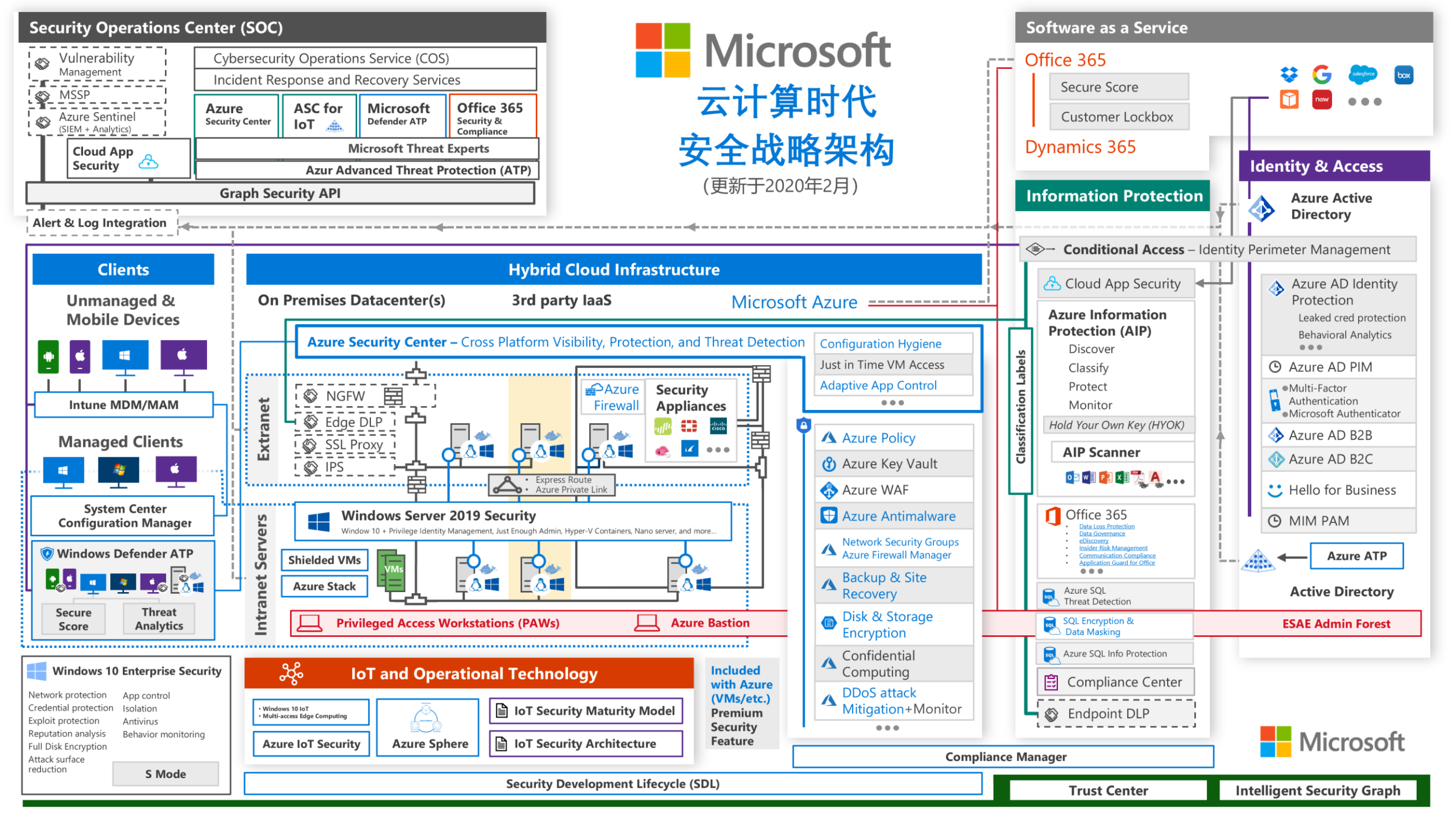


现代化基础设施安全

“信任但确认”每一个云提供商

云平台安全响应

- 启用多因素认证（MFA），阻止99.9%针对身份的攻击
- 在构建生产环境同时设计启用安全特性
  - Secure Score
  - 启用并保存日志，定期备份日志
- 关注官方公开信息并采取行动 （https://aka.ms/SUG）
- 云平台安全应急响应
  - 报告资源滥用、报告钓鱼邮件 （https://cert.Microsoft.com）
  - 冷静分析追踪，补足短板


Security Operations Center (SOC)
Vulnerability Management
MSSP
Azure Sentinel (SIEM + Analytics)
Cloud App Security
Cybersecurity Operations Service (COS)
Incident Response and Recovery Services
Azure Security Center
ASC for IoT
Microsoft Defender ATP
Office 365 Security & Compliance
Microsoft Threat Experts
Azur Advanced Threat Protection (ATP)
Graph Security API
Alert & Log Integration
Microsoft
云计算时代
安全战略架构
(更新于2020年2月)
Software as a Service
Office 365
Secure Score
Customer Lockbox
Dynamics 365
Identity & Access
Azure Active Directory
Conditional Access – Identity Perimeter Management
Information Protection
Clients
Unmanaged & Mobile Devices
Intune MDM/MAM
Managed Clients
System Center Configuration Manager
Windows Defender ATP
Secure Score
Threat Analytics
Hybrid Cloud Infrastructure
On Premises Datacenter(s)
3rd party IaaS
Microsoft Azure
Azure Security Center – Cross Platform Visibility, Protection, and Threat Detection
Extranet
NGFW
Edge DLP
SSL Proxy
IPS
Azure Firewall
Security Appliances
Express Route
Azure Private Link
Intranet Servers
Windows Server 2019 Security
Window 10 + Privilege Identity Management, Just Enough Admin, Hyper-V Containers, Nano server, and more...
Shielded VMs
Azure Stack
VMs
Privileged Access Workstations (PAWs)
Azure Bastion
Configuration Hygiene
Just in Time VM Access
Adaptive App Control
Azure Policy
Azure Key Vault
Azure WAF
Azure Antimalware
Network Security Groups
Azure Firewall Manager
Backup & Site Recovery
Disk & Storage Encryption
Confidential Computing
DDoS attack Mitigation+Monitor
Classification Labels
Cloud App Security
Azure Information Protection (AIP)
Discover
Classify
Protect
Monitor
Hold Your Own Key (HYOK)
AIP Scanner
Office 365
Data Loss Protection
Data Governance
eDiscovery
Insider Risk Management
Communication Compliance
Application Guard for Office
Azure SQL Threat Detection
SQL Encryption & Data Masking
Azure SQL Info Protection
Compliance Center
Endpoint DLP
Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
Azure AD PIM
Multi-Factor Authentication
Microsoft Authenticator
Azure AD B2B
Azure AD B2C
Hello for Business
MIM PAM
Azure ATP
Active Directory
ESAE Admin Forest
Windows 10 Enterprise Security
Network protection
Credential protection
Exploit protection
Reputation analysis
Full Disk Encryption
Attack surface reduction
App control
Isolation
Antivirus
Behavior monitoring
S Mode
IoT and Operational Technology
Windows 10 IoT
Multi-access Edge Computing
Azure IoT Security
Azure Sphere
IoT Security Maturity Model
IoT Security Architecture
Included with Azure (VMs/etc.) Premium Security Feature
Compliance Manager
Security Development Lifecycle (SDL)
Trust Center
Intelligent Security Graph
Microsoft

Microsoft

云平台安全响应利器和最佳实践

ASC, MDATP, AAD, Azure Sentinel

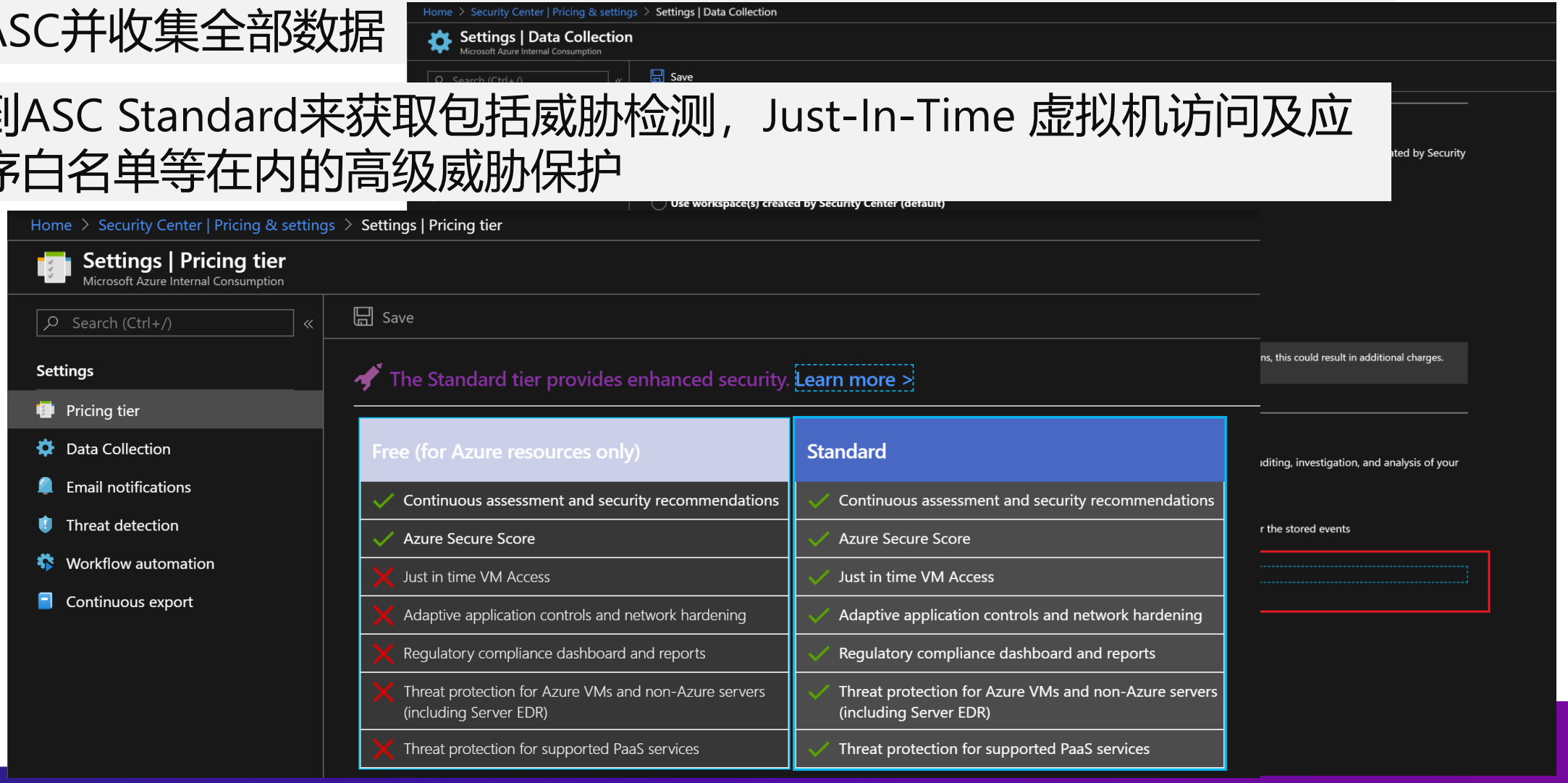
Azure Security Center 提供的解决方案

- ✓ 持续评估云端和本地环境安全态势
- ✓ 结合行业和监管标准，确保安全合规性
- ✓ 采用网络访问控制及应用控制来阻拦恶意行为
- ✓ 在漏洞被利用前检测系统和应用带来的安全漏洞
- ✓ 采用高级分析及威胁情报快速检测威胁
- ✓ 对威胁简单而高效的调查

Azure Security Center 最佳实践（1）

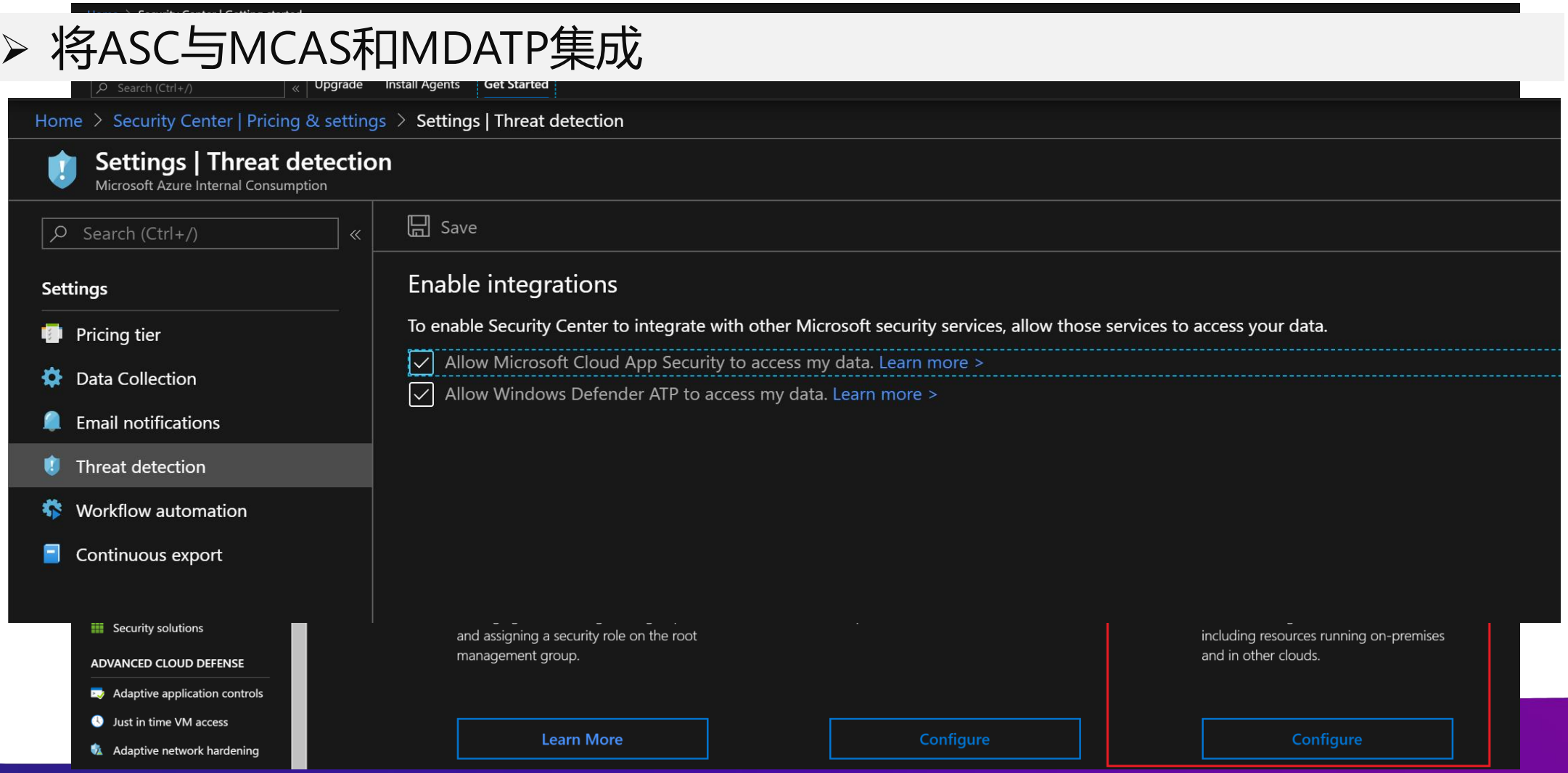
微软建议您采取以下行动保护Azure云端及本地负载

- 启用ASC并收集全部数据
- 升级到ASC Standard来获取包括威胁检测，Just-In-Time 虚拟机访问及应用程序白名单等在内的高级威胁保护



Azure Security Center 最佳实践（2）

- 将ASC扩展到本地及其他云平台上的负载
- 将ASC与MCAS和MDATP集成



ASC 案例

- 管理员发现某个月Azure的账单中出现大量的对外流量的费用

Row Labels	Sum of Updated Cost
A2m v2	156.0300109
Azure VM and on-premises Server Protected Instances	18.68
Batch Write Operations	0.00060067
D1 v2/DS1 v2	87.43998735
Data Transfer In	0
Data Transfer Out	3325.317341

- 通过ASC发现大量来自Internet的到389端口访问的报警，初步判断为基于LDAP网络放大的DDOS攻击

```
{
 "resourceType": "Virtual Machine",
 "Attacker IP": "199.59.x.x",
 "Victim IP": “x.x.x.x",
 "Attacker Port": "15796",
 "Victim Port": "389"
}
```

- 发现虚拟机没有使用NSG进行访问控制，导致了安全漏洞。此前，ASC已经给出加固NSG及JIT的建议

MDATP 提供的解决方案

威胁和漏洞管理 Threat & Vulnerability Management

减少攻击面 Attack surface reduction

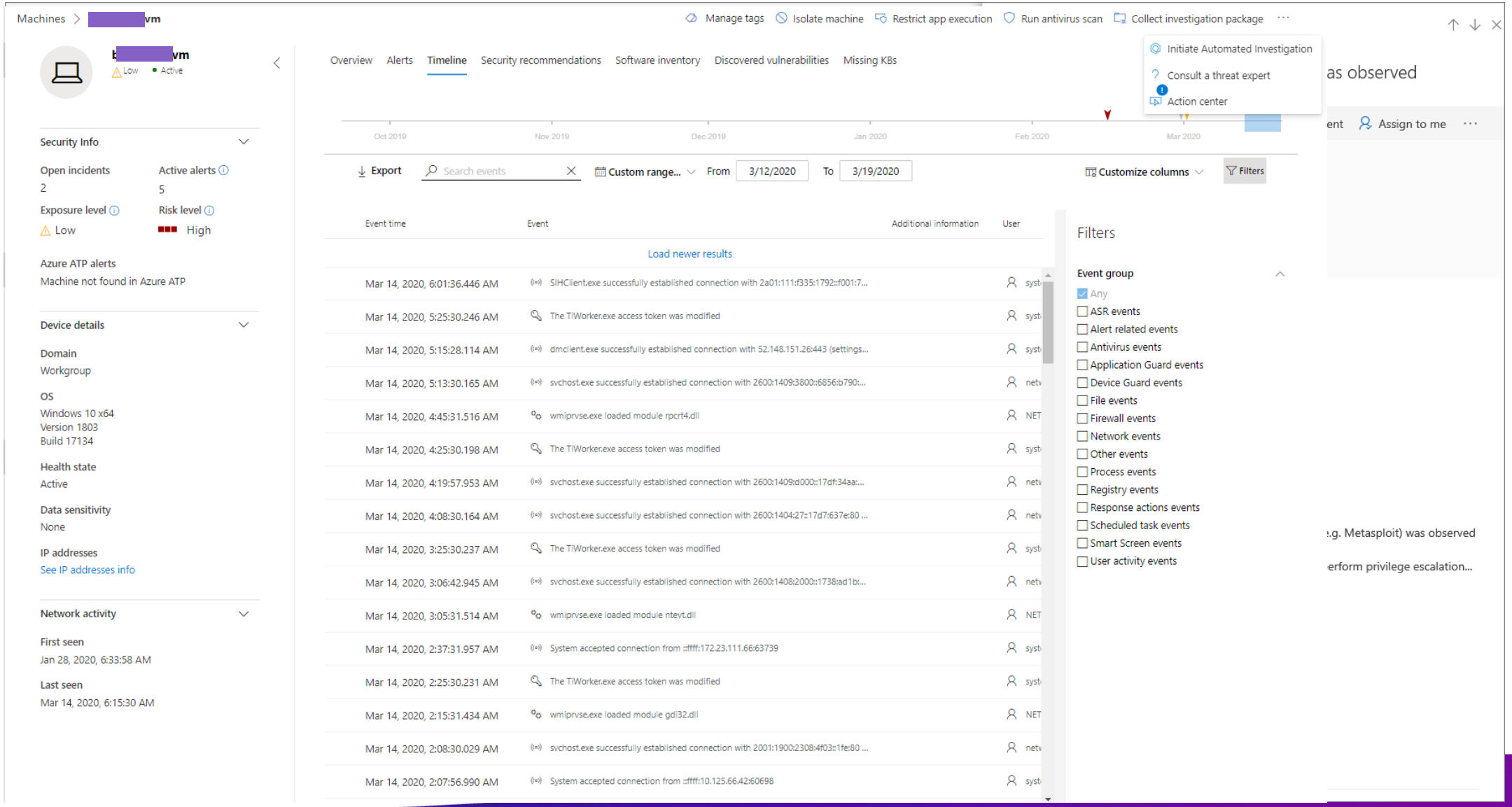
下一代保护 Next generation protection

终端检测和响应 Endpoint detection and response

自动化分析和修复 Automated investigation and remediation

微软威胁专家 Microsoft Threat Experts

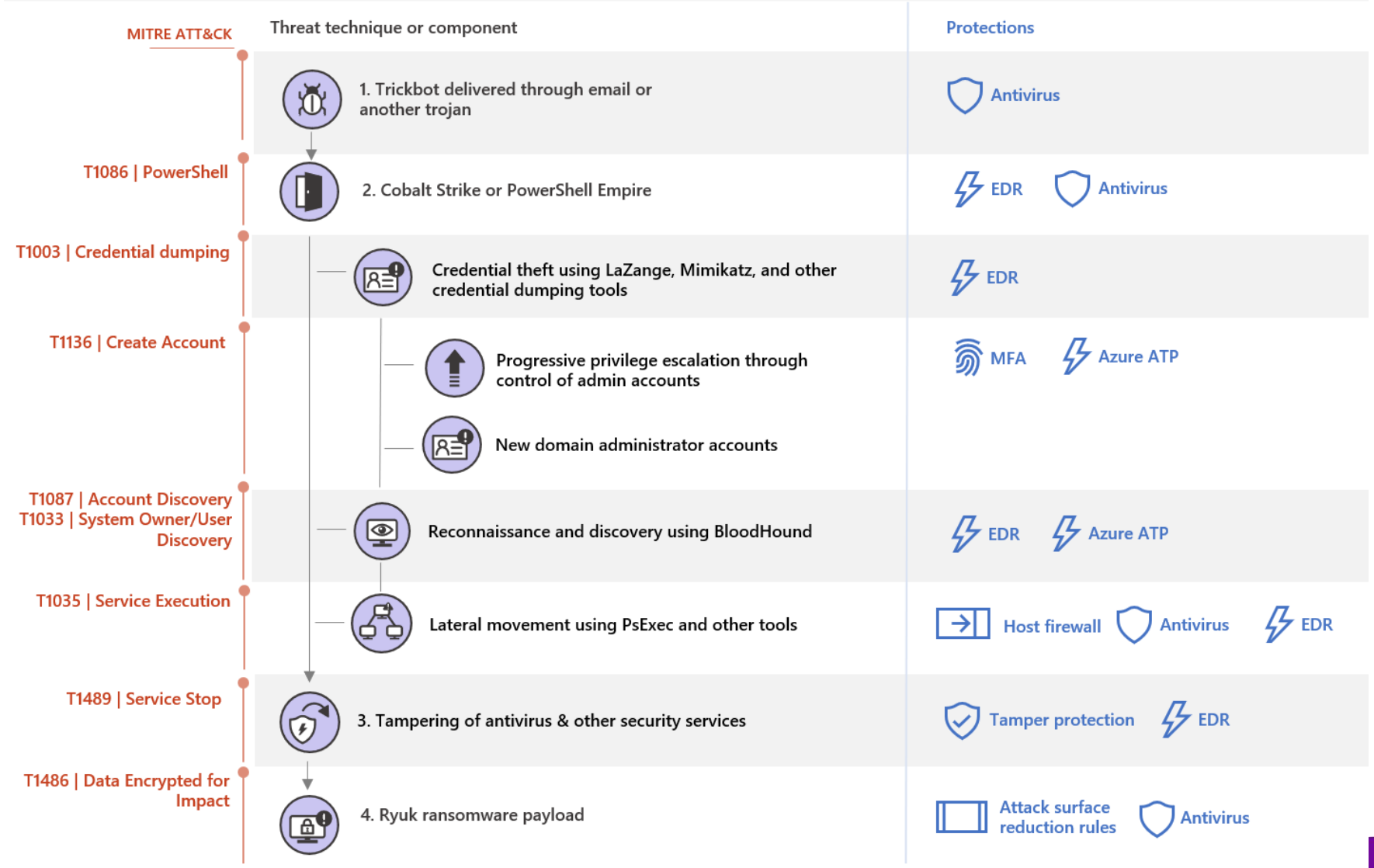
MDATP 管理员面板


Machines > [redacted]vm
Manage tags
Isolate machine
Restrict app execution
Run antivirus scan
Collect investigation package
Initiate Automated Investigation
Consult a threat expert
Action center
Low
Active
Overview
Alerts
Timeline
Security recommendations
Software inventory
Discovered vulnerabilities
Missing KBs
as observed
Assign to me
Oct 2019
Nov 2019
Dec 2019
Jan 2020
Feb 2020
Mar 2020
Export
Search events
Custom range...
From 3/12/2020
To 3/19/2020
Customize columns
Filters
Security Info
Open incidents
2
Active alerts
5
Exposure level
Low
Risk level
High
Azure ATP alerts
Machine not found in Azure ATP
Device details
Domain
Workgroup
OS
Windows 10 x64
Version 1803
Build 17134
Health state
Active
Data sensitivity
None
IP addresses
See IP addresses info
Network activity
First seen
Jan 28, 2020, 6:33:58 AM
Last seen
Mar 14, 2020, 6:15:30 AM
Event time
Event
Additional information
User
Load newer results
Mar 14, 2020, 6:01:36.446 AM SIHClient.exe successfully established connection with 2a01:111:f335:1792::f001:7...
Mar 14, 2020, 5:25:30.246 AM The TiWorker.exe access token was modified
Mar 14, 2020, 5:15:28.114 AM dmclient.exe successfully established connection with 52.148.151.26:443 (settings...
Mar 14, 2020, 5:13:30.165 AM svchost.exe successfully established connection with 2600:1409:3800::6856:b790:...
Mar 14, 2020, 4:45:31.516 AM wmiprvse.exe loaded module rpcrt4.dll
Mar 14, 2020, 4:25:30.198 AM The TiWorker.exe access token was modified
Mar 14, 2020, 4:19:57.953 AM svchost.exe successfully established connection with 2600:1409:d000::17df:34aa:...
Mar 14, 2020, 4:08:30.164 AM svchost.exe successfully established connection with 2600:1404:27::17d7:637e:80 ...
Mar 14, 2020, 3:25:30.237 AM The TiWorker.exe access token was modified
Mar 14, 2020, 3:06:42.945 AM svchost.exe successfully established connection with 2600:1408:2000::1738:ad1b:...
Mar 14, 2020, 3:05:31.514 AM wmiprvse.exe loaded module ntevt.dll
Mar 14, 2020, 2:37:31.957 AM System accepted connection from ::ffff:172.23.111.66:63739
Mar 14, 2020, 2:25:30.231 AM The TiWorker.exe access token was modified
Mar 14, 2020, 2:15:31.434 AM wmiprvse.exe loaded module gdi32.dll
Mar 14, 2020, 2:08:30.029 AM svchost.exe successfully established connection with 2001:1900:2308:4f03::1fe:80 ...
Mar 14, 2020, 2:07:56.990 AM System accepted connection from ::ffff:10.125.66.42:60698
Filters
Event group
Any
ASR events
Alert related events
Antivirus events
Application Guard events
Device Guard events
File events
Firewall events
Network events
Other events
Process events
Registry events
Response actions events
Scheduled task events
Smart Screen events
User activity events
.g. Metasploit) was observed
erform privilege escalation...

使用MDATP响应安全事件

- 监控Alert queue和Incident queue
- 实施响应行动
  - 开启自动调查
  - 将机器从网络中隔离
  - 限制只运行特定的应用
  - 收取调查日志包
  - 运行杀毒软件扫描
  - 开启实时响应会话
  - 利用Machine timeline检查报警发生时间点附近的行为
  - 查看机器文件信息，是否签名，是否被威胁情报所检测
  - 收集文件或隔离文件
- 通过Advanced hunting功能调查其它信息

案例——Ryuk勒索软件攻击链检测



案例——Advanced Hunting

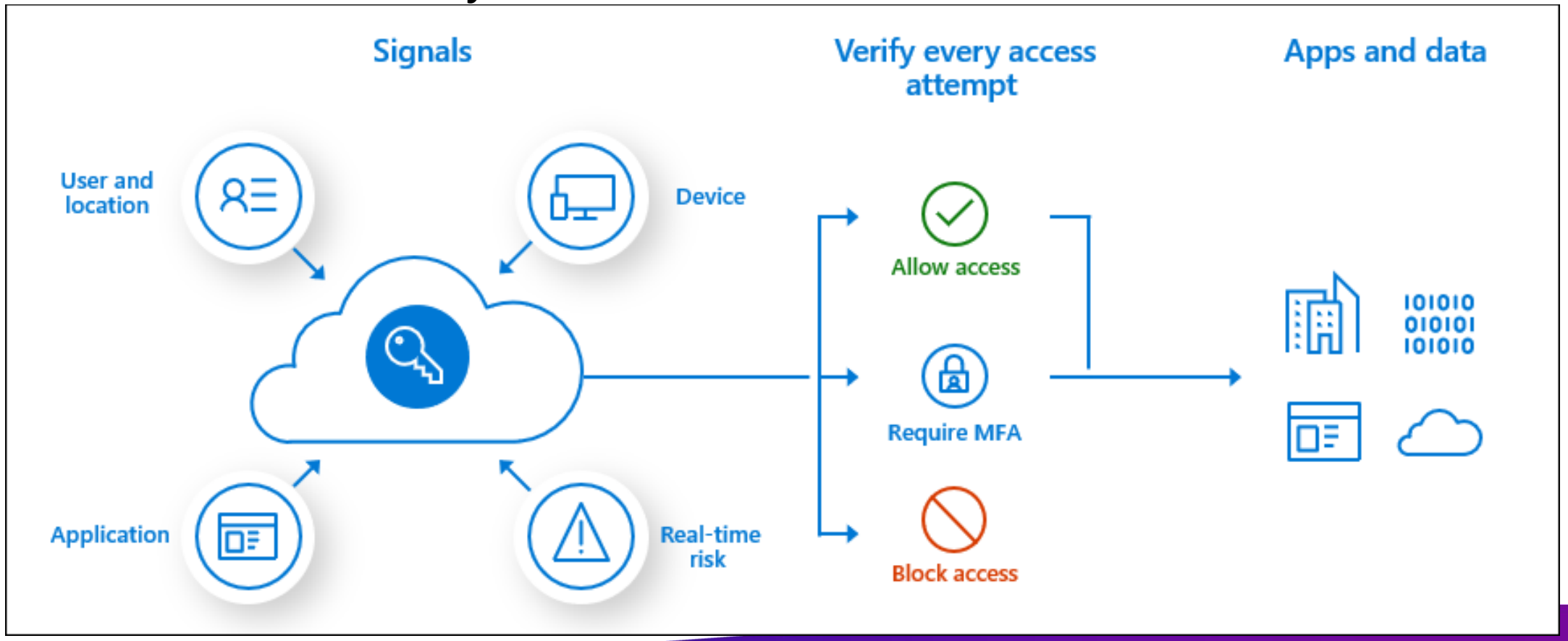
查看由WMI Provider 进程生成的命令行中带有base64编码的字符串的PowerShell进程：

```
// Find use of Base64 encoded PowerShell
// Indicating possible Cobalt Strike
DeviceProcessEvents
| where Timestamp > ago(7d)

| where InitiatingProcessFileName =~ 'wmiprvse.exe’

| where FileName =~ 'powershell.exe'
 and (ProcessCommandLine hasprefix '-e' or  ProcessCommandLine contains 'frombase64')

| where ProcessCommandLine matches regex '[A-Za-z0-9+/]{50,}[=]{0,2}’

| project DeviceId, Timestamp, InitiatingProcessId,
InitiatingProcessFileName, ProcessId, FileName, ProcessCommandLine
```

AAD保护身份，检测异常

常见攻击场景：
攻击者获取特定账户身份信息后登录Azure创建性能强大的虚拟机进行挖矿行为，造成用户收到高额账单

Conditional Access 及 Identify Protection



AAD身份信息保护最佳实践

- 利用Conditional Access
  - 对管理角色用户进行多因素认证
  - 对所有用户进行多因素认证
  - 对Azure的管理访问（Azure portal, Azure PowerShell, Azure CLI）登陆进行多因素认证
  - 禁用传统认证协议
  - 结合AAD Identity Protection，对高风险用户强制密码重置，对中风险及以上用户要求多因素认证
  - 对访问发起的地点进行限制
  - 只允许特定客户端访问特定服务
  - 对设备合规性进行要求
- 利用Identity Protection：
  - 设置MFA策略
  - 设置风险策略对风险采取控制
    - 风险用户
    - 风险登录
- 确保AAD 登录日志的保存期限符合安全审计及响应策略

案例——AAD身份信息保护

3/10/2020: 安全人员发现某台Azure虚拟机被异常开启，机器没有NSG网络安全组保护，暴露给Internet后遭遇攻击

我们调查发现2020年第一次开机请求是通过用户A的Azure Portal应用发起，发起时间为1/22

此后在3/5，3/6，3/7 又由相同账号通过Azure Portal发起另外三次开机请求

利用AAD 登录日志发现了3/5，3/6，3/7的登录来源于合理的IP，并确认由用户A发起

由于1/22的登录日志已经被冲涮掉，无法获取1/22登录的具体原因和源头IP地址

客户重置用户A密码，开启Conditional Access策略要求MFA并结合Identity Protection进行更好的风险检测

安全人员面临的挑战

威胁的复杂性

本地IT部署及维护

76%
机构的安全数据持续增加

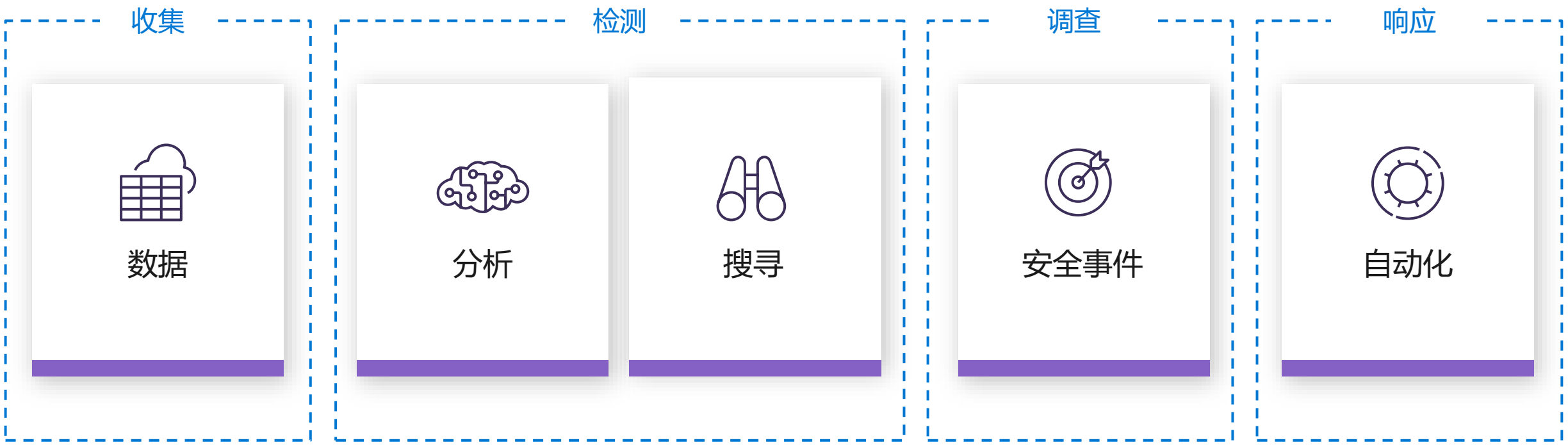
44%
的报警从没被分析

太多不相关的安全产品

3.5M
的安全人员缺口

缺乏自动化

Azure Sentinel 点对点的安全解决方案



小结

- 安全事件的响应离不开良好的风险评估，保护和检测基础架构
- 微软在Azure云平台上提供了深层防御模型下的安全解决方案
- 云平台是一个责任共享平台

Azure Security Center
https://docs.microsoft.com/en-us/azure/security-center/
Microsoft Defender ATP
https://docs.microsoft.com/en-us/windows/security/threat-protection/
AAD Conditional Access
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/
Azure Sentinel
https://docs.microsoft.com/en-us/azure/sentinel/

答疑环节

Microsoft

Thank you