Cloud

On-Premises

Microsoft Endpoint Configuration Manager
System Center Configuration Manager (SSCM)

Additional license required

Web Content Filtering — CYREN

URL Categorization

Requires EMS E5 license

Microsoft Cloud App Security

Activities
Alerts
Host Metadata

Unsanctioned Apps notifications

Requires EMS E3 minimum license

Azure Information Protection

Apply labels

Azure ATP

Data Enrichment

Threat Intelligence

Intelligent Security Graph

Office 365

Requires O365 E5 or O365 ATP Plan 2 license

Microsoft Threat Experts

Consult Threat Experts

MSSP Support

Compliance Enforcement

Configuration Management metadata

Microsoft Intune

Microsoft Defender ATP

- Threat & Vulnerability Management
- Attack Surface Reduction (Web Content Filtering)
- Next Generation Protection
- Endpoint Detection and Response (EDR)
- Automated Investigation & Remediation
- Microsoft Threat Experts

Software Inventory

Security Recommendations

Storage | Reports | Rules | Incidents | Dashboards | Live Response

Azure AD

Power BI

Alerts / SOAR

User Information

Skype

Installation Package

Event IDs: 5007, 1121, 1122

Alerts, Incidents, Automated Investigations (security and health)

Installation Package
Configuration Package

Alerts, Incidents (security and health)

Alerts, Incidents (security and health)

Alerts, Incidents, Automated Investigations (security and health)

Azure Security Center

Onboarding

SHA, FIM, AAP

Windows 7 SP1
Windows 10

Windows OS

MDATP Package

AD Group Policy

Manual/Local Script

Up to 10 devices

Windows AD Domain Controller

macOS

Up to 10 devices

Manual/Local Script

Security Analyst

Linux

Up to 10 devices

Manual/Local Script

Installation Package

Linux Configuration Manager

Versions:
2008 R2 SP1, 2012
R2, 2016, 2019

Windows Server
(via Microsoft Monitoring Agent)

MDATP included in ASC Standard license

Up to 10 devices

Manual/ Local Script

Intune ticket

Remediation Request ticket

ASR: Web Protection, Hardware Isolation, firewall, FIM

Live Response session

Live Response session

End User

Windows Defender Application Guard

Windows OS

Remediation Activities

Security Alerts/Reports
Threat Analytics
Vulnerability Management

Advanced Hunting Queries, Custom Detection (KQL scripts)

kql

Security Operation Center (SOC)

Legacy SIEM

IT Operation Center

REST API through Microsoft Security Graph

Security Alerts

Security Alerts

Security Alerts

Azure Sentinel
Log Analytics Workspace

Logs / Metrics

Kusto Query Language Queries / Log Correlation / Enrichment

Security Alerts

Playbooks

Logic Apps

Other logs

Incidents/Tickets/Reports

SOAR: Isolate endpoint

Managed Sentinel
www.managedsentinel.com

Custom Alerts

Security Investigation

SOAR Automation

Management & Health Monitoring

M365 Integration

Defender ATP Deployment

	Windows 7	Windows 8.1	Windows 10	Windows 2008 R2	Windows 2012 R2	Windows 2016	Windows 2019	macOS	Linux	Android	iOS
Threat & Vulnerability Management	■	■	■	■	■	■	■			On the roadmap for 2020	On the roadmap for 2020
Attack Surface Reduction			■								
Next Generation Protection			■		■	■	■				
Endpoint Detection and Response (EDR)	■	■	■	■	■	■	■	■	■		
Automated Investigation and Remediation			■				■				

MDATP supported features by OS

Managed Sentinel