Microsoft cloud security tools and products

Azure

Azure Active Directory Identity Protection
- Detect potential identity vulnerabilities
- Configure automated responses & actions
- Investigate suspicious incidents

IP TD 7

Azure Information Protection (AIP)
- Classify and protect emails and documents
- Track doucments and revoke access
- Sensitivity headers, footers, watermarks

ARMS

DP 4

Windows Information Protection (WIP)
- Protect against accidental data leakage
- For enterprise and BYO devices
- Works together with Azure RMS and AIP

DP 4

Azure Sentinel
- Cloud native security information event management (SIEM) & security orechestration automated response (SOAR)

TD 9

Azure Advanced Threat Protection
- Identify, detect, investigate advanced threats
- Protect user identites and credentials
- Investigate suspicious user behaviour

IP TD 3

Azure Security Center
- Unified security management across the cloud
- Advanced threat detection
- Security for VMs, IoT, Networks, Storage etc.

TD 9

Azure Privileged Identity Management (PIM)
- Management of privileged accounts
- Make Azure admin roles eligble
- Approve/deny role requests

TP 7

Microsoft Intune
- Protect company resources
- Mobile Device Management (MDM)
- Mobile Application Management (MAM)

TP DP 4 9

Portals/jump-off points

protection.microsoft.com
- General portal for security & compliance
- Solutions will be moved to other portals

- Alerts
- Classifications
- Data loss prevention (DLP)
- Data governance
- Supervision
- Threat management
- Mail flow
- Data privacy
- Search
- eDiscovery
- Reports

compliance.microsoft.com
- General portal for compliance
- Data, documents, apps, sharing

- Alerts
- Monitoring & reports
- Classification (labels, sensitivity info)
- Policies
- eDiscovery
- Supervision
- Data investigations
- Data subject requests (DSR)

servicetrust.microsoft.com
- General portal for audit and compliance

- Compliance Manager (GDPR, DSGVO, ISO)
- Trust documents
- Regional compliance information & resources
- Trust center

security.microsoft.com
- General portal for security
- Devices, users, identities, apps

- Alerts
- Monitoring & reports
- Secure Score
- Hunting
- Classification (labels, sensitivity info)
- Policies

Azure Active Directory (AAD)
- General portal to manage identity & access

- Security overview
- Idenitity Secure Score
- Conditional Access (CA)
- Multi-Factor-Authentication (MFA)
- Users flagged for risk
- Risk events
- Authentication methods

securitycenter.windows.com
- Portal to manage Microsoft Defender ATP

- Dashboards
- Incidents
- Machines list
- Alerts queue
- Auomated investigations
- Advanced hunting
- Reports

securescore.microsoft.com
- Overview over organizations security posture
- Centralized dashboard

- Identities, data, apps, devices, infrastructure

securescore.office.com
- Overview over O365 security posture
- Centralized dashboard

- OneDrive, SharePoint, Exchange Online

Azure AD Application Proxy
- Grant access to on-premises web applications for remote clients
- Passthrough of Azure AD tokens

DP 8

Microsoft Defender Advanced Threat Protection
- Advanced protection for Windows Defender
- Prevent, detect, investigate
- Advanced threat detection and protection

MD

TP TD 2

Get data from Azure

Get data from O365

Microsoft Cloud App Security
- Detect and investigate anomalies
- Discover and control shadow IT
- Protect sensitive cloud information and data

IP TP TD 3

Get data from other cloud providers

servicenow, AWS, Dropbox, Google Suite, okta, salesforce

Microsoft 365 Device Management
- One-stop shop to manage mobile devices
- Data from Intune and Azure Active Directory
- Manage client apps

Office 365

Office 365 Advanced Threat Protection
- Cloud-based email filtering
- Protect against malware
- Protect from harmful links

TP 1

Information Rights Management (IRM)
- Protect files in SharePoint Online
- Protection for libraries and lists
- Applies protection upon download

ARMS

DP 6

TP Threat protection

TD Threat detection

DP Data protection

IP Identity protection

1 Office 365 Enterprise E5, Office 365 Education A5, Microsoft 365 Business or standalone license

2 Windows 10 Enterprise E5, Windows 10 Education E5, Microsoft 365 E5

3 Enterprise Mobility + Security E5 or standalone license

4 Enterprise Mobility + Security E3, Azure AD Premium P1

5 O365 Business Premium, O365 Business Essentials

6 SharePoint Online Plan 1, Office 365 Enterprise E1

ARMS Azure Rights Management Service

MD Microsoft Defender

7 Azure AD Premium P2

8 Azure AD Basic

9 Custom license/tier/pricing

Description

- Identity protection
- Device protection
- E-Mail protection
- Attachment protection
- Investigation
- Mobile Device protection
- Document/data protection
- Encryption
- Alerting
- Link protection
- Malware protection
- Cloud/tenant protection

Feature/product name with hyperlink to Microsoft Docs article (use Ctrl + click to open URL)

Key features of the product

Office 365 Advanced Threat Protection
- Cloud-based email filtering
- Protect against malware
- Protect from harmful links

TP 4

4 Enterprise Mobility + Security E3, Azure AD Premium P1

Describes the lowest necessary licenses.

For example at least "EMS E3" or "AAD Premium P1" **or higher**.

TP Threat protection

Describes the main protection topic

christoph.ratavaara@isolutions.ch | V 1.1 | 18.04.19