2020北京网络安全大会

2020 BEIJING CYBER SECURITY CONFERENCE

零信任｜从理论模型到实践落地

Zero Trust: From Theoretical Model to Practical Landing

演讲人：李雨航 Yale Li

云安全联盟大中华区主席兼研究院院长

道路起点：零信任落地是企业一把手工程，不是购买产品服务

安全理念

- 永不信任，始终验证
- 网络环境无时无刻不危险
- 网络内部外部时时受到威胁
- 网络位置无法决定可信度
- 所有人/物/网流均需认证授权多源动态智能安全策略

安全战略

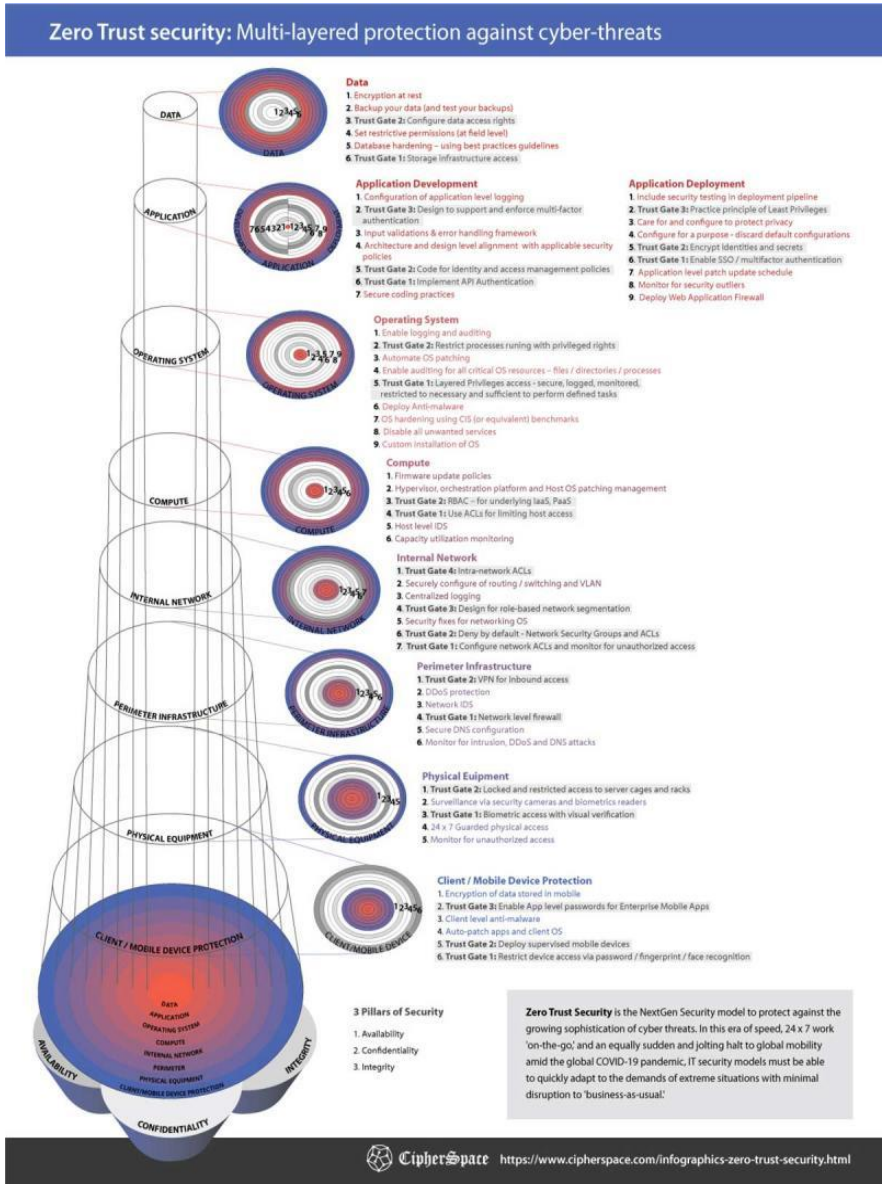
- 领导团队自上而下推动与引导
- 管理能力与技术能力双驱动
- 战略高于单一产品
- 咨询赋能发挥优势

安全架构

- NIST ZTA 零信任参考架构
- 零信任IAM身份访问管理
- SDP软件定义边界
- MSG微隔离

零信任在全球被全面拥抱；甲方、乙方、中立机构一起大规模落地实施；中国工信部确定零信任为安全关键技术

道路目标 -- 记住你的北斗七星“1个理念，5项原则，1个含义”



1个理念

永不信任 始终验证

5项原则

A B C D E

- **A**ssume nothing 不做任何假定
- **B**elieve nobody 不信任何人员
- **C**heck everything all the time 随时检查一切
- **D**efeat Dynamic threats/risks 防范动态威胁
- **E**xpect and prepare for the worst 做好最坏打算

1个含义

零信任不是零访问，而是更安全访问被防护的资源

企业零信任之旅的六大收获

● 降低风险

强化资产的发现，任何应用与服务都会被识别并给予身份，对敏感信息的攻击途径会被分析，数据流图使网络的透明度增加

● 降低成本

将保护目标聚焦到负载与数据，通过策略与控制排除不需要访问资源的用户/设备/应用，恶意行为被限制，大大降低安全事件数量，企业有更多时间与资源来迅速恢复少数的安全事件，降低业务成本

● 业务敏捷

摈弃了静态边界防御的慢速与不方便的检查，安全不再是业务的绊脚石，使业务能更快上线，用户的安全体验更好，增加了业务的速度与敏捷性

● 安全合规

使安全审计师更容易看清网络，便于审计工作并减少违规发现，其架构本身已经具有多项安全控制措施满足合规条款，包括国际与行业安全标准及中国的等级保护2.0等

● 有效控制

在公有云，混合云，多云环境下把网络通信限制在有身份被验证的负载中，防止包括云服务商管理员在内的各方向攻击

● 改善管理

对于数字化转型依赖软件与应用的组织机构，零信任能很好地支持DevOps，使应用部署适配业务优先级减低各组织部门之间的摩擦

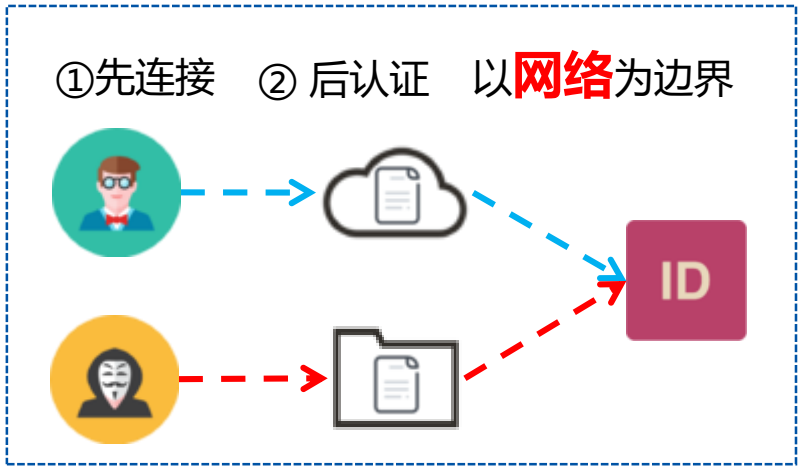

B52常规轰炸机

安全从防弹衣走向隐身衣
漏洞仍存在，但很难发现
事件仍发生，但几率变小


B2隐身轰炸机

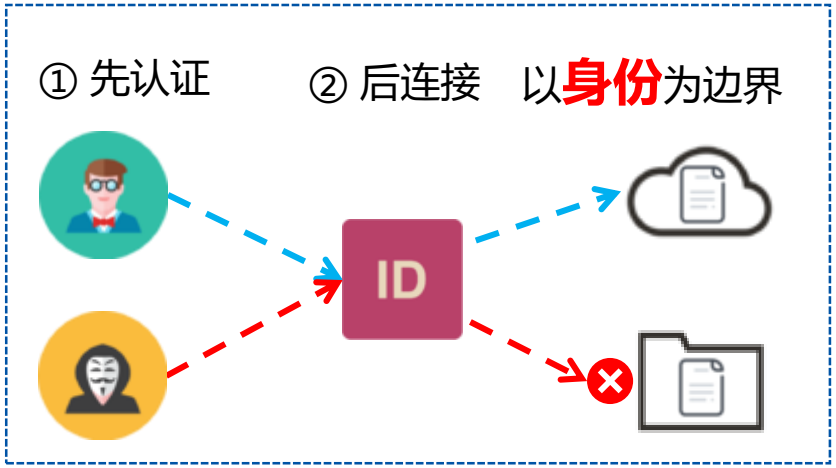
零信任战略核心 -- 以身份为边界（Identity based）

传统架构



- 通过防火墙，VPN、IDS/IPS等设备建立企业的网络边界
- 构筑基于内网位置的信任体系，认为网络内部的人员与设备是可信的

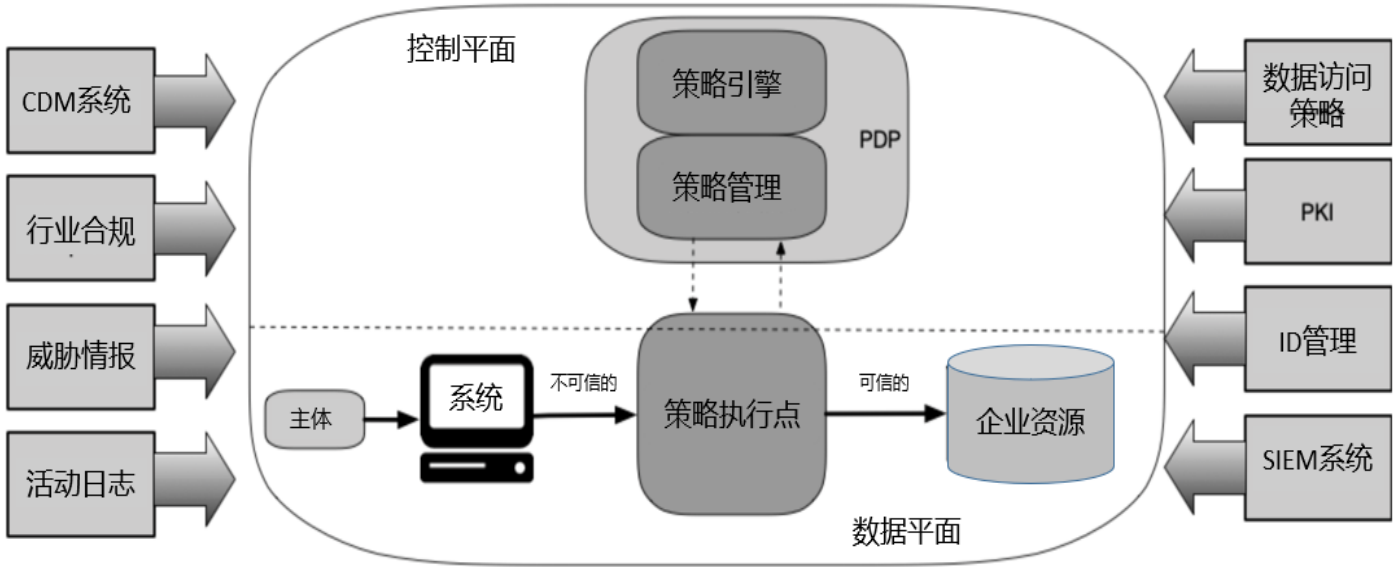
零信任架构



- 从不信任，始终验证
- 基于身份--人、设备、应用等
- 看不见、拿不走、可追溯、能销毁
- 云管端、动静用、前中后
- 防范和保护：隐身与防弹并重
- 智能化和自适应

零信任架构：1个标准（ZTA），3大技术（SIM）

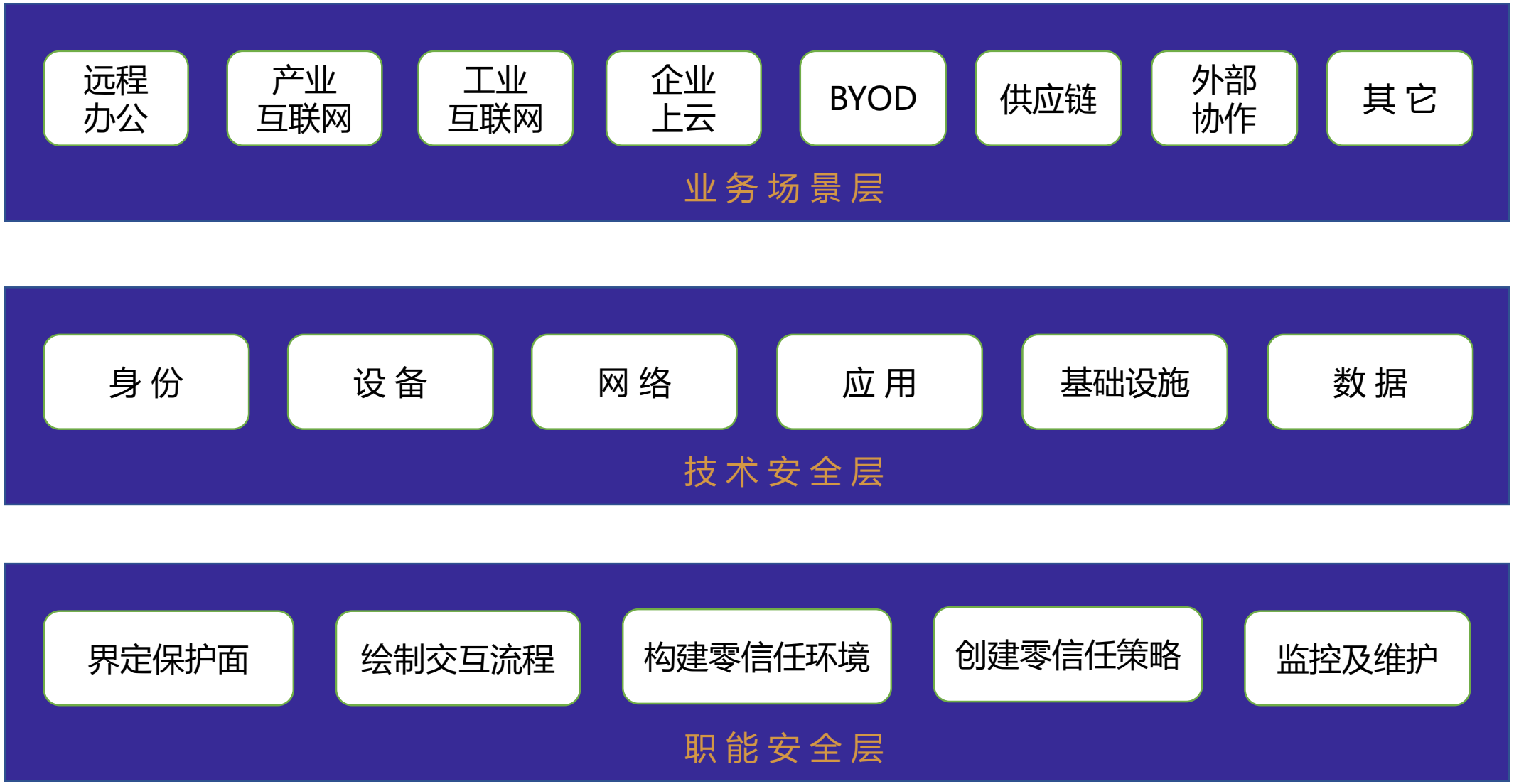
NIST SP 800-207 Zero Trust Architecture
（NIST 零信任架构草案第二版）



- 最小授权：缺省是无权
- 三个层面：数据、控制、管理
- 被保护资源：网络/数据/应用/系统/存储等
- 身份认证：支持人、设备等动态实时管理
- 防范和保护：防弹衣、双向防护
- 通信加密

SDP　ZT-IAM　MSG

CSA零信任成熟度模型框架 ZT-CMM Framework



CSA零信任战略咨询服务框架 ZT-SCS Framework

CSA授权第三方机构提供服务，框架立足客户实际业务保障需求，对安全知识进行重构与梳理，拥有系统性、战略级安全知识架构，提供综合性零信任战略咨询服务产品包，**四大服务包，十一类安全交付件。**

Ⅰ 安全评估	Ⅱ安全战略规划	Ⅲ 安全解决方案	Ⅳ 知识转移
(1) 业务场景诊断	(4) 安全SP / BP	(6) 技术路标	(9) 安全技术培训
(2) 技术安全诊断	(5) 安全效能提升	(7) RFP服务	(10) 安全意识培训
(3) 职能安全诊断		(8) 方案实施管理服务	(11) 中高级管理者安全培训

企业零信任实践之路的步骤（职能安全）

1 界定保护范围

确认保护面：关键数据/应用程序/资产/服务（DAAS）

把控件移近保护面并附上限制性的/精确的/可理解的策略声明

创建微边界或分隔微边界

2 记录业务流转

流转传输方式决定保护方式

通过获得有关DAAS相互依赖关系的上下文信息，记录特定资源的交互方式有助于加强控制并提供有价值的上下文信息，确保最佳安全环境

降低对用户和业务运营的干扰

3 构建零信任环境

以保护面为中心自定义并构建网络

根据业务需求记录流程，从下一代防火墙开始制定零信任架构

下一代防火墙充当分段网关，在保护面周围创建一个微边界。对任何尝试访问保护表面内的对象使用分段网关，强制执行附加的检查和访问控制层，一直到第七层。

4 创建零信任安全策略

创建策略确定访问流程

提前了解访问用户对象/访问的应用程序/访问原因/连接方式等，确认合适控件保护该访问

精细化实施，仅允许已知流量或合法应用程序连接

5 监视和维护

检查内外部所有日志

侧重零信任操作方面

检查记录所有流量

改进环境

案例：微软20年零信任之路-从无边界网络到零信任

Microsoft

2001
Anywhere Access/MSI
政府安全计划源代码共享基础设施

2002
微软启用 IPSec 隔离
"所有企业内部网络端到端通信都是安全的"

2004
Jericho Forum
"去网络边界化，限制基于网络的隐式授权"

~2004
网络访问控制(NAC)架构

2009
DirectAccess
Windows 7/Windows Server 2008 R2
"无边界网络"

2009
Forefront 安全产品系列
"集成联动安全，统一安全策略"

2010
Forrester 提出
"Zero Trust" 概念

2012
Dynamic Access Control
Windows 8/Windows Server 2012
"基于用户、设备、资源和内容分级的动态访问控制"

2014
微软提出"新安全边界"、"现代化企业安全模型"、"假定被攻击"、"层级保护模型"等概念

2014
Google 发布
"BeyondCorp"

安全行业

2016
发布"按条件访问(Conditional Access)"

2017
Microsoft IT 发布
"Internet-first" 战略

2017
O'Reilly 出版
<<Zero Trust Networks>>

2018
"无密码"战略

2019
完成"零信任"阶段性部署，并持续改进

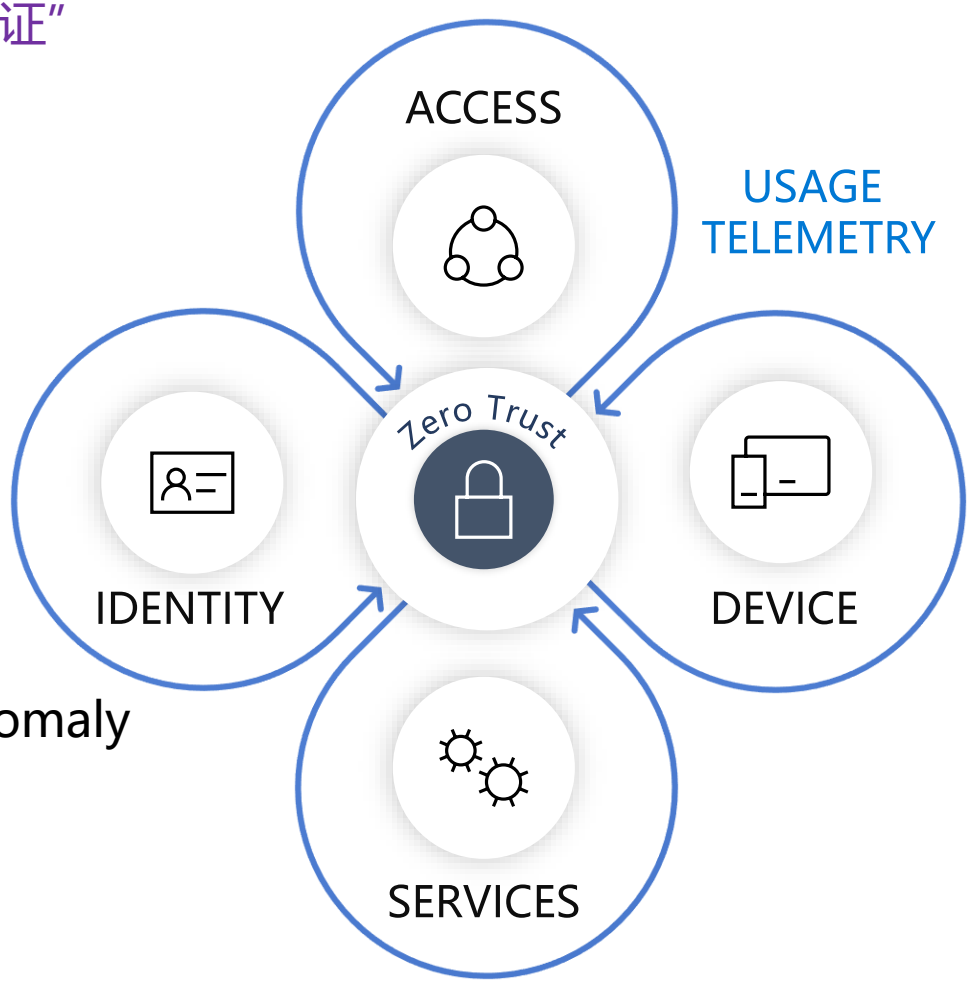
2019
NIST SP 800-207 Draft

微软IT：2019年零信任新战略 – 目标与收益

"Strong identity + device health + least privilege user access verified with telemetry"

"身份强认证+设备健康度+最小权限用户访问，由安全大脑验证"

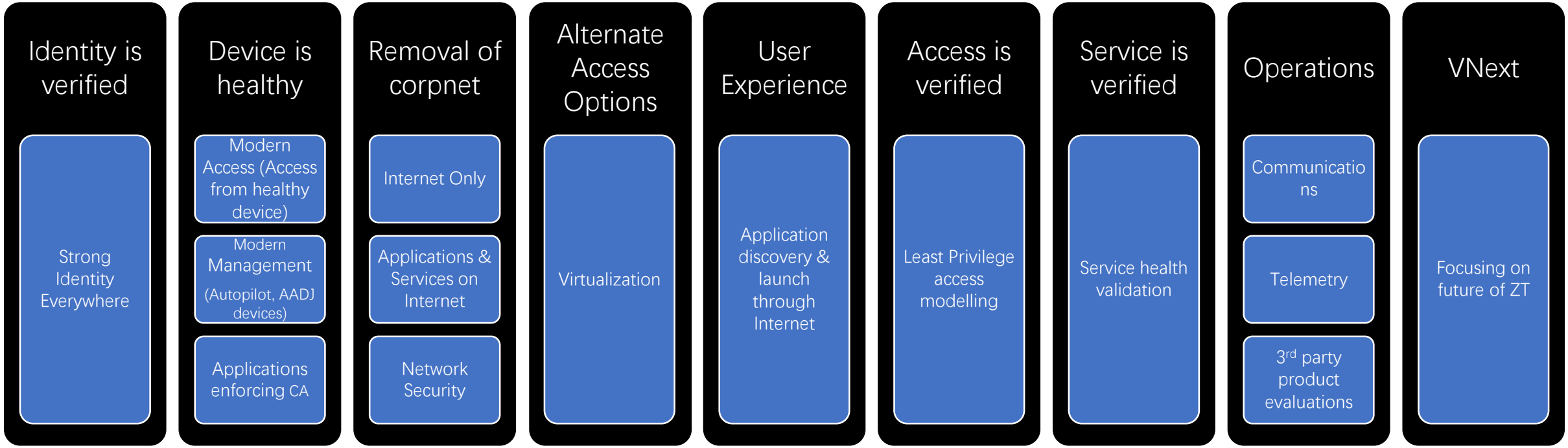
- ✓ Assets are moved from the internal network to the internet… except for the most critical assets
  从内网迁移到互联网的数字资产
- ✓ Enhanced user experience with Internet First
  互联网优先的增强用户体验
- ✓ Reduced attack surface of the environment
  环境中减小的攻击面
- ✓ Comprehensive telemetry, artificial intelligence for anomaly detection, service health verification
  发达的安全大脑，人工智能异常检测，服务健康验证



CSA零信任成熟度模型-业务场景：远程办公

微软IT：2019年零信任新战略 – 实施计划

- Scenarios-> Requirements->Workstreams owned by various sub-organizations
  场景-> 需求->工作流 涉及公司大批部门
- Resulted in 15 sub programs reporting under ZT 零信任下面分解为15个子项目
- Yes, Zero Trust is a Super Epic ☺ 零信任是漫长而艰难的伟大史诗



CSA零信任战略咨询服务框架 – 安全战略规划

微软IT：2019年零信任新战略 – 实施思路

身份 IDENTITY	• Eliminate passwords and migrate to Windows Hello 消除密码登录认证，迁移到“Windows Hello”生物特征登录认证 • Set Multifactor Authentication as the default 设置多因素认证为默认
设备 DEVICE	• Require all devices to be Modern Managed 要求所有设备被现代化管理 • Ensure all devices meet health requirements 确保所有设备满足健康度要求
访问 ACCESS	• Move devices and users to respective network segments 迁移设备和用户到相应的网络隔断 • Grant bare minimum access and permissions 授予最低限度的访问权限
服务 SERVICE	• All the applications and services apply Zero Trust principles 使所有应用和服务采用零信任原则 • Require applications and services to provide their health certificate 要求应用和服务提供各自的健康证书

CSA零信任成熟度模型-技术安全：身份、设备、网络、应用

微软IT：2019年零信任新战略 – 保护范围

服务/应用数量：	2K+ (e.g., Microsoft Office apps, line-of-business apps)
用户数量：	150K+ (e.g. employees, vendor contractors, partner users)
设备数量：	600K+ (e.g. iPhone, Android, Mac, and Windows (Linux is an eventual goal))
不包含：	175 million partners, 3.5 billion customers

Scenario 1 剧情效果1	As an **employee**, I can **enroll my device into management** to get access to company resources.
Scenario 2 剧情效果2	As an **employee** or a business guest, **I have a method to access corporate resources when not using a managed device**.
Scenario 3 剧情效果3	As an **employee**, I have **user interface options** (portal, desktop apps) that provides the ability to discover and launch applications and resources that I need.
Scenario 4 剧情效果4	As an **application or security stakeholder**, **my application validates the health of devices** prior to allowing them to connect.

CSA零信任成熟度模型-职能安全： 界定保护范围

微软IT：2019年零信任新战略 – 业务流转

Pre-Zero Trust

- ✓ Device management not required
- ✓ Single factor authentication to resources
- ✓ Capability to enforce strong identity exists

Verify Identity

- ✓ All user accounts set up for strong identity enforcement
- ✓ Strong identity enforced for O365
- ✓ Least privilege user rights
- ✓ Eliminate passwords – biometric based model

Verify Device

- ✓ Device health required for SharePoint, Exchange, Teams on iOS, Android, Mac, and Windows
- ✓ Usage data for Application & Services
- ✓ Device Management required to tiered network access

Verify Access

- ✓ Internet Only for users
- ✓ Establish solutions for unmanaged devices
- ✓ Least privilege access model
- ✓ Device health required for wired/wireless corporate

Verify Services

- ✓ Grow coverage in Device health requirement
- ✓ Service health concept and POC **(Distant Future)**

CSA零信任成熟度模型-职能安全：记录业务流转

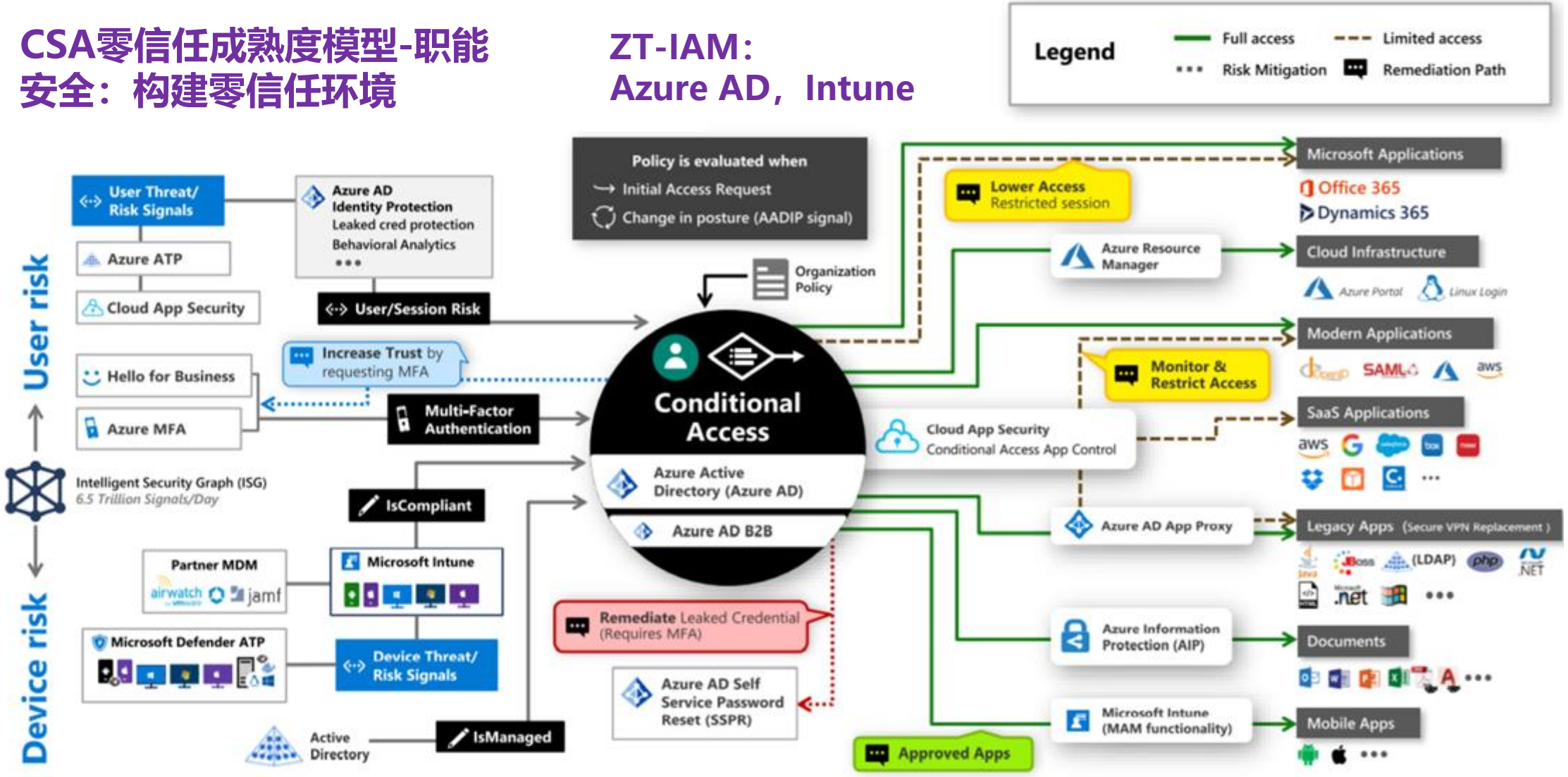
User and Access Telemetry

微软IT：2019年零信任新战略 – “IAM”零信任环境

CSA零信任成熟度模型-职能

安全：构建零信任环境

ZT-IAM：
Azure AD，Intune



状态数据（Signal）
用于支持后续的评估决定

评估决定（Decision）
基于企业的统一安全策略管控

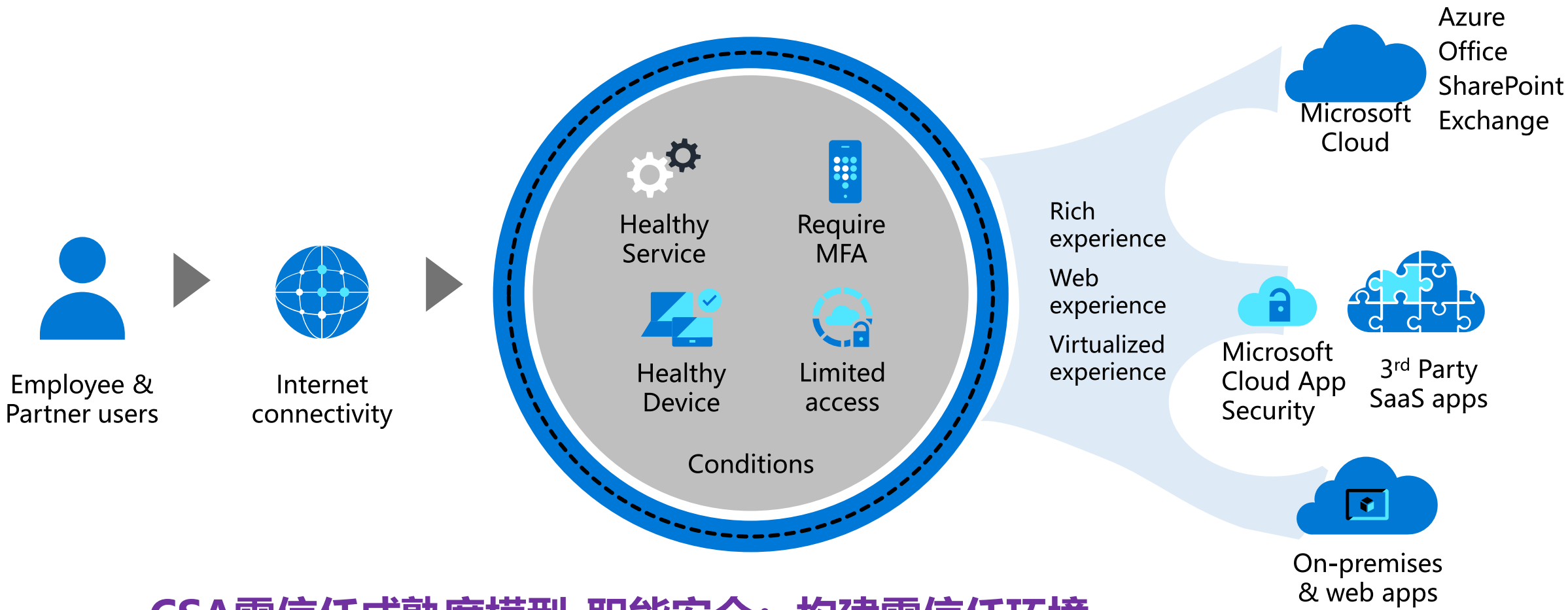
强制执行（Enforcement）
确保安全控制的有效性并持续监控

微软IT：2019年零信任新战略 – “SDP”零信任环境

“软件定义边界SDP”代理

“软件定义边界SDP”网关

“ 软件定义边界SDP”控制器



CSA零信任成熟度模型-职能安全：构建零信任环境

微软IT：2019年零信任新战略 – “MSG”零信任环境

Unmanaged Internet

- Sponsored Acces
- Event Access
- BYOD

Internet Only

Managed Internet

- Managed Devices
- Authenticated Devices

Access to Corp services

Managed CORP

- Managed Devices
- Special purpose on

Direct to Corpnet

Get Connected

Please select one of the following login methods:

Guest Access

Employee Internet

Employee Corpnet

Guests require employee sponsorship

Employees can self-sponsor

User MFA and device is AD or AAD managed + Device health

User MFA and device is AD or AAD managed + device health

Asset/Device registration

Specialized Segments

- Administration (Infra)
- Dev/Research Scenarios
- Game Studios
- IoT/Security (Facilities)

Controlled Access to Corp

Pre-Authentication Process

Admin Network

Dev Network

Games Network

Facilities Network

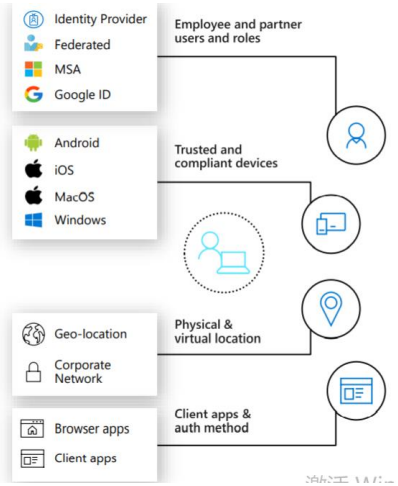
Device is pre-registered for access to specialized segments

“微隔离MSG”网络

CSA零信任成熟度模型-职能安全：构建零信任环境

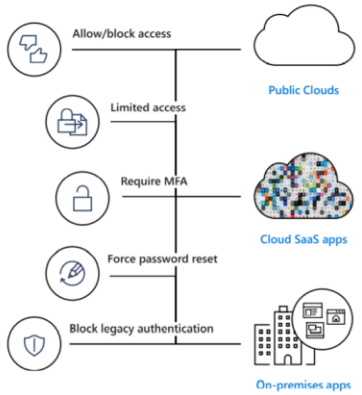
微软IT：2019年零信任新战略 – 创建策略

- 谁访问数据？他们的角色是什么？他们如何访问？
- 用户账户的安全风险如何？（例如使用弱密码/泄露的密码、低密码强度、使用行为等）
- 设备类型是什么？设备健康状态/安全状态如何？它在访问什么数据？数据重要性/机密性/敏感性如何？
- 用户所在位置如何？当前登录位置？历史登录行为？
- 访问的目标应用是什么？SaaS、云端应用、企业本地部署应用、还是移动App？



基于动态评估结果，给与决定是：

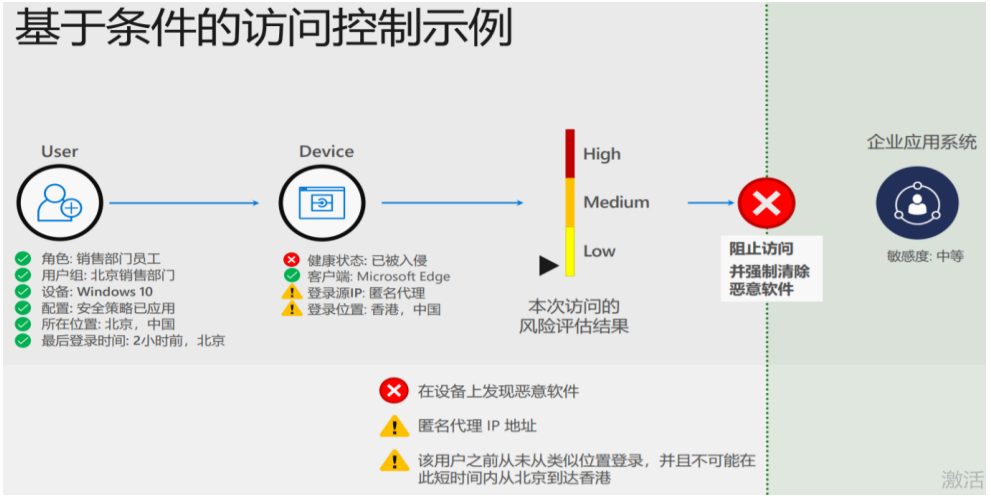
- 允许/拒绝访问
- 要求多因素身份验证
- 强制重置用户密码
- 限制访问特定应用、特定功能（例如禁止下载文件等）



最终组合在一起，就是：

按条件访问、动态风险评估的"零信任"部署模型

基于条件的访问控制示例



CSA零信任成熟度模型-职能安全：创建零信任安全策略

微软IT：2019年零信任新战略 – 监视维护

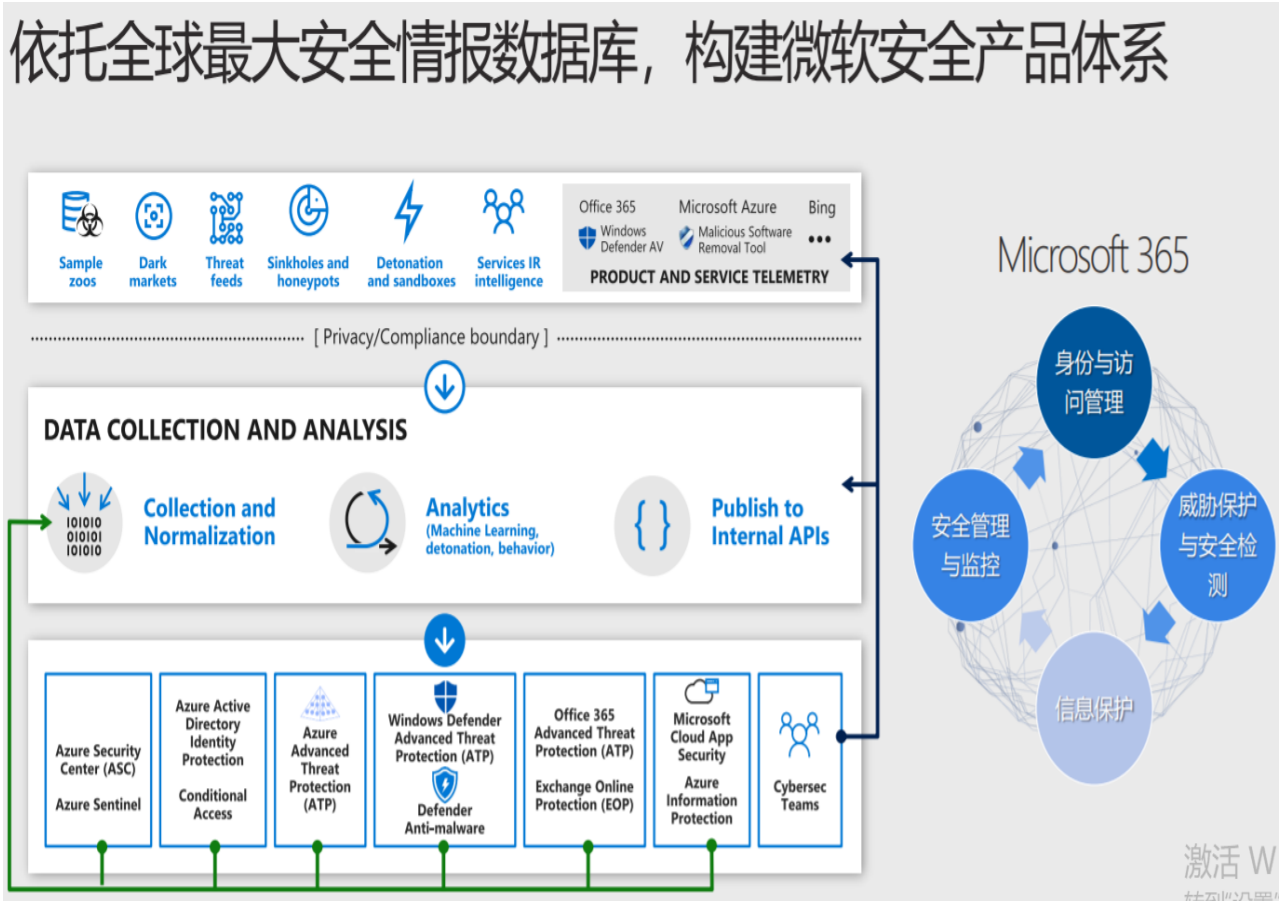
Microsoft ATA 部署

1. 地表最强的"Windows"入侵监测系统
   a) 针对活动目录的APT 高级攻击监测
   b) 基于大数据/机器学习的用户及实体行为分析
   c) 揭秘极为隐秘的攻击行为
2. Detecting the undetectable
3. 覆盖完整的 APT 攻击链

安全审计日志优化与规范

1. 溯源/还原用户/系统行为
2. 有效检测攻击行为
3. 高效检测，优化日志数据量

依托全球最大安全情报数据库，构建微软安全产品体系



CSA零信任成熟度模型-职能安全：监视和维护

零信任落地之路总结

- 微软零信任之路获得全部6大价值：98%用户可以远程办公，100% iOS/Android/Mac/Windows设备可管理
- 这世界上没有两个企业是完全相同的， “零信任”落地也是。
- “零信任”是一个持续进化的旅程，而不是一个结果。
- 成功部署零信任的企业遵循123456：

一个理念	二轮驱动	三项技术	四种能力	五项原则	六大价值
• 永不信任 始终验证	• 战略 • 架构	• SDP • IAM • MSG	• 安全成熟度 • 安全战略规划 • 安全解决方案 • 安全人才培养	• 不做任何假定 • 不信任何人员 • 随时检查一切 • 防范动态威胁 • 做好最坏打算	• 降低风险 • 降低成本 • 业务敏捷 • 安全合规 • 有效控制 • 管理改善

Accelerating to Zero Trust

微软CEO纳德拉：“零信任使我们应花两年的数字转型缩短到两个月”

“We've seen two years' worth of digital transformation in two months.”

—Satya Nadella, CEO, Microsoft

CZTP™
Certified
Zero Trust Professional

认证零信任专家

- “认证零信任专家”CZTP课程 – 欢迎各培训机构
- “零信任行业全景图” – 欢迎各公司参与入榜
- “零信任研究工作组” - 欢迎各位安全专家参与

微信：csagcr　　电话：18098258797

邮箱：info@c-csa.cn　官网：www.c-csa.cn

CSA GCR cloud security alliance®
GREATER CHINA REGION


2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音