



# Microsoft Defender

## Cheat Sheet

### DEFENDER XDR

Microsoft Defender XDR helps coordinate detection, prevention, investigation and response actions. It provides a central view by using information from other Microsoft Security products, including:

- Microsoft Defender for Endpoint
- Microsoft Defender for Office365
- Microsoft Defender for Identity
- Microsoft Defender for Cloud Apps
- Microsoft Defender Vulnerability Management
- Microsoft Defender for Cloud
- Microsoft Entra ID Protection
- Microsoft Data Loss Prevention

### DEFENDER PRODUCTS – LICENSED BY M365

Defender for:		Licensed:
Endpoint	MDE is an Enterprise endpoint security platform for prevention, detection and response. Available in different flavours (P1, P2, Business).	Per User
Office365	Provides protection against threats in email, links, URLs, file attachments and collaboration tools. Available in different flavours (P1, P2).	Per User
Identity	Leverages signals from on-premises Active Directory to identify, detect and investigate suspicious activities.	Per User
Cloud Apps	Provides discovery and protection for SaaS applications using CASB & SSPM functionality.	Per User
Vulnerability Management	Provides asset visibility, assessment and remediation for Endpoint and Network based devices.	Per User

### DEFENDER PRODUCTS – LICENSED BY AZURE

Defender for:		Licensed:
Cloud	A cloud-native application protection platform (CNAPP) that includes security solutions for different cloud-based workloads.	N/A
CSPM	Provides advanced security posture assessment capabilities for multi-cloud environments.	<a href="#">Per Billable Resource</a>
Servers	Uses the same technology as MDE for protection of Servers. Deployment of Defender for Servers differs from MDE and is controlled via the Azure portal. Available in different flavours (P1, P2).	Per Server
App Service	Identifies attacks targeting applications running over App Service.	Per Instance
Storage	Prevents malicious file uploads, sensitive data exfiltration and data corruption.	Per Storage Account
Containers	Provides security posture management, vulnerability assessment and run-time threat protection of container services.	Per VM Core
Key Vault	Detects unusual and potentially harmful attempts to access or exploit Key Vault accounts.	Per Vault
Resource Manager	Monitors the resource management operations via security analytics to detect threats.	Per Subscription
API	Helps improve your API security posture, identify vulnerabilities and detect active real-time threats.	Per Subscription