

# Microsoft cloud security tools and products

## Azure

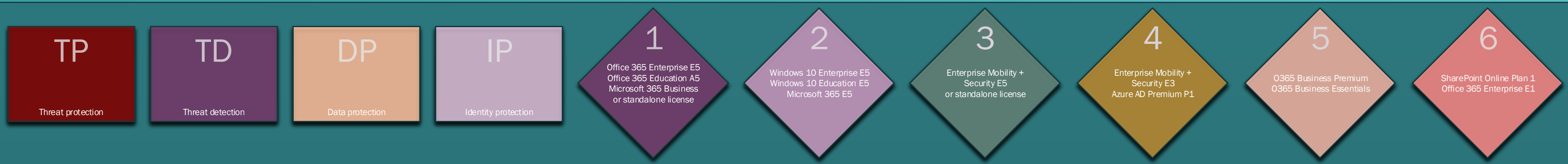
- Azure Active Directory Identity Protection**
  - Detect potential identity vulnerabilities
  - Configure automated responses & actions
  - Investigate suspicious incidents
- Azure Information Protection (AIP)**
  - Classify and protect emails and documents
  - Track documents and revoke access
  - Sensitivity headers, footers, watermarks
- Windows Information Protection (WIP)**
  - Protect against accidental data leakage
  - For enterprise and BYO devices
  - Works together with Azure RMS and AIP
- Azure Sentinel**
  - Cloud native security information event management (SIEM) & security orchestration automated response (SOAR)
- Azure Advanced Threat Protection**
  - Identify, detect, investigate advanced threats
  - Protect user identities and credentials
  - Investigate suspicious user behaviour
- Azure Security Center**
  - Unified security management across the cloud
  - Advanced threat detection
  - Security for VMs, IoT, Networks, Storage etc.
- Azure Privileged Identity Management (PIM)**
  - Management of privileged accounts
  - Make Azure admin roles eligible
  - Approve/deny role requests
- Microsoft Intune**
  - Protect company resources
  - Mobile Device Management (MDM)
  - Mobile Application Management (MAM)

## 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
  - Identity 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
  - Automated investigations
  - Advanced hunting
  - Reports
- seurescore.microsoft.com**
  - Overview over organizations security posture
  - Centralized dashboard
  - Identities, data, apps, devices, infrastructure
- Azure AD Application Proxy**
  - Grant access to on-premises web applications for remote clients
  - Passthrough of Azure AD tokens
- seurescore.office.com**
  - Overview over O365 security posture
  - Centralized dashboard
  - OneDrive, SharePoint, Exchange Online
- Microsoft Defender Advanced Threat Protection**
  - Advanced protection for Windows Defender for remote clients
  - Prevent, detect, investigate
  - Advanced threat detection and protection
- Microsoft Cloud App Security**
  - Detect and investigate anomalies
  - Discover and control shadow IT
  - Protect sensitive cloud information and data
- 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
- Information Rights Management (IRM)**
  - Protect files in SharePoint Online
  - Protection for libraries and lists
  - Applies protection upon download



## Description

