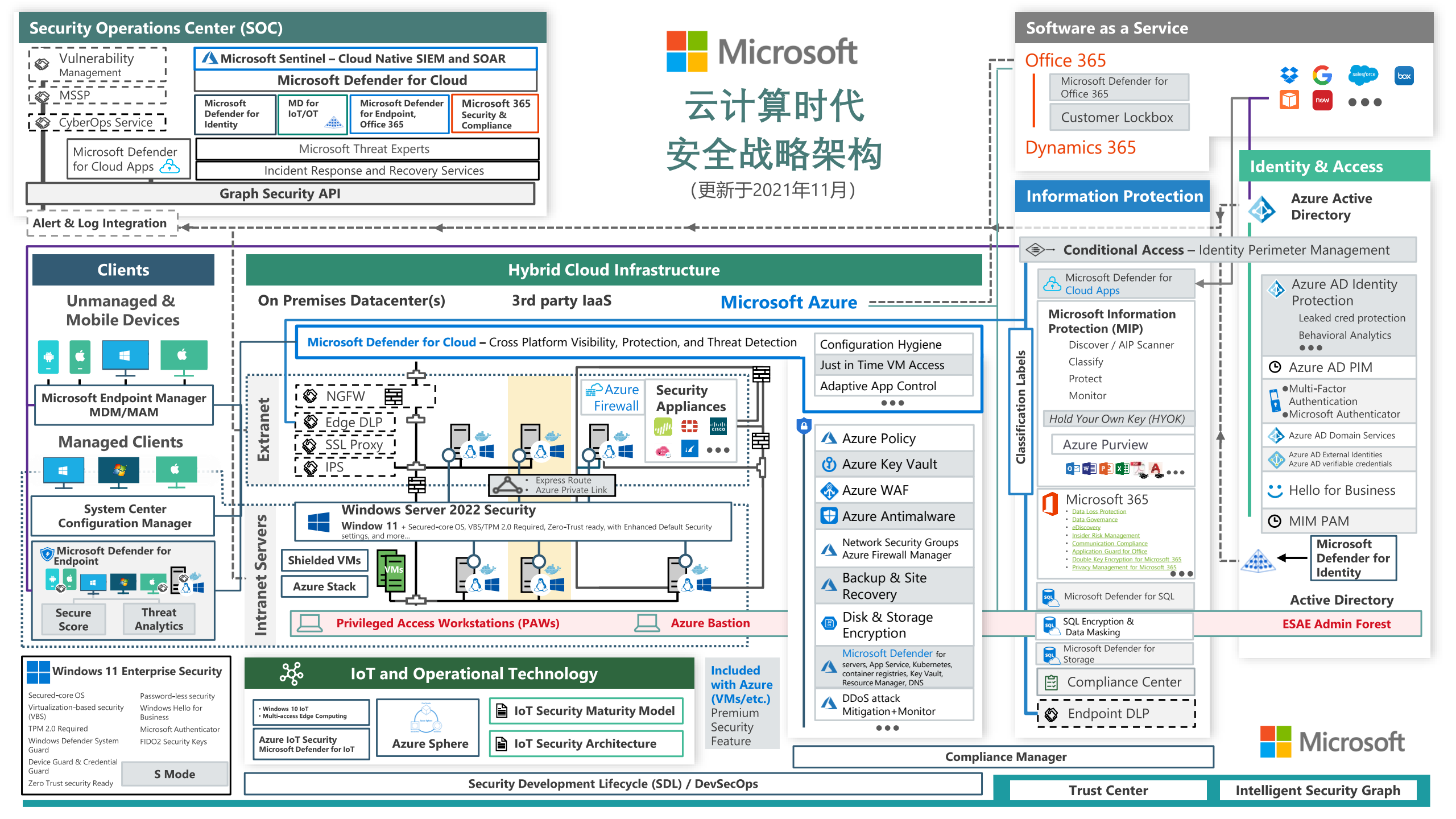
Microsoft
云计算时代
安全战略架构
(更新于2021年11月)
Security Operations Center (SOC)
Vulnerability Management
MSSP
CyberOps Service
Microsoft Sentinel – Cloud Native SIEM and SOAR
Microsoft Defender for Cloud
Microsoft Defender for Identity
MD for IoT/OT
Microsoft Defender for Endpoint, Office 365
Microsoft 365 Security & Compliance
Microsoft Defender for Cloud Apps
Microsoft Threat Experts
Incident Response and Recovery Services
Graph Security API
Alert & Log Integration
Software as a Service
Office 365
Microsoft Defender for Office 365
Customer Lockbox
Dynamics 365
Identity & Access
Azure Active Directory
Conditional Access – Identity Perimeter Management
Azure AD Identity Protection
Leaked cred protection
Behavioral Analytics
Azure AD PIM
Multi-Factor Authentication
Microsoft Authenticator
Azure AD Domain Services
Azure AD External Identities
Azure AD verifiable credentials
Hello for Business
MIM PAM
Microsoft Defender for Identity
Active Directory
ESAE Admin Forest
Information Protection
Microsoft Defender for Cloud Apps
Microsoft Information Protection (MIP)
Discover / AIP Scanner
Classify
Protect
Monitor
Hold Your Own Key (HYOK)
Azure Purview
Microsoft 365
Data Loss Protection
Data Governance
eDiscovery
Insider Risk Management
Communication Compliance
Application Guard for Office
Double Key Encryption for Microsoft 365
Privacy Management for Microsoft 365
Microsoft Defender for SQL
SQL Encryption & Data Masking
Microsoft Defender for Storage
Compliance Center
Endpoint DLP
Classification Labels
Clients
Unmanaged & Mobile Devices
Microsoft Endpoint Manager MDM/MAM
Managed Clients
System Center Configuration Manager
Microsoft Defender for Endpoint
Secure Score
Threat Analytics
Hybrid Cloud Infrastructure
On Premises Datacenter(s)
3rd party IaaS
Microsoft Azure
Microsoft Defender for Cloud – Cross Platform Visibility, Protection, and Threat Detection
Configuration Hygiene
Just in Time VM Access
Adaptive App Control
Extranet
NGFW
Edge DLP
SSL Proxy
IPS
Azure Firewall
Security Appliances
Express Route
Azure Private Link
Intranet Servers
Windows Server 2022 Security
Window 11 + Secured-core OS, VBS/TPM 2.0 Required, Zero-Trust ready, with Enhanced Default Security settings, and more...
Shielded VMs
Azure Stack
VMs
Privileged Access Workstations (PAWs)
Azure Bastion
Azure Policy
Azure Key Vault
Azure WAF
Azure Antimalware
Network Security Groups Azure Firewall Manager
Backup & Site Recovery
Disk & Storage Encryption
Microsoft Defender for servers, App Service, Kubernetes, container registries, Key Vault, Resource Manager, DNS
DDoS attack Mitigation+Monitor
Windows 11 Enterprise Security
Secured-core OS
Virtualization-based security (VBS)
TPM 2.0 Required
Windows Defender System Guard
Device Guard & Credential Guard
Zero Trust security Ready
Password-less security
Windows Hello for Business
Microsoft Authenticator
FIDO2 Security Keys
S Mode
IoT and Operational Technology
Windows 10 IoT
Multi-access Edge Computing
Azure IoT Security Microsoft Defender for IoT
Azure Sphere
IoT Security Maturity Model
IoT Security Architecture
Included with Azure (VMs/etc.) Premium Security Feature
Compliance Manager
Security Development Lifecycle (SDL) / DevSecOps
Trust Center
Intelligent Security Graph
Microsoft

Microsoft Cybersecurity Reference Architecture

(November 2021)

Security Operations Center (SOC)

- Vulnerability Management
- MSSP
- CyberOps Service
- Microsoft Sentinel – Cloud Native SIEM and SOAR
- Microsoft Defender for Cloud
- Microsoft Defender for Identity
- MD for IoT/OT
- Microsoft Defender for Endpoint, Office 365
- Microsoft 365 Security & Compliance
- Microsoft Defender for Cloud Apps
- Microsoft Threat Experts
- Incident Response and Recovery Services
- Graph Security API
- Alert & Log Integration

Software as a Service

- Office 365
  - Microsoft Defender for Office 365
  - Customer Lockbox
- Dynamics 365

Identity & Access

- Azure Active Directory
- Conditional Access – Identity Perimeter Management
- Azure AD Identity Protection
  - Leaked cred protection
  - Behavioral Analytics
- Azure AD PIM
- Multi-Factor Authentication
- Microsoft Authenticator
- Azure AD Domain Services
- Azure AD External Identities
- Azure AD verifiable credentials
- Hello for Business
- MIM PAM
- Microsoft Defender for Identity
- Active Directory
- ESAE Admin Forest

Information Protection

- Microsoft Defender for Cloud Apps
- Microsoft Information Protection (MIP)
  - Discover / AIP Scanner
  - Classify
  - Protect
  - Monitor
- *Hold Your Own Key (HYOK)*
- Azure Purview
- Microsoft 365
  - Data Loss Protection
  - Data Governance
  - eDiscovery
  - Insider Risk Management
  - Communication Compliance
  - Application Guard for Office
  - Double Key Encryption for Microsoft 365
  - Privacy Management for Microsoft 365
- Microsoft Defender for SQL
- SQL Encryption & Data Masking
- Microsoft Defender for Storage
- Compliance Center
- Endpoint DLP
- Classification Labels

Clients

Unmanaged & Mobile Devices

- Microsoft Endpoint Manager MDM/MAM

Managed Clients

- System Center Configuration Manager
- Microsoft Defender for Endpoint
  - Secure Score
  - Threat Analytics

Hybrid Cloud Infrastructure

On Premises Datacenter(s) | 3rd party IaaS | Microsoft Azure

Microsoft Defender for Cloud – Cross Platform Visibility, Protection, and Threat Detection

- Configuration Hygiene
- Just in Time VM Access
- Adaptive App Control

Extranet

- NGFW
- Edge DLP
- SSL Proxy
- IPS
- Azure Firewall
- Security Appliances
- Express Route
- Azure Private Link

Intranet Servers

- Windows Server 2022 Security
- Window 11 + Secured-core OS, VBS/TPM 2.0 Required, Zero-Trust ready, with Enhanced Default Security settings, and more...
- Shielded VMs
- Azure Stack
- VMs
- Privileged Access Workstations (PAWs)
- Azure Bastion

- Azure Policy
- Azure Key Vault
- Azure WAF
- Azure Antimalware
- Network Security Groups Azure Firewall Manager
- Backup & Site Recovery
- Disk & Storage Encryption
- Microsoft Defender for servers, App Service, Kubernetes, container registries, Key Vault, Resource Manager, DNS
- DDoS attack Mitigation+Monitor

Windows 11 Enterprise Security

- Secured-core OS
- Virtualization-based security (VBS)
- TPM 2.0 Required
- Windows Defender System Guard
- Device Guard & Credential Guard
- Zero Trust security Ready
- Password-less security
- Windows Hello for Business
- Microsoft Authenticator
- FIDO2 Security Keys
- S Mode

IoT and Operational Technology

- Windows 10 IoT
- Multi-access Edge Computing
- Azure IoT Security Microsoft Defender for IoT
- Azure Sphere
- IoT Security Maturity Model
- IoT Security Architecture

Included with Azure (VMs/etc.) Premium Security Feature

Compliance Manager

Security Development Lifecycle (SDL) / DevSecOps

Trust Center | Intelligent Security Graph

Microsoft