### Microsoft 365 Defender Overview

Microsoft 365 Defender is an extended detection and response (XDR) solution that protects across:

- **Endpoints** (Defender for Endpoint)
- **Office 365** (Defender for Office 365)
- **Identities** (Defender for Identity, Entra ID Protection)
- **Cloud Apps** (Defender for Cloud Apps)
- **Data** (Purview DLP and Insider Risk)

---

### Defender Product Suite

- **Defender for Office 365** – Email, links, attachments, phishing
- **Defender for Endpoint** – Threat & vulnerability management, EDR, ASR
- **Defender for Cloud Apps** – CASB for Shadow IT, anomaly detection
- **Defender for Identity** – On-prem AD threat detection
- **Defender Vulnerability Management** – Exposure insights
- **Microsoft 365 Defender** – Centralized XDR portal

---

### Data Loss Prevention (DLP)

DLP in Microsoft Purview helps protect sensitive data across services.

**Components:**

- **Sensitivity Labels** – Classify documents/emails
- **Sensitive Info Types** – Detect PII, financial, health info via patterns, keywords, checksums
- **Policy Locations** – SharePoint, Exchange, OneDrive, Teams
- **File Policies** – Used in Defender for Cloud Apps (MCAS) for alerting and remediation
- **Purview Console** – Investigate DLP incidents

---

### Defender for Office 365

Protects against email-based threats.

**Key Features:**

- **Safe Attachments** – Scans attachments (Block, Replace, Monitor, Dynamic Delivery)

- **Safe Links** – URL protection across:
    - Microsoft 365 apps
    - Office for the web
    - Teams
- **Anti-phishing policies**
- **Attack simulations**
- **Remediation via Action Center**

---

### Defender for Endpoint (MDE)

Provides endpoint protection and EDR capabilities.

**Capabilities:**

- Threat and vulnerability management
- Attack surface reduction (ASR)
- Endpoint detection and response
- Automated investigation & remediation
- Data retention default: 6 months

**Setup Highlights:**

- Portal: security.microsoft.com
- Device Discovery via portal
- RBAC and Device Group configuration

**Security Controls:**

- Exploit protection
- Network & Web protection
- Controlled folder access
- Device control

**Response Actions:**

- Isolate device
- Restrict app execution
- Collect investigation package
- Live Response
- Threat expert consultation

---

**Defender for Identity**

Monitors on-premises Active Directory activity to detect advanced threats.

**Steps to Configure:**

1. Create instance in Defender for Identity portal
2. Install sensors on domain controllers
3. Configure AD service accounts and permissions (SAM-R)
4. Integrate with M365 Defender and Defender for Cloud Apps

**Detections:**

- Lateral movement
- Pass-the-ticket
- Domain dominance
- Malicious insider behavior

---

**Defender for Cloud**

CSPM for Azure resources and workloads.

**Supported Resources:**

- Servers, Containers, App Services, Storage, SQL, Key Vaults, DNS, etc.

**Capabilities:**

- Continuous security assessments
- Security recommendations
- Integration with Azure Resource Graph for asset inventory

---

**Defender for Cloud Apps (MCAS)**

Microsoft's CASB solution.

**Core Functions:**

- Discover Shadow IT
- Data classification & protection
- Anomaly & threat detection
- Cloud app compliance scoring

**Policy Types:**

- File policies
- Session policies (real-time)
- Anomaly detection (e.g., impossible travel, infrequent country)

**Data Classifications:**

- Personal, Public, General, Confidential, Highly Confidential

---

**Azure AD Identity Protection**

Protects identities via risk-based policies.

**Risk Categories:**

- **User risk** – Leaked credentials, unusual behavior
- **Sign-in risk** – Impossible travel, malware-linked IPs, anonymous Ips

**Response Types:**

- **Self-remediation** – User password reset
- **Admin remediation** – Manual investigation

**Policy Types:**

- **User risk policy**
- **Sign-in risk policy**

---

**Microsoft Purview (Insider Risk)**

Manages internal risks and compliance.

**Focus Areas:**

- Data theft
- Espionage
- Insider trading
- Code-of-conduct violations

**Workflow:**

Policies → Alerts → Triage → Investigate → Take Action

---

**Audit Logging**

**Standard Audit** (Default)

- 90-day retention
- Thousands of events captured

**Advanced Audit (E5)**

- Longer retention

- High-value events (email read/forward, file access)
- Higher API bandwidth

**Setup:**

- Enable in Microsoft 365 Admin Center
- Assign proper roles
- Verify licensing

---

**eDiscovery**

**Standard eDiscovery:**

- Content search
- Export results
- Role-based access

**Premium eDiscovery:**

- Custodian management
- Advanced indexing
- Review sets, tagging, analytics
- Legal hold

---

**Microsoft Sentinel (SIEM/SOAR)**

Central SIEM for ingesting, analyzing, and responding to incidents.

**Setup Components:**

- Azure tenant, subscription, resource group, workspace
- Enable Sentinel

**Core Features:**

- **Analytics Rules** – Incident detection
- **Automation Rules** – Conditional, prioritized playbook triggers
- **Playbooks** – Logic Apps for SOAR automation
- **Workbooks** – Custom dashboards
- **Watchlists** – Whitelist users/IPs
- **Hunting Queries** – Proactive investigation using KQL
- **Content Hub** – Import analytics rules, playbooks, connectors
- **Sentinel Repos** – CI/CD integration for MSSPs

---

### ASIM & Data Normalization

**ASIM (Advanced Security Information Model):**

Standardizes log data from different sources to a common schema.

**Normalization Example:**

Match different field names like IP_Address and IpAddress for consistent analysis.

---

### KQL (Kusto Query Language) Essentials

Used extensively in Sentinel for analysis and threat hunting.

**Key Operators:**

- where, let, join, extend, project, summarize, render
- mv-expand (expand arrays), todynamic() (parse JSON), split()

**Common Queries:**

```
kql
CopyEdit
SigninLogs
| extend dynProps = todynamic(extendedProperties)
| mv-expand dynProps
| extend IPAddress = dynProps.IPAddress
| project tostring(IPAddress)
```

**Learn More:**

Join types in KQL (Docs)

Visual Video Guide