

CANCOM

Microsoft Defender Lifecycle Services

Support Package – im Rahmen der Premium Support Services



Hohe Bedrohungslage – steigert sich

Unterstützungsleistungen massiv gefragt

Differenzierte Angriffe aller Art auf alle Kundensegmente

- Angriffe finden statt, es ist nur eine Frage des Zeitpunkts und der Größe des Schadens

Trend **weg von Best-of-Breed** hin zu gesamtheitlichen, durchgängigen Lösungen & Ansätzen

- Vendor-Agnostische Architekturen – z.B. CANCOM Microsoft Cyber Security Architektur

Bedarf an **Unterstützung durch Dienstleister steigt an** – durch Komplexität & Ressourcenmangel

- Professional- & Managed-Services bei Security im Fokus



Verlässliche Services für alle Fälle – Einordnung Support Packages

CANCOM XAAS	Workplace as a Service		Security as a Service		UC as a Service	
	Network as a Service		Device as a Service		u.v.m.	
MANAGED SERVICES	Remote Managed Services		Hosted Managed Services		Cloud Managed Services	
	Business Applications	Datacenter	Connectivity		Security	
	Data & IoT	Workplace	UCC & Media		Customer Service	
SUPPORT SERVICES	Basic Support		Premium Support Services			
CANCOM Support Packages / Lifecycle Services						
PROFESSIONAL SERVICES	Analyse & Assess		Strategy & Plan		Build & Transform	

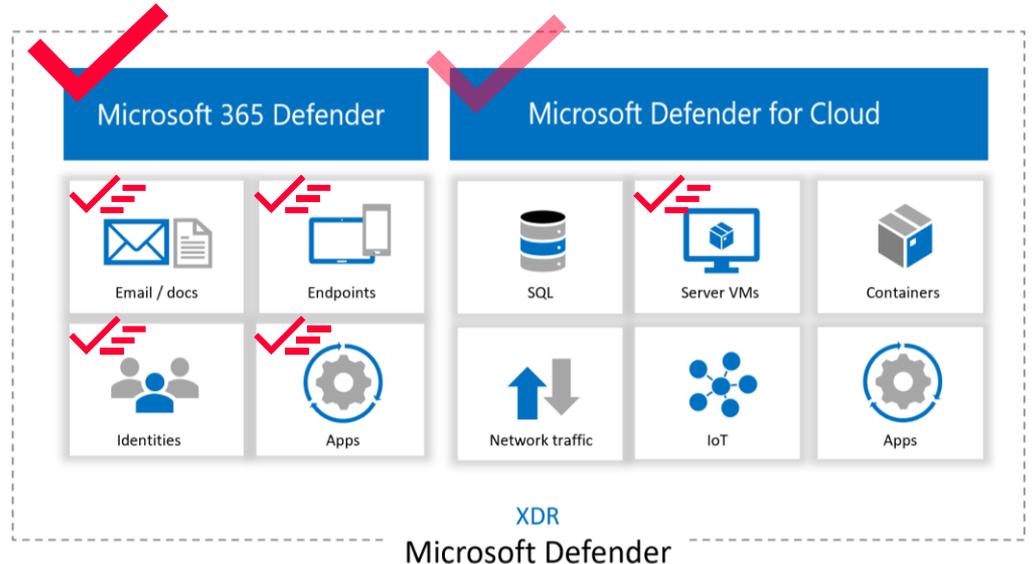
Welche Microsoft Defender Dienste unterstützen wir?

Abdeckung (fast) aller Microsoft Defender Dienste

Leistungen zur Unterstützung im Betrieb

(Kundenverantwortung)des Microsoft Defenders:

- Regelmäßigen Sichtung und Besprechung der aktuellen Auswertung/ Daten in/aus der Defender Plattform
 - Plattform-Anpassungen oder Behebungen von Störungen werden gemeinsam mit Kunden abgestimmt und analysiert
 - Durchführung eines abgestimmten Vorgehens
- ! Dies ist keine Betriebsleistung und enthält keine SLA´s für Incidents !



Was ist überhaupt ein Support Package

Planbar - regelmäßige Begleitung, fachliche Betreuung und Unterstützung



Lifecycle Service
wiederkehrende Dienstleistung

Entkoppelt von einem Incident-/Support-Vertrag – es muss kein Support/Managed-Service abgeschlossen werden



Vertrag
über CANCOM Support Center

Mehrwerte durch kontinuierliche (Security) Reifegrad-Entwicklung



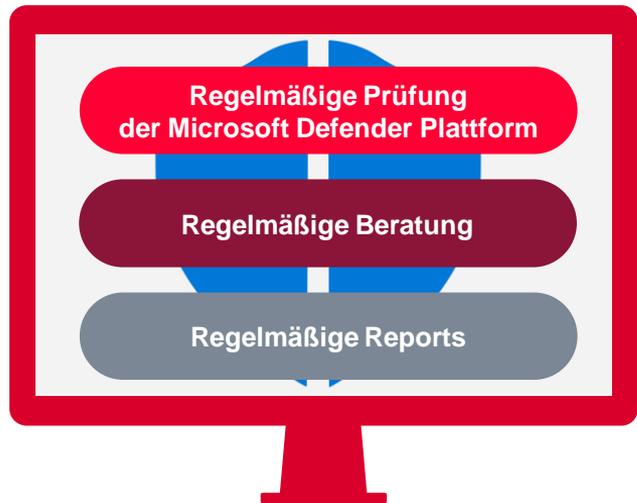
Reifegrad-Erhöhung

Standardisiert - Support Packages werden anhand definierter Best Practices & Standards erbracht



CANCOM Consultants

Grundsätzlicher Leistungsumfang des CANCOM Support Packages für Microsoft Defender



ZIEL

Erhöhung des Security Reifegrads

u.a. auch Grundlage für optimale AI/KI Nutzung,
z.B. für Microsoft Security Copilot

Regelmäßige Überprüfungen

- Konstante Prüfung der Umgebung auf Optimierungen
- Überprüfung und Bewertung von Incidents im Microsoft Defender Portal



Regelmäßige Beratungen

- regelmäßige Besprechung der erstellten Reports
- Erstellung von Handlungsempfehlungen zu entdeckten Risiken innerhalb des Reports



Regelmäßige Reports

- Erstellung regelmäßiger Reports zur Übersicht des aktuellen Sicherheits-Status



Varianten S/M/L der Support Package Microsoft Defender

Onboarding



Initiales Kunden-Onboarding über Standard
„Defender Maturity Check (DMC)“

- Leistungen
 - Onboarding des Kunden in die CANCOM Support-Prozesse
 - Analyse & Prüfung des Deployments der eingesetzte Dienste
 - Grundlegende Prüfung der eingerichteten Dienste
 - Unabhängig von Art und Anzahl der eingesetzten Defender (Endpoint, Cloud, Office 365, Identity, Cloud Apps)

Leistungsumfang enthalten in den Paketen:

SMALL

MEDIUM

LARGE

Ergänzende Leistungen*



Advisory Service

- Leistungen
 - Vorstellungen neuer Features
 - Analyse der letzten Wochen in Bezug und Betrachtung auf: Tendenzen der Incidents (Trends), Auswirkungen, Optimierungsvorschläge
- Enthaltene Kontingent je Jahr
 - 4 Personentage (PT)
- Verteilung auf folgenden regelmäßigen Zyklus
 - 1 Personentage (PT) je Quartal

Leistungsumfang enthalten in den Paketen:

MEDIUM

LARGE



Preisbeispiele

1.290€ / Monat
+
1.090€ / einmalig

**CANCOM Support Package
Microsoft Defender**

- Enthaltene Kontingent je Jahr
12 Personentage (PT)
- Verteilung auf regelmäßigen
Zyklus
½ PT zweiwöchentlich

Paket Small, optional Advisory

Small

2.890€ / Monat
+
1.090€ / einmalig

**CANCOM Support Package
Microsoft Defender**

- Enthaltene Kontingent je Jahr
24 Personentage (PT)
- Verteilung auf regelmäßigen
Zyklus
1 PT zweiwöchentlich

Paket Medium, inkl. Advisory

Medium

5.290€ / Monat
+
1.090€ / einmalig

**CANCOM Support Package
Microsoft Defender**

- Enthaltene Kontingent je Jahr
48 Personentage (PT)
- Verteilung auf regelmäßigen
Zyklus
1 PT wöchentlich

Paket Large, inkl. Advisory

Large



Kundenvorteile

1

Planbar

Regelmäßige proaktive Betreuung durch unsere Experten – mit Ihnen durch uns geplant und nachgehalten

2

Optimierung

kontinuierliche Analysen und Auswertungen und Optimierung Ihrer Microsoft Defender Plattform

3

Best Practices

Standardisierte Leistungen, die ständig aus den Erfahrungen (weiter-)entwickelt werden und in die Regeln, Betreuung einfließt

4

Reifegrad

Erhöhung des Security-Reifegrades – u.a. Grundlage für eine optimale Nutzung von AI/KI-Möglichkeiten wie z.B. Microsoft Security Co-Pilot

5

SOC Integration

Optionales Einbindung von Microsoft Lösungen in das CANCOM SOC*
*(eigenständiger CANCOM Service)



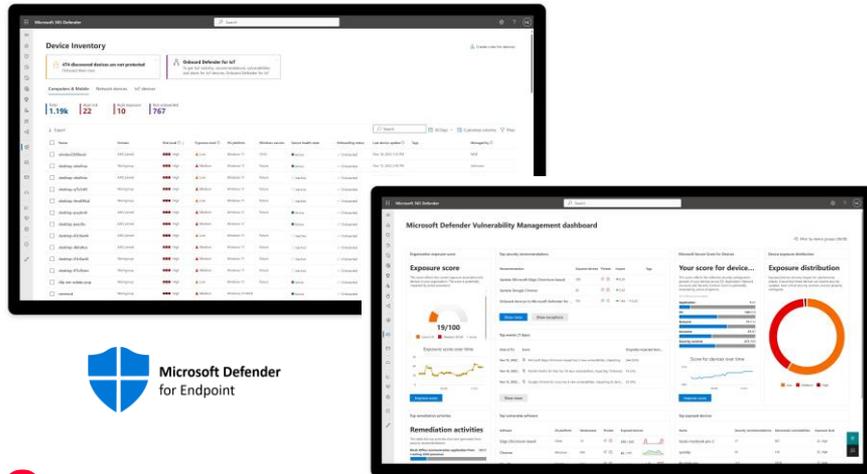
Leistungsinhalte im Detail

Je Microsoft Defender Dienst

Leistungen für: Microsoft Defender for Endpoint

Einsatzszenarien des Produktes (u.a.)

- Die Zentrale für umfassende **Endpunktsicherheit**
 - Sicherheitsrisiken und Fehlkonfigurationen in Echtzeit erkenne
 - Risiken beseitigen und Angriffsfläche verringern
 - Mobilgeräte absichern



CANCOM-Leistungen im Rahmen des Support Package

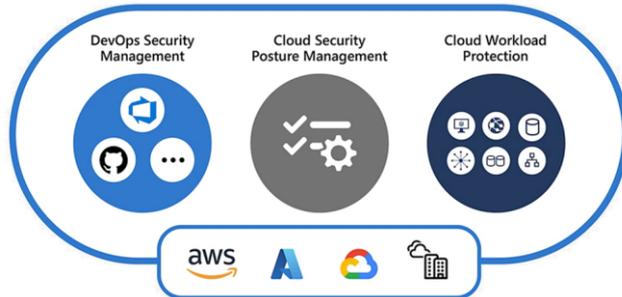
- Incident Bewertungen
 - Empfehlung / Priorisierung von Incident Betrachtung
 - Unterstützung im Auflösen von Incidents
- Individuelle Vulnerability Bewertung/ Report
 - Einschätzung neuer CVE's
 - Priorisierung von Schwachstellen
- Blockieren von besonders gefährdeten Anwendungen (Block vulnerable applications)
- Device Inventory
 - Gefährdete Geräte
 - Nicht geschützte Geräte
- Empfehlungen zum Secure Score

Leistungen für: Microsoft Defender for Cloud

Einsatzszenarien des Produktes (u.a.)

- Schützen Sie Ihre Multicloud- und Hybrid-Umgebungen
 - Profitieren Sie von komplexem Schutz für Ihre Windows- und Linux-Computer – ob lokal oder über mehrere Clouds wie Azure, AWS oder GCP
 - Risiken mit kontextbezogener Sicherheitsstatusverwaltung verringern
 - Neuartige Bedrohungen schnell erkennen, abwehren und vermeiden

Microsoft Defender for Cloud



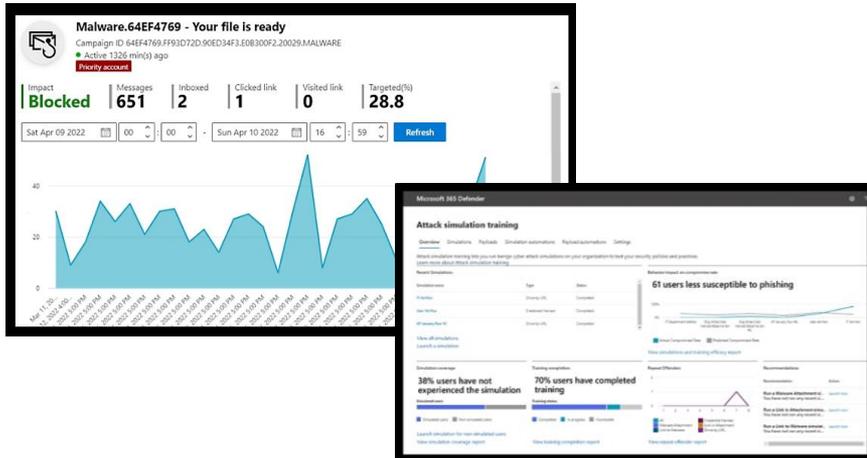
CANCOM-Leistungen im Rahmen des Support Package

- Prüfung erweiterter Sicherheitsfeatures auf Defender-Plattform
 - Überwachung von Standards NIST/ CIS1
 - Konformität mit dem integrierten Benchmark überprüfen
- Empfehlungen zur Unterstützung bei Härtung (Azure VM, Hybrid)
- Defender Cloud Security Posture Management (CSPM) *(nur im Large-Paket – und Kundenlizenz als Voraussetzung)*
 - Erkennung von Identitäts- und Netzwerkkrisiken
 - Verringerung von Risiken durch eine proaktive Angriffspfadanalyse
 - Verwendung von Cloud Security Explorer für die Risikoanalyse
 - Agentenloses Scannen von Schwachstellen
 - Governance-Richtlinien zur rechtzeitigen Vermeidung von möglichen Risiken
 - Einhaltung gesetzlicher Vorschriften und Anwendung von Best Practices

Leistungen für: Microsoft Defender for Office 365

Einsatzszenarien des Produktes (u.a.)

- Integrierter Bedrohungsschutz für Tools rund um E-Mails und Zusammenarbeit
 - E-Mail-Sicherheit stärken – ohne Kompromisse
 - Tools für die Zusammenarbeit umfassend absichern



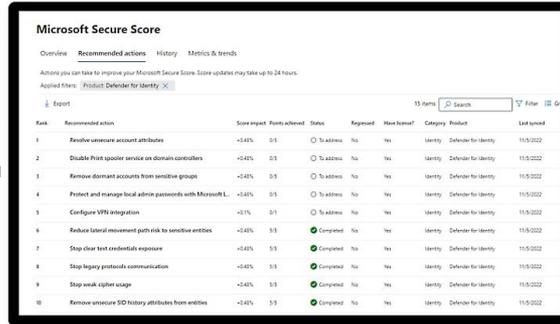
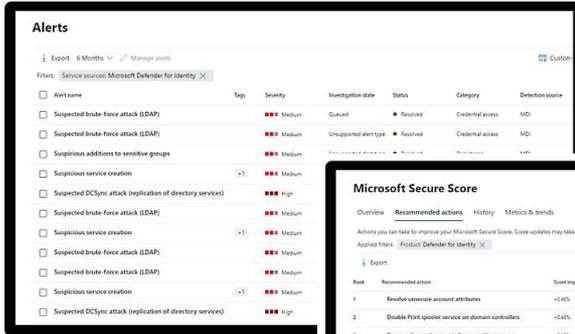
CANCOM-Leistungen im Rahmen des Support Package

- E-Mail
 - Erweiterte Alert Policies
 - Konfigurationsanalyse
 - Richtlinien-/ Regel-Empfehlungen
 - Unterstützung im Policy Design
- Reporting
 - Zusammenfassung
 - Mail Flow, Kampagnen, Mobile Device Access
 - Inbound und Outbound Mail Flow
 - Safe Attachments & Safe Links
 - Von Benutzer gemeldete Nachrichten
 - Häufigste Schadsoftware
- Awareness Schulung (*nur im Large-Paket*)
 - Angriffssimulationstraining (Phishing Simulation) halbjährlich

Leistungen für: Microsoft Defender for Identity

Einsatzszenarien des Produktes (u.a.)

- Beherrschen Sie Identitätsrisiken
 - Identitätsstatus bewerten und Abwehr stärken
 - Meistgefährdete Identitäten ermitteln



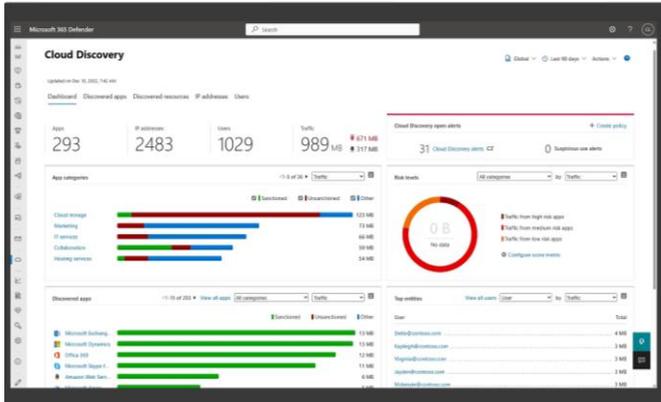
CANCOM-Leistungen im Rahmen des Support Package

- Monitoring von Identitätskonfigurationen
- Prüfung auf Best Practices
- Attack Surface Reduction
 - Exposure von Klartextkennwörtern (Report)
 - Lateral Movement-Paths (Report)
- Pflege von Ausnahmen / Policy

Leistungen für: Microsoft Defender for Cloud Apps

Einsatzszenarien des Produktes (u.a.)

- Vollständigen Überblick über SaaS-App-Landschaft verschaffen und Apps schützen
 - Shadow IT erkennen und eingrenzen
 - Vertrauliche Informationen/ Daten in SaaS-Apps schützen
 - Interaktion zwischen Apps steuern
 - Sicherheitsstatus von SaaS-Apps verwalten



CANCOM-Leistungen im Rahmen des Support Package

- Cloud Discovery Report
 - Fortlaufendes Monitoring über Apps oder Shadow IT
 - Sanktionierung von Apps
 - Top Apps von Mitarbeitern
 - Traffic from High-Risk Apps
- Empfehlungen zu Policy-Erstellung und -Verwaltung
- Recommendations Identity Security Posture
- Alert Support
- Investigations
 - Status zu App-Konnektoren
 - Überwachung welche neuen O-Auth Apps im Azure AD registriert wurden

Angebotspakete

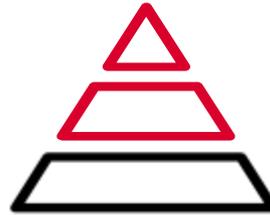


Varianten S/M/L der Support Package Microsoft Defender



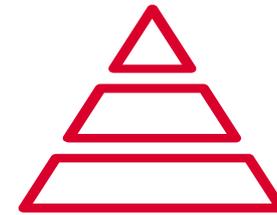
Small

- Enthaltene mögliche MS Defender Module
 - Endpoint, Cloud, Office 365, Identity, Cloud Apps
- Enthaltene Kontingent je Jahr
 - **12 Personentage (PT)**
- Verteilung auf folgenden regelmäßigen Zyklus
 - **½ PT zweiwöchentlich**



Medium

- Enthaltene mögliche MS Defender Module
 - Endpoint, Cloud, Office 365, Identity, Cloud Apps
- Enthaltene Kontingent je Jahr
 - **24 Personentage (PT)**
- Verteilung auf folgenden regelmäßigen Zyklus
 - **1 PT zweiwöchentlich**



Large

- Enthaltene mögliche MS Defender Module
 - Endpoint, Cloud, Office 365, Identity, Cloud Apps
- Enthaltene Kontingent je Jahr
 - **48 Personentage (PT)**
- Verteilung auf folgenden regelmäßigen Zyklus
 - **1 PT wöchentlich**

Preisbeispiele

1.290€ / Monat
+
1.090€ / einmalig

CANCOM
Support Package
Microsoft Defender

Paket Small, optional Advisory

Small

2.890€ / Monat
+
1.090€ / einmalig

CANCOM
Support Package
Microsoft Defender

Paket Medium, inkl. Advisory

Medium

5.290€ / Monat
+
1.090€ / einmalig

CANCOM
Support Package
Microsoft Defender

Paket Large, inkl. Advisory

Large



Summary

... zum Support/ Lifecycle Package – Microsoft Defender

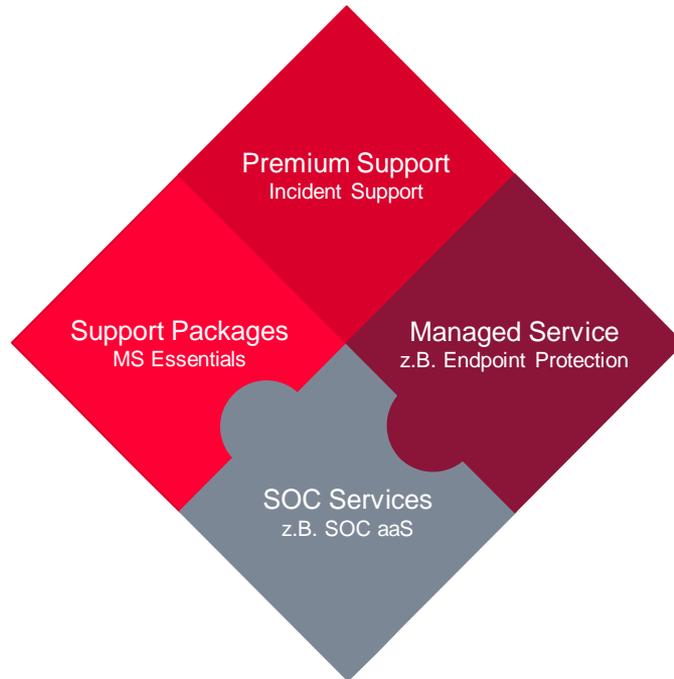


Was ist CANCOM Support Package NICHT!

- dieses Support Package ist kein proaktiver Service
 - enthält keine proaktive Erkennung wie in einem SOC (separater Service)
 - Enthält keinen Incident Support per SLA
- dieses Support Package ist kein Managed Service
 - keine Betriebsleistung
 - keine Betriebsübernahme
 - keine Betriebsverantwortung



Ergänzende Services



Premium Support Service

Genereller **Incident Service** – auf Basis klarer SLA´s und integriert mit Microsoft Herstellerservices

ergänzende Support Packages

z.B. Kombination mit dem Support Package „Microsoft 365 Essentials“

Managed Services

Managed Service für viele Microsoft Dienste & Services
Security Operations Center (SOC) as-a-Service

Eure Fragen!?



CANCOM