神州数码
Digital China

神州数码安全解决方案

成为
领先的数字化转型合作伙伴

解决方案概述

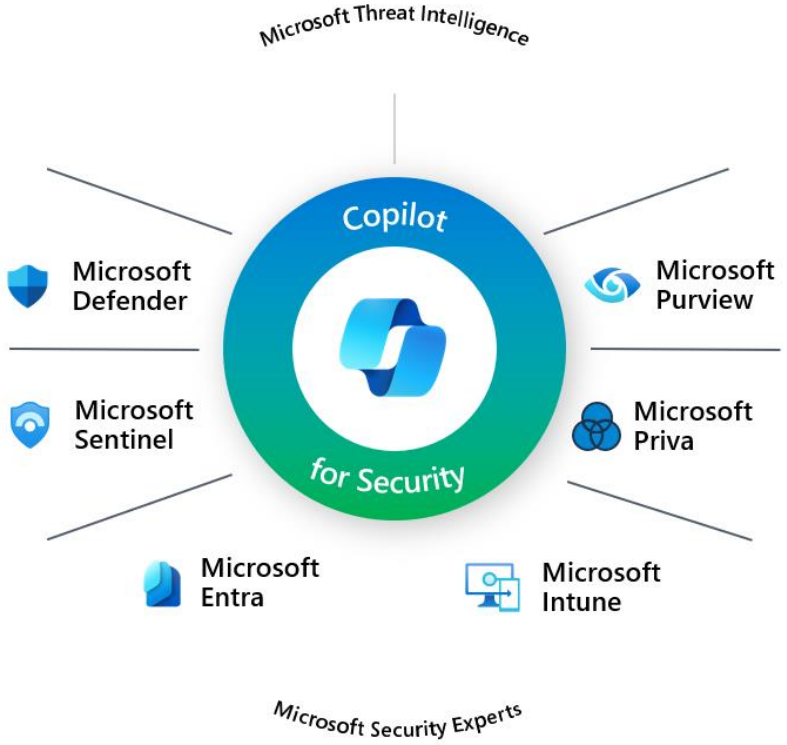
身份访问安全

通过微软 Microsoft Entra ID（原 Azure AD）提供强大的身份验证和访问控制能力，支持 单点登录（SSO）、多因素认证（MFA）、条件访问策略以及基于风险的身份保护。它是 Zero Trust 架构的核心，确保用户、设备和应用在访问资源前都经过验证和授权，降低凭据泄露和未经授权访问的风险。

威胁防护与检测

借助微软的 Microsoft Defender 系列覆盖端点、邮件、身份、云应用和 IoT/OT 环境，提供跨平台的威胁检测与响应能力。这些解决方案通过 Microsoft 365 Defender 实现统一的威胁情报和自动化响应。

- Defender for Endpoint：高级防护、行为分析、EDR。
- Defender for Office 365：防御钓鱼、恶意附件和链接。
- Defender for Identity：检测 AD 攻击和横向移动。
- Defender for Cloud Apps：CASB 功能，监控云应用风险。
- Microsoft Defender for Cloud ：帮助企业在多云和混合环境中实现安全态势管理（CSPM）和工作负载保护（CWPP）



数据安全和合规

Purview 专注数据的全生命周期管理，通过数据分类、敏感信息保护、合规性报告、内幕风险管理和审计，确保企业满足法规要求并降低数据泄露风险。

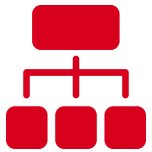
通过Purview里的AI，帮助用户智能发现与分类，自适应数据保护策略，实时分析并进行风险监测和智能预警，支持AI应用与合规。

安全运营与自动化

通过微软 Microsoft Sentinel（云原生 SIEM）和 Security Copilot 提供智能化的安全运营能力。Sentinel 整合日志、威胁情报和分析，支持自动化响应（SOAR），帮助安全团队快速检测、调查和修复威胁。Security Copilot利用生成式 AI 提升分析效率，简化复杂事件调查，降低安全运营成本并提高响应速度。

解决方案应用场景

神州数码 Digital China


企业零信任安全

场景：企业在多云、多设备和远程办公环境下，传统边界防护已无法满足安全需求。零信任架构要求“永不信任，始终验证”，通过身份验证、设备合规性检查和最小权限访问控制，确保每一次访问都经过严格验证。

方案：微软的零信任解决方案（如 Microsoft Entra ID、条件访问策略）能够实现基于身份和风险的动态访问控制，降低凭据泄露和横向移动攻击风险，同时支持多因素认证（MFA）和自适应策略，提升安全性与用户体验。

终端安全防护

场景：企业终端设备（PC、移动设备、服务器）面临恶意软件、漏洞利用和勒索攻击的威胁，尤其在混合办公和 BYOD 场景下更为复杂。

方案：Microsoft Defender for Endpoint 提供跨平台防护，结合行为分析、威胁情报和自动化修复，能够实时检测并阻止高级攻击。其与 Intune 集成可实现设备合规性管理，降低攻击面并简化安全策略部署。

信息安全与合规

场景：企业需要保护敏感文件和数据在传输、共享和存储过程中的安全，尤其在跨部门协作和外部共享场景中。

方案：Microsoft Purview 信息保护通过标签和加密技术实现数据分类与保护，支持自动识别敏感信息（如财务数据、个人隐私），并与 Microsoft 365 深度集成，确保数据在本地、云端和移动端的全生命周期安全。

云应用安全

场景：企业广泛使用 SaaS 应用（如 Microsoft 365、Salesforce），面临数据泄露、账户劫持和影子 IT 风险。

方案：Microsoft Defender for Cloud Apps（CASB）可对云应用进行发现、访问控制和数据保护，支持 OAuth 应用治理和实时会话策略，防止敏感数据外泄。结合 Microsoft Purview，可实现跨云的数据合规与审计，满足监管要求。可借助Entra ID的

安全运营与威胁狩猎

场景：企业安全团队需要应对海量日志和告警，快速识别潜在威胁并进行响应，尤其在面对高级持续性威胁（APT）时。

方案：Microsoft Sentinel 作为云原生 SIEM 平台，结合 AI 和自动化剧本，实现跨环境的威胁检测、调查和响应。其内置威胁狩猎查询和丰富的连接器，帮助企业主动发现隐蔽攻击，提升安全运营效率并降低成本。

Security Copilot赋能实现端到端的安全防护与合规管理

Imcloud

01. 公司简介

成为
领先的数字化转型合作伙伴

神州数码，领先的数字化转型合作伙伴

神州数码 Digital China

1196+亿元
全年营收 (2023)

6100+
员工数量

2600+
技术人员数量

300+
技术生态伙伴

30000+
渠道生态伙伴

123位
《财富》中国上市公司500强 (2023)

No. 38
《财富》最受赞赏中国公司全明星榜 (2023)

29位
福布斯中国数字经济100强(2022)

80位
中国民营企业500强 (2024)

26位
新型实体企业100强 (2024)

No. 1
连续十余年蝉联IT分销、IT增值分销

No. 2
中国云运维管理服务市场份额 (2022)

No. 2
中国应用交付市场份额-国产应用交付产品 (2023)

Top. 8
信创PC企业排行榜 (2022)

Top. 9
中国信创服务器企业排行榜 (2022)

2023年度最具投资价值上市公司
资本市场水晶球奖

中国最具价值品牌 500 强
GY Brand

Imcloud

一站式云资源平台

神州数码 Digital China

与全球云资源商深度合作，构建覆盖主流IaaS、PaaS及SaaS的云资源池，方便客户比选及一站式采购。火山渠道框架正在进行中。

Microsoft

Microsoft Azure Expert MSP合作伙伴
金牌合作伙伴
微软人才培训暨认证合作伙伴
Azure、Office365、Dynamics365 Indirect OSPA Partner
2019 微软年度最佳云管理服务合作伙伴
2019 微软中国最佳培训服务合作伙伴
2020 微软年度最佳合作伙伴（中国区）

中国移动 China Mobile

战略合作伙伴
签订战略合作伙伴协议之后，在专有云等领域展开多维度布局与落地实践
移动云全国总经销商

亚马逊云科技

全球MSP认证合作伙伴
战略合作伙伴
中国区VAP合伙伙伴（总代理）
全球及中国授权SPP合作伙伴
Advanced Consulting Partners
Migration Competency认证
APN高级咨询合作伙伴
中国解决方案提供商

HUAWEI

华为云战略级经销商
同舟共济合作伙伴
CSSP伙伴
DevOps平台方向优选级认证
华为认证级培训合作伙伴
北京、江苏、广东、四川、深圳伙伴能力中心

阿里云

全国总经销商
战略合作伙伴
MSP核心合作伙伴
精英级合作伙伴
大数据与AI生态合作计划伙伴
IOT渠道分销合作伙伴

京东智联云

全国总经销商
战略合作伙伴

腾讯云

腾讯会议企业版总经销商
战略合作伙伴
腾讯公有云CSP服务合作伙伴
腾讯安全产品总经销商

Google Cloud

谷歌云Premier Partner

IBM IBM Bluemix redhat

IBM Cloud Paks 臻选合作伙伴
红帽认证云计算及服务供应商(CSSP)
红帽认证云计算及服务分销商(CSSPD)
红帽VAD合作伙伴
红帽软件经销商RBP
红帽全球培训服务供应商
红帽服务外包商

vmware

Digital China Innovation Center
Powered by VMware、VMware中国区VCPP Aggregator、VMware中国区阿里ACVS业务战略合作伙伴、VMware中国区总分销

paloalto NETWORKS　ORACLE　influxdata Act in Time　elastic　Adobe　webex　aruba a Hewlett Packard Enterprise company　AUTODESK.

FORCEPOINT　Check Point SOFTWARE TECHNOLOGIES LTD.　bmc　AUTOMATION ANYWHERE　AZUL SYSTEMS　f5　+ableau　splunk>　puppet　Imcloud

专业技术服务能力

神州数码 Digital China

技术背景

- 团队拥有非常强的技术背景
- 拥有所在领域的专业认证
- 专注技术能力积累，不断学习

客户经验

- 多年大型项目交付经验
- 丰富的中大型客户经验
- 注重行业应用场景的积累

管理流程

- 标准的项目管理体系
- 能服务于软件的整个生命周期
- 以客户为中心，反应迅速

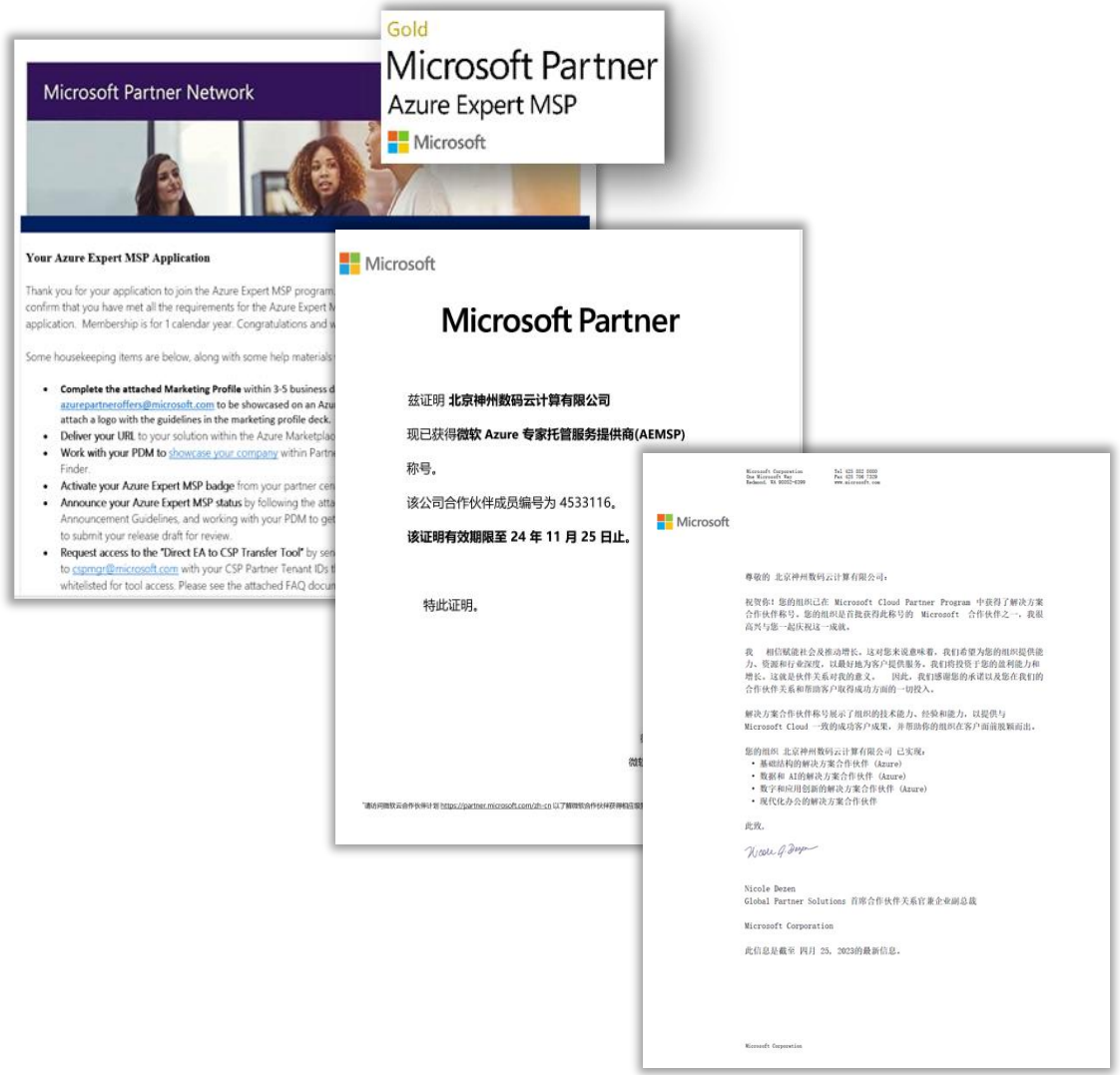
平台资源&战略合作态度

- 上市公司背书，财务稳健
- 运营牌照、资质齐全
- 集团转型决心及技术投入
- 集平台所有能力与客户合作

Imcloud

微软体系认证

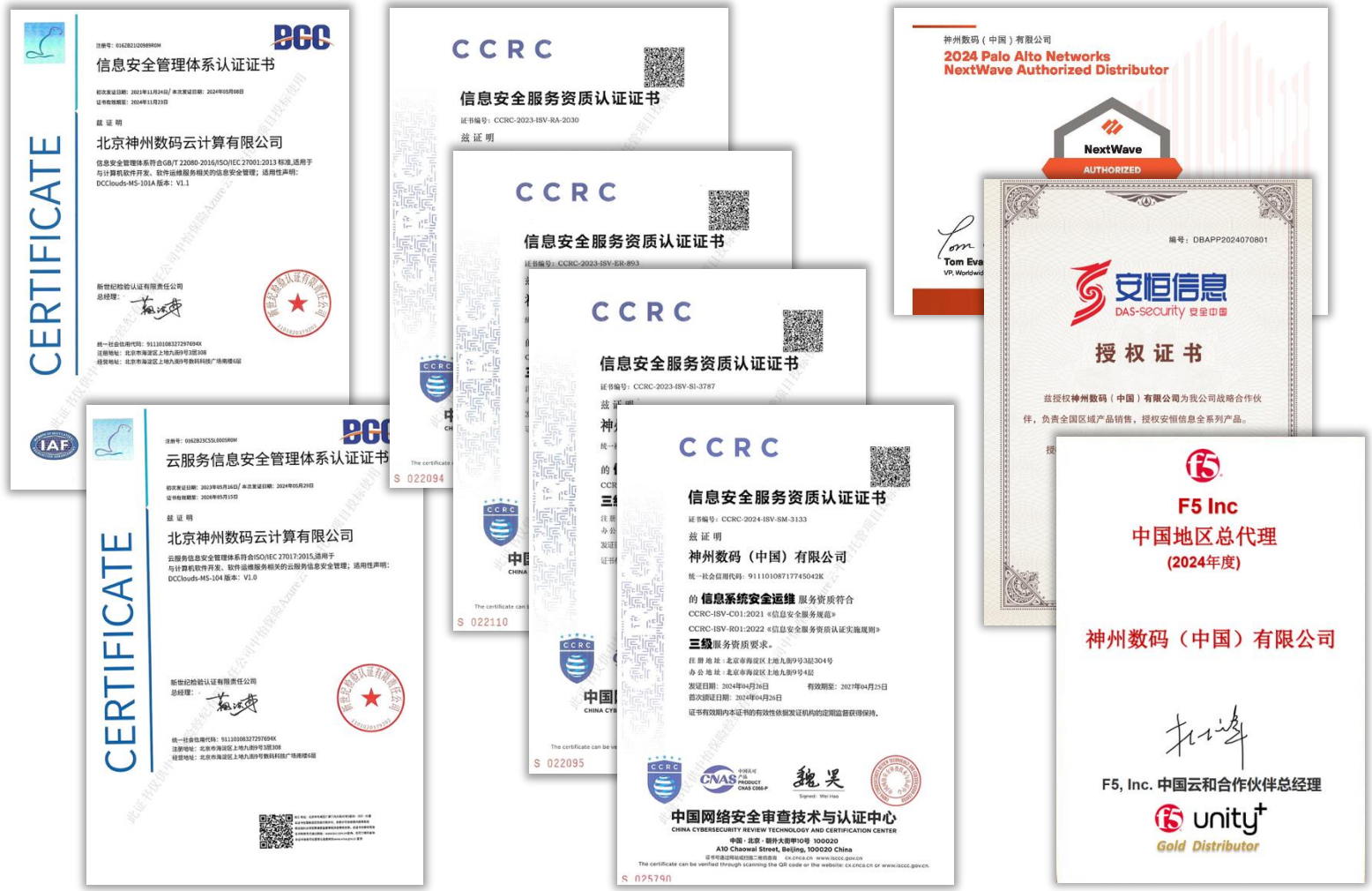
- Microsoft Azure Expert MSP 金牌合作伙伴
- 微软Azure专家托管服务提供商（AEMSP）
- FY23 Microsoft Cloud Partner Program（首批获得）
- Microsoft Azure Advanced Specialization 合作伙伴（Build AI Apps On Microsoft Azure、Infra and Database Migration to Microsoft Azure、Migrate Enterprise Apps to Microsoft Azure、Adoption and Change Management、Cloud Security）
- 微软云解决方案间接提供商(Indirect OSPA Provider)
- 微软云解决方案提供商(O365 CSP 2T总代)
- 微软许可解决方案提供商(LSP)
- 微软云解决方案聚合器提供商(Solution Aggregator)
- 微软中国云解决方案供应商(Direct CSP)
- Solutions Partner for Data & AI 合作伙伴
- Solutions Partner for Digital & App Innovation 合作伙伴
- Solutions Partner for Modern Work 合作伙伴
- Solutions Partner for Security 合作伙伴
- Solutions Partner for Infrastructure 合作伙伴



安全服务资质

- ISO 27001
- ISO 27017
- CCRC-信息安全风险评估
- CCRC-信息安全应急处理
- CCRC-信息系统安全集成
- CCRC-信息系统安全运维

- Palo Alto 授权认证合作伙伴
- F5 授权认证合作伙伴
- 安恒战略合作伙伴



团队介绍

神州数码 Digital China

- 公有云BU战略技术售前、交付基地：
  - ✓ 技术人员招聘
  - ✓ 人员培养及管理
  - ✓ 项目需求提供咨询
  - ✓ 项目交付等技术服务
  - ✓ 技术调研及创新

发展

99% 本硕学历比例	100% 专业认证比例	32岁 平均年龄	50+ 累计交付项目数

公有云BU-微软产品部-微软技术部

10+技术人员

公有云BU-技术部

40+技术人员

云技术工程师

500+正式员工

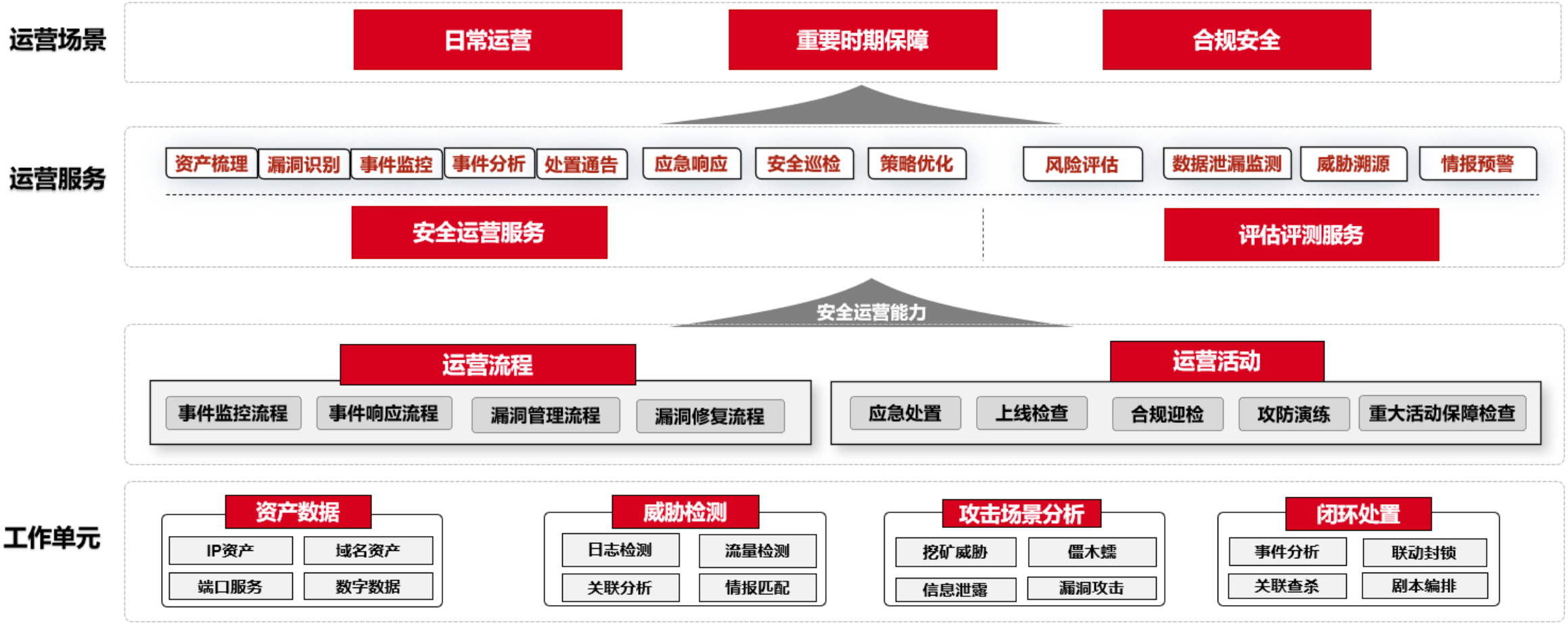
02. 解决方案&案例

成为
领先的数字化转型合作伙伴

神州数码安全管理体系

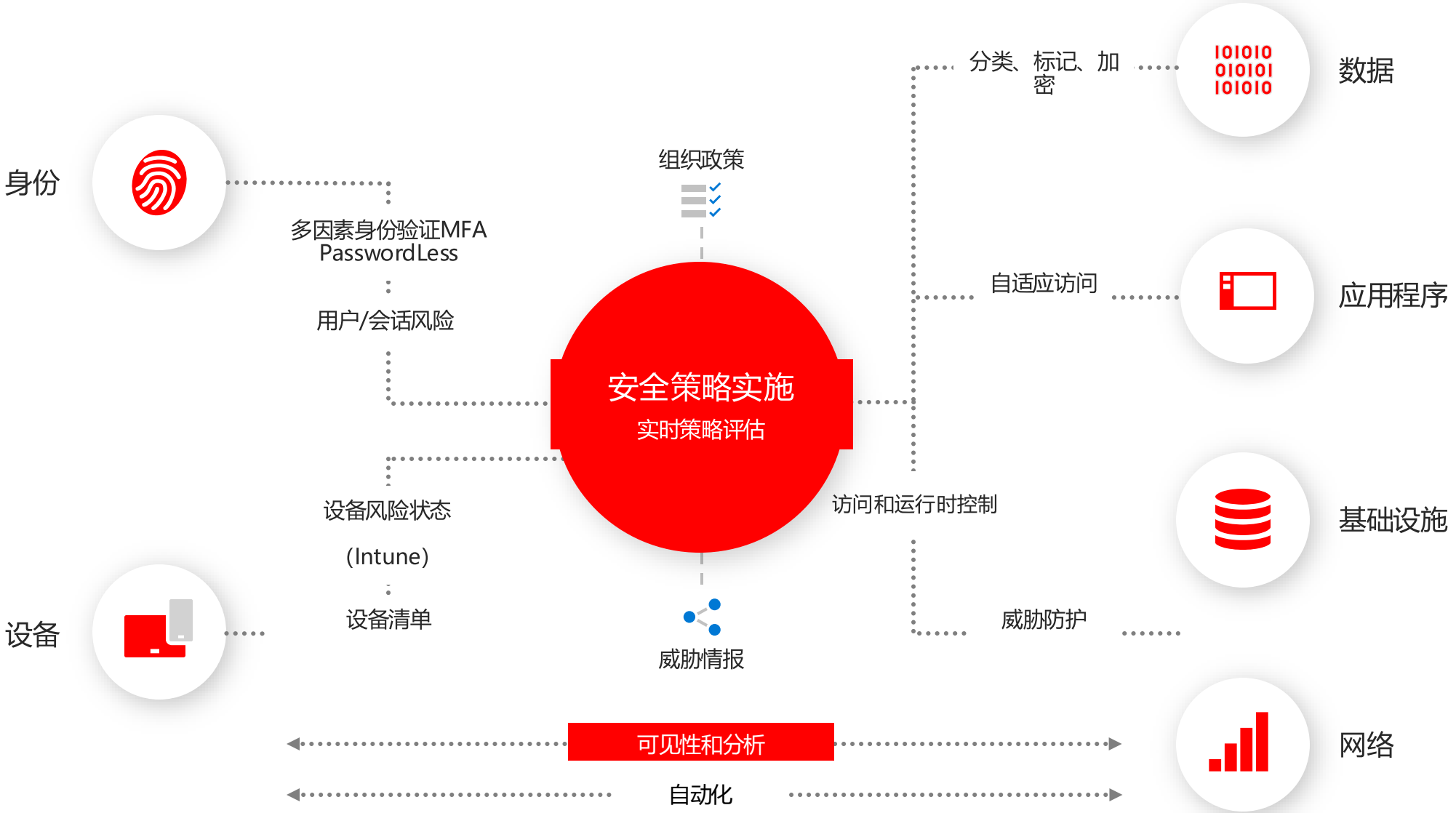
神州数码 Digital China

安全运营体系是通过人、工具(技术)和流程的深度融合，围绕日常安全运维工作和重大时期安全保障方向进行设计，同时以安全验证手段辅助，形成持续迭代优化的过程，构建可持续的安全监测和响应能力。



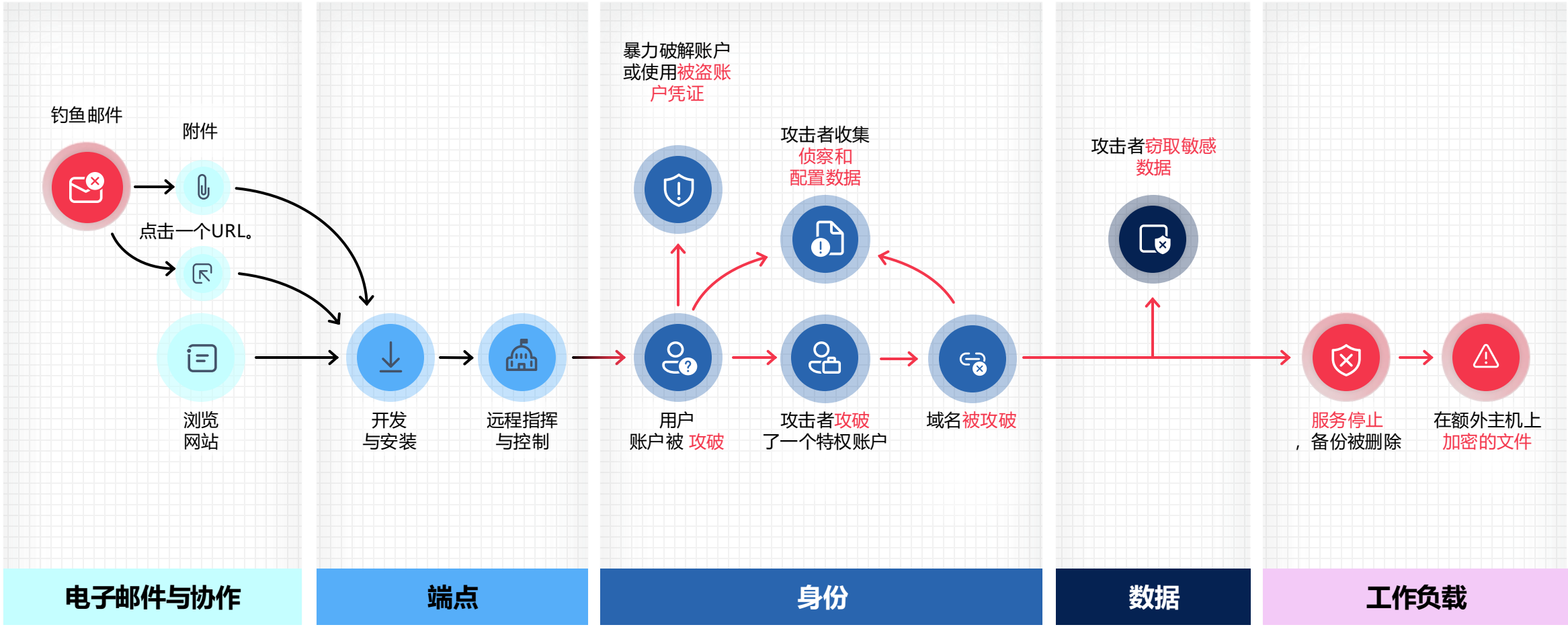
Imcloud

赋能企业实现零信任管理策略



使用图标思维来应对攻击

端到端安全解决方案



企业零信任解决方案概述

神州数码 Digital China

部署阶段	身份与访问控制			设备与应用安全			数据安全与威胁防护		
	MFA	条件访问	PIM	Intune	MDE/ MDB	MAM	Purview	MDCA	Sentinel
部署原则	以身份为核心，确保每个用户和设备都经过验证 最小权限原则，基于风险动态调整访问			确保设备合规性，阻止不安全设备访问企业资源 应用级别防护，防止数据泄露			数据全生命周期保护，防止敏感信息泄露 主动威胁检测与响应，提升安全运营能力		
部署要点	• 启用 MFA：为所有用户配置多因素认证，尤其是管理员账户。 • 实施条件访问：根据用户位置、设备合规性和风险级别动态控制访问。 • 身份治理：配置生命周期管理、访问评审，防止权限过度分配。 • 集成单点登录（SSO）：统一身份认证，减少凭据暴露风险。			• 设备注册与合规策略：通过 Intune 强制设备加密、补丁更新。 • 终端防护：部署 Defender for Endpoint，启用实时威胁检测与响应。 • 应用保护策略：在移动设备上实施应用隔离和数据防护。 • 风险信号集成：将设备风险纳入条件访问策略，实现动态控制。			• 数据分类与标签：使用 Purview 自动识别敏感数据并应用加密策略。 • 云应用治理：通过 Defender for Cloud Apps 管控 SaaS 应用访问和数据共享。 • 安全运营中心建设：部署 Microsoft Sentinel，配置告警规则和自动化响应剧本。 • 威胁狩猎与持续改进：利用内置查询和 AI 分析，主动发现潜在攻击。		

Imcloud

根据您关心场景选择要导入的方案

神州数码 Digital China

防外部攻击

- Defender for Office365 （啟用簡單)
- Defender for Endpoint （EDR)
- Defender for Identity + Entra ID protection
- Defender for Cloud Apps(CASB)

设备管理与帐户安全

- Defender for Endpoint （EDR)
- Defender for Identity + Entra ID protection
- Intune

零信任 (ZTA)

- Entra ID
- Intune （端点管理，适用多种不同的OS环境)
- Defender for Endpoint
- 微软全套安全方案

* 微软零信任解决方案通过资安院认证

防内部资料外泄&合规管理

- DLP（数据丢失预防）
- Informatio Protection
- 内部风险 / 电子发现 / 人工智能DSPM / ...

Imcloud

案例分享

某制造业企业零信任安全治理

背景

- 客户新部署M365租户，需要对企业安全进行总体设计以及实施
- 需要满足客户Global总部的安全需求，从身份，设备到云应用
- 整体设计需要满足微软最佳实践以及CIS benchmark

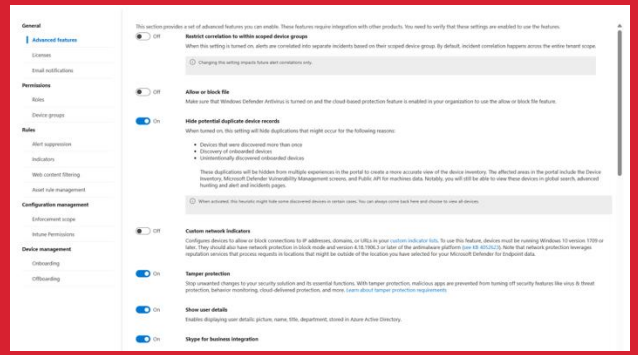
解决方案

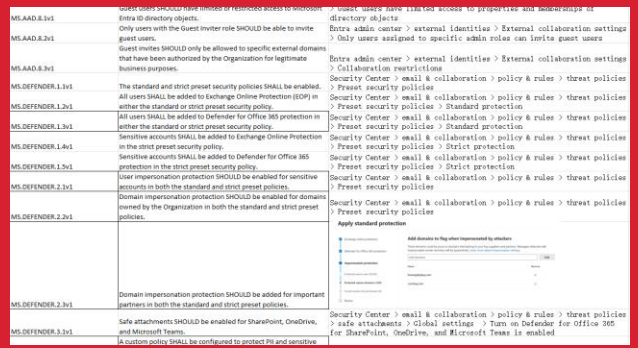
该方案基于微软零信任架构，以身份为核心，结合设备安全、应用防护、数据保护和威胁检测，实现从用户到资源的全方位安全防护。核心组件包括：Microsoft Entra ID（Azure AD）：统一身份认证与访问控制，支持 MFA、条件访问、身份治理。

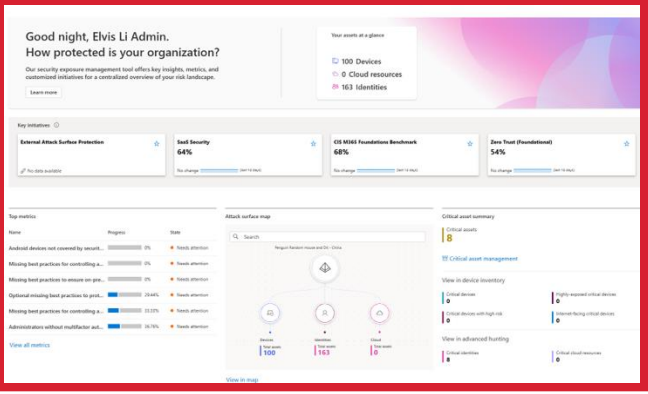
- Microsoft Entra ID: 管理身份验证，MFA，条件访问控制
- Microsoft Intune：设备管理与合规策略，确保终端安全并与身份策略联动。
- Microsoft Defender for Endpoint (MDE)：终端防护与威胁检测，提供实时防御和自动化修复。
- Microsoft Defender for Cloud Apps (CASB)：云应用安全与数据防护，防止影子 IT 和敏感数据泄露。
- Microsoft Purview 信息保护：数据分类、标签和加密，保障敏感信息全生命周期安全。
- Microsoft Sentinel：安全运营与威胁狩猎，集中日志分析与自动化响应。

收益

- 安全性提升：通过零信任架构，显著降低凭据泄露、设备入侵和数据外泄风险。
- 合规性保障：满足 GDPR、ISO等合规要求，降低审计风险。
- 运营效率提高：自动化修复、集中管理和智能告警，减少人工干预，降低安全运营成本。
- 可扩展性与未来适应性：方案基于云原生架构，支持多云和混合环境，易于扩展和升级。







终端管理及安全解决方案

神州数码 Digital China

MDM & MAM

使用 Intune 保护几乎任何设备上的数据

移动设备管理（MDM）

条件访问:
限制对托管和合规设备的访问

- 管理注册设备
- 预配设置、证书、配置文件
- 报告和检查设备合规性
- 删除设备中的公司数据

移动应用管理（MAM）

条件访问:
限制可用于访问电子邮件或文件的应用

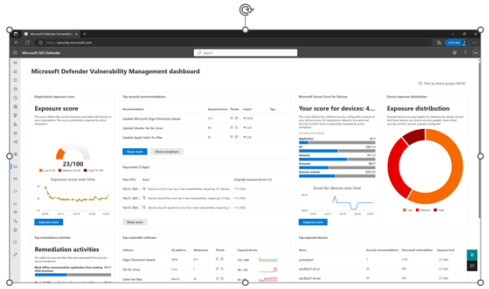
- 向用户发布移动应用
- 配置和更新应用
- 报告应用安全和使用情况
- 保护和删除移动应用中的公司数据

漏洞管理

一种基于风险的方法，用于确定漏洞的优先级并修复漏洞

- 持续的实时发现
- 情境感知优先级Context-aware prioritization
- 内置的端到端修复过程

Powered by Microsoft Defender Vulnerability Management

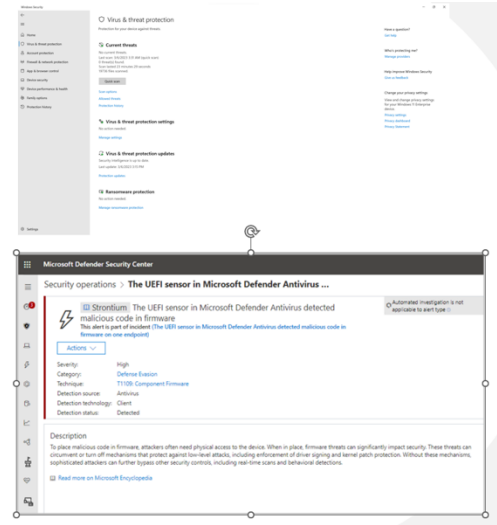


下一代威胁防护

阻止并处理复杂的威胁和恶意软件

- 基于行为的实时保护
- 阻止基于文件和无文件的恶意软件
- 阻止来自受信任和不受信任的应用程序的恶意活动

“连续 12 个月进行 Aceed 保护测试。”在现场经过验证的保护，在行业比较测试（AV-TEST、SE Labs）中始终名列前茅。

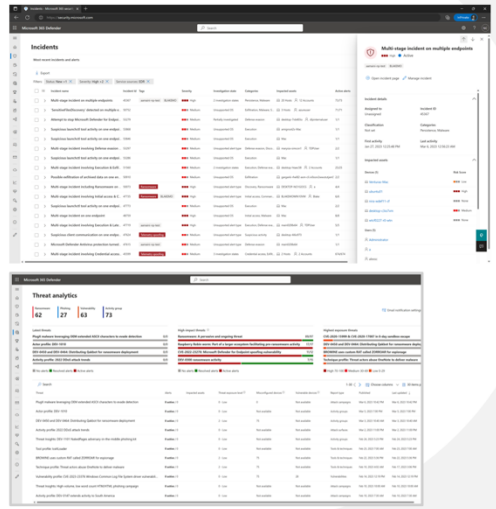


终端检测及响应

检测和调查高级持续性攻击

- 在基于 MITRE ATT&CK 的评估中展示了行业领先的检测能力
- 相关行为警报
- 调查和搜寻超过六个月的数据
- 丰富的响应操作集

威胁态势视图：通过交互式报告，了解您如何针对重要和新兴的营销活动进行评分
识别未受保护的系统 获取实时见解，以评估威胁对环境的影响
获取指导 提供建议的操作，以提高安全复原能力、预防或遏制威胁



Imcloud

终端管理及安全解决方案概述

神州数码 Digital China

1

集中设备管理

统一管理多平台设备：

- 支持 Windows、macOS、iOS、Android 等多种操作系统，适用于企业自有设备和 BYOD 场景。
- 提供集中化策略配置，简化 IT 管理流程。

设备注册与合规性策略：

- 强制设备注册到 Intune，确保企业资产可控。
- 配置合规策略（如操作系统版本、加密状态、补丁更新），不合规设备自动限制访问企业资源。

应用管理与分发：

- 支持应用部署、更新和卸载，确保应用版本一致性。
- 应用保护策略（App Protection Policies）可在 BYOD 场景下隔离企业数据与个人数据。

条件访问集成：

- 与 Microsoft Entra ID 条件访问策略联动，根据设备合规性动态控制访问，防止不安全设备访问敏感资源。

2

终端安全及威胁检测

跨平台终端防护：

- 提供针对 Windows、macOS、Linux、iOS、Android 的防病毒、防恶意软件和漏洞防护能力。
- 实时监控设备行为，阻止已知和未知威胁。

威胁检测与响应（EDR）：

- 高级威胁检测，利用行为分析和云端威胁情报识别复杂攻击。
- 自动化修复功能，减少人工干预，加快响应速度。

漏洞管理与攻击面缩减

- 集成漏洞扫描和补丁管理，帮助企业及时修复安全缺陷。
- 攻击面缩减规则（ASR）阻止恶意脚本、宏和可疑应用运行。

与 Intune 深度集成：

- 将设备风险评分纳入条件访问策略，实现基于风险的动态访问控制。
- 在 Intune 控制台统一查看设备安全状态，简化管理和监控。

Imcloud

案例分享

神州数码 Digital China

某汽车业企业海外终端管理与安全

背景

- 客户具有30+海外办公室及3000+设备需要进行统一管理和安全运维
- 需要满足客户如下核心需求：

全部设备纳入MDM管理，对不符合的设备进行告警， 对接ITSM系统，终端安全管理， 安全策略整理，应用管理等

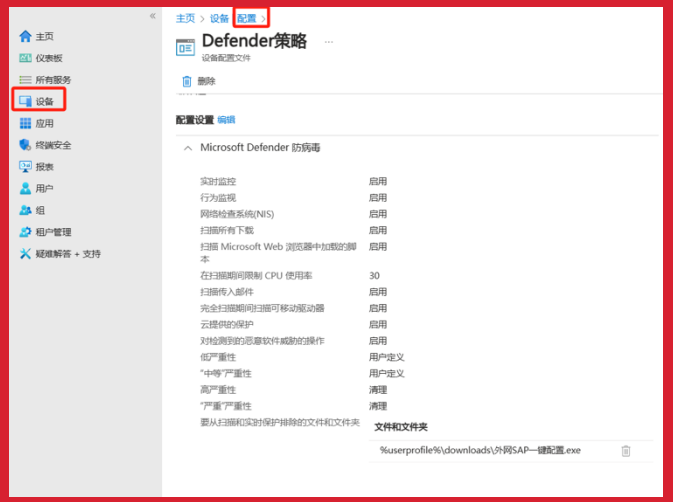
解决方案

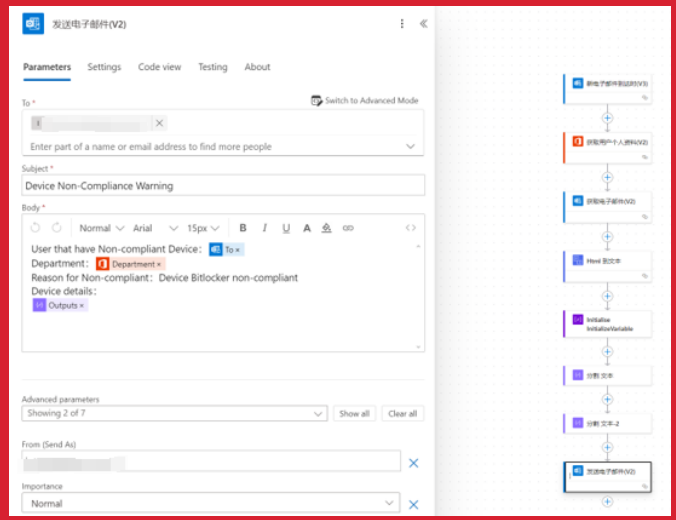
该方案基于微软Intune以及Microsoft defender for endpoint实现终端的通知管理及安全加固，通过如下方式实现了客户的核心需求

- windows autopilot注册设备实现海外设备的开箱即用
- 配置MDM策略实现终端管理及终端安全策略下发
- 配置设备合规性策略实现设备的合规管理，对于不合规的设备通过power automate流程对接ITSM系统进行工单处理
- 通过Company portal进行了应用的统一管理并使用power app开发了企业的应用入口网站平台进行应用申请及升级审批，并通过企业应用控制实现应用的黑白名单
- 通过Microsoft defender for endpoint实现了设备的EDR，威胁响应及漏洞管理

收益

- 设备开箱即用：无论设备采购地或使用地，均可实现统一的配置和策略，提升用户体验和企业标准化水平
- 确保设备符合企业安全标准；对于不合规设备，自动触发 Power Automate + ITSM 工单处理，实现闭环管理，减少人工干预。
- 结合云端威胁情报和行为分析，快速识别并处置潜在攻击，减少安全事件影响
- 通过企业应用黑白名单策略，防止安装未经授权的应用，降低安全风险。





Imcloud

神州数码
Digital China

Thanks!