



MDR

**Managed Endpoint
Detection & Response
Falcon Complete**

MDR | Endgeräteschutz as a Service

Cybersecurity neu gedacht

Deine Endgeräte sind die typischen Eintrittspunkte für Cyberangriffe. Hochentwickelte Bedrohungen kompromittieren deine Computer, Laptops oder Server. Konventionelle Virenschutzprogramme können diese Angriffe nicht detektieren, da die Angreifer dateilos und durch geschicktes Hacking den Zugriff auf deine Systeme erlangen.

MDR wird durch CrowdStrike bereitgestellt. Threat Detection mit KI und Machine Learning plus Overwatchteam stehen 24/7 bereit um diese Bedrohungen zu identifizieren zu neutralisieren und den Systemzustand wieder herzustellen. Deine Endpoints werden durch Threathunter und Analysten permanent überwacht. Hier agieren echte Menschen und können Angriffsverhalten effektiv einschätzen, verfolgen und abwehren. Wird ein Angriff durch das System detektiert kommen sofort die Cyberspezialisten von CrowdStrike zum Einsatz. Der Vorfall wird bis zum Ende verfolgt und behoben. Dein Administratorenteam braucht sich um deine Cybersecurity nicht mehr zu kümmern.

Angreifer werden umgehend ausgeschaltet. Somit werden die Cyberrisiken für dich auf ein höstmögliches Minimum reduziert. Sollte es trotzdem zu einem Breach kommen, so unterstützt dich CrowdStrike mit der Breach Prevention Warranty.

Das Onboarding der MDR Lösung dauert nur wenige Tage. Somit ist die Optimierung deiner Cybersecurity in kürzester Zeit möglich. Ineffektive Anti Virus Lösungen können entfernt werden.

Der CrowdStrike Unterschied

Einzigartige Technologie

Ein revolutionärer neuer Software Agent ermöglicht eine einfache und störungsfreie Bereitstellung und stoppt alle Arten von Angriffen. Eine Planung von Scans oder Anpassung von Ausnahmen sowie Signaturupdates sind Relikte aus der Vergangenheit.

Cloud Native Plattform

Das System hat keine Notwendigkeit zur Wartung von Agents, Policies oder Konfigurationsdateien. Das System ist Always Optimized und somit auf dauerhaft beste Performance und optimalen Schutz ausgelegt.



Woher kommen die Gefahren für meine Endpoints?

Kennst du deine Gegner aus dem Darknet?

Moderne Angriffe sind ausgeklügelt, trickreich und perfekt geplant. Spuren durch Dateien oder Scripte werden nicht hinterlassen. Die Bewegung in deinem Netzwerk erfolgt vorsichtig und dateilos.



- Infektion des Browsers durch geleakte Website
- Download von infizierten Dateivorlagen
- Sicherheitslücken in deiner Software
- Sicherheitslücken in deinen Clouddiensten
- Direkte Infektion durch Datenträger

- Gefälschte Emails vom Unternehmensvorstand
- Ein verlockendes Linkangebot im Posteingang
- Fachlich interessante Themen in Email-Links
- Paketverfolgung vom Versanddienstleister
- Angeblicher Anruf aus der Nachbarabteilung

- Angriff durch staatliche Hackergruppen
- Gezielte Wirtschaftsspionage
- Angriff über Cloudanbieter oder Dienstleister
- USB Stick angeblich aus der IT-Abteilung
- Angriff über Homeoffice durch das VPN



Der Schutz der Endpoints ist ohne geeignete Technologie faktisch nicht möglich



Der CrowdStrike Technologievorsprung

- “Schützt vor bekannter und unbekannter Malware sowie vor malwarefreien oder dateilosen Angriffen”
- “Verbindet die besten und neuesten Präventionstechnologien wie maschinelles Lernen und Threat KI”
- “Beseitigt Ransomware. Schützt die Endgeräte vollständig online und offline”
- “Umfassende proaktive Lösung als vollständig verwalteter Dienst”



MDR - CrowdStrike Technologie in Perfektion

Sicherheitskomponenten perfekt kombiniert

MDR

Managed Endpoint
Detection & Response
Falcon Complete



Falcon Prevent

Prävention auf dem neuesten Stand der Technik. Volle Angriffstransparenz auf einen Blick. Einfach, schnell und schlank.

Next-Generation KI Based Endpointdetection. Schützt vor Angriffen mit oder ohne Malware. Zertifiziert, getestet und ausgezeichnet von unabhängigen Prüforganisationen.



Falcon Insight

Endgeräteerkennung und Reaktion (EDR). Unübertroffene Sichtbarkeit. Schutz gegen Datendiebstahl.

Dank kontinuierlicher Überwachung werden alle Aktivitäten an den Endgeräten erfasst. So siehst du stets genau, was passiert – von der Bedrohung an einem einzelnen Endgerät bis hin zum Bedrohungsgrad des gesamten Unternehmens.



Falcon X

Automatisierte Threat Intelligence ermöglicht es Sicherheitsteams dem Angreifer einen Schritt voraus zu sein.

Automatische Untersuchung von Vorfällen und Beschleunigung der Alarmeinteilung und Reaktion darauf. Automatische Bearbeitung der (IOCS) Kompromittierungsindikatoren.



Falcon Complete Services

Endgeräteschutz als Service. Das Höchstmaß an Endgerätesicherheit ohne den Aufwand selbst ein System erstellen und administrieren zu müssen.

Falcon Complete kümmert sich um alle Aspekte deiner Endgerätesicherheit und gewährleistet so eine optimale Effektivität. Rund um die Uhr und an 365 Tagen des Jahres Überwachung und Unterstützung bei der Reaktion auf Vorfälle, sodass wirklich alle Wammeldungen effektiv bearbeitet werden.



Falcon Device Control

Problemlose, sichere und kontrollierbare USB-Gerätenutzung.

Eine sichere und zuordnungsfähige Nutzung von USB-Geräten mit voller Transparenz und präziser sowie detaillierter Kontrolle der Nutzung von USB-Geräten.



Falcon Overwatch

Versteckte komplexe Bedrohungen erkennen und stoppen. Nahtlose Erweiterung deines Administratorenteams.

Das Overwatch Team sucht unermüdlich nach Bedrohungen und **stoppt** diese, sobald sie erkannt werden. Es sind die 1% aus 1% der Bedrohungen, die normalerweise im Verborgenen bleiben und zu Datendiebstählen führen, wenn sie nicht frühzeitig erkannt werden.



Reiner SCT Authenticator

Unknackbare TOTP 2FA Authentisierung ohne Netzwerkverbindung.



Breach Prevention Warranty

Falcon Complete Breach Warranty.

CrowdStrike bietet Falcon Complete™-Kunden eine Garantie, die bei einem Vorfall in der durch CrowdStrike Falcon Complete geschützten Umgebung bis zu \$ 1 Million für Sicherheitsverletzungsabwehrkosten abdeckt.

MDR - Optimaler Schutz für mittlere und große Unternehmen oder kleine Unternehmen mit hohem Schutzbedarf

Was kann **MDR** für mich tun?

MDR

**Managed Endpoint
Detection & Response
Falcon Complete**

**Entwickelt für
permanente
Cybersicherheit**

CrowdStrike Falcon Complete stellt dir auf einzigartige Weise die Technologie, die Plattform, die aussagekräftigen Aufklärungsdaten und das Know-how zur Verfügung – für eine umfassende und durchgängige Endgerätesicherheit. Mit Falcon Complete können Kunden die Endgerätesicherheit den bewährten Sicherheitsexperten von CrowdStrike anvertrauen; das gilt für die Implementierung ebenso wie für das Handling und die Reaktion auf Sicherheitsvorfälle. Das Ergebnis ist eine sofort optimierte Sicherheitslage, ohne den Aufwand, den Overhead und die Kosten für die interne Administration eines umfassenden Endgerätesicherheitsprogramms.

Cybersicherheit auf höchstem Niveau

Falcon Complete baut auf der CrowdStrike Falcon®-Plattform auf und ist die umfassendste Lösung von CrowdStrike für den Endgeräteschutz. Die Lösung bietet unübertroffene Sicherheit durch Kombination von Falcon Prevent™ Antivirus der neuesten Generation (NGAV), Falcon Insight™ Endgeräteerkennung und Reaktion (EDR) und Falcon OverWatch™ als verwaltete Bedrohungssuche mit dem Fachwissen und dem 24/7-Einsatz des CrowdStrike-Teams. Das Team verwaltet und überwacht aktiv die Falcon-Plattform für Kunden und behebt bei Bedarf Vorfälle per Fernzugriff. Falcon Complete verbindet die Effektivität der Falcon-Plattform mit der Effizienz eines engagierten Teams von Sicherheitsexperten, das in Ihrem Namen zielgerichtete Maßnahmen auf der Basis definierter Musterleitfäden ergreift.

Völlige Entlastung deines Administratorenteams

Falcon Complete ist die umfassende Lösung für den gesamten Lebenszyklus der Endgerätesicherheit, die alle Bereiche der Endgerätesicherheit abdeckt, einschließlich der zuverlässigen Behebung von Vorfällen per Fernzugriff – damit du dich nicht darum kümmern musst. Du erzielst damit ein Höchstmaß an Endgerätesicherheit und vereinfachst gleichzeitig die Implementierung und den täglichen Betrieb deines Endgeräteschutzprogramms. Falcon Complete stellt dir auf einzigartige Weise die Technologie, die Plattform, die aussagekräftigen Aufklärungsdaten und das Know-how zur Verfügung – für ein umfassendes Handling und eine durchgängige Endgerätesicherheit.

Deine Cybersicherheit wieder im Griff haben

Ein wirksames Programm zur Endgerätesicherheit praktisch umzusetzen, kann schwierig sein. Die notwendigen Werkzeuge setzen oft detaillierte Kenntnisse voraus. Zudem verlangen richtige Implementierung, Unterstützung und Wartung oft umfangreiche Ressourcen. Daher gelingt es vielen Unternehmen und Institutionen nicht, das Beste aus den erworbenen Technologien für die Endgerätesicherheit herauszuholen. Falcon Complete ist ein voll gemanagter Dienst, der alle Aspekte der Endgerätesicherheit abdeckt, zu festen, kalkulierbaren Kosten.

Cybersicherheit als Wettbewerbsvorteil

Über CrowdStrike

“BREACHES STOP HERE”

EIN RADIKAL NEUER ANSATZ DER NACHWEISLICH SICHER- HEITSVERLETZUNGEN STOPPT

Besserer Schutz

Die Kombination von maschinellem Lernen, künstlicher Intelligenz, Verhaltensanalysen und präventivem Aufspüren von Bedrohungen in einer einzigen Lösung bietet Schutz über den gesamten Lebenszyklus – all das unterstützt durch Threat Graph, die größte Analyseplattform der Sicherheitsbranche in der Cloud.

Vertrauen auf CrowdStrike



254 of 500

der Fortune 500 Unternehmen



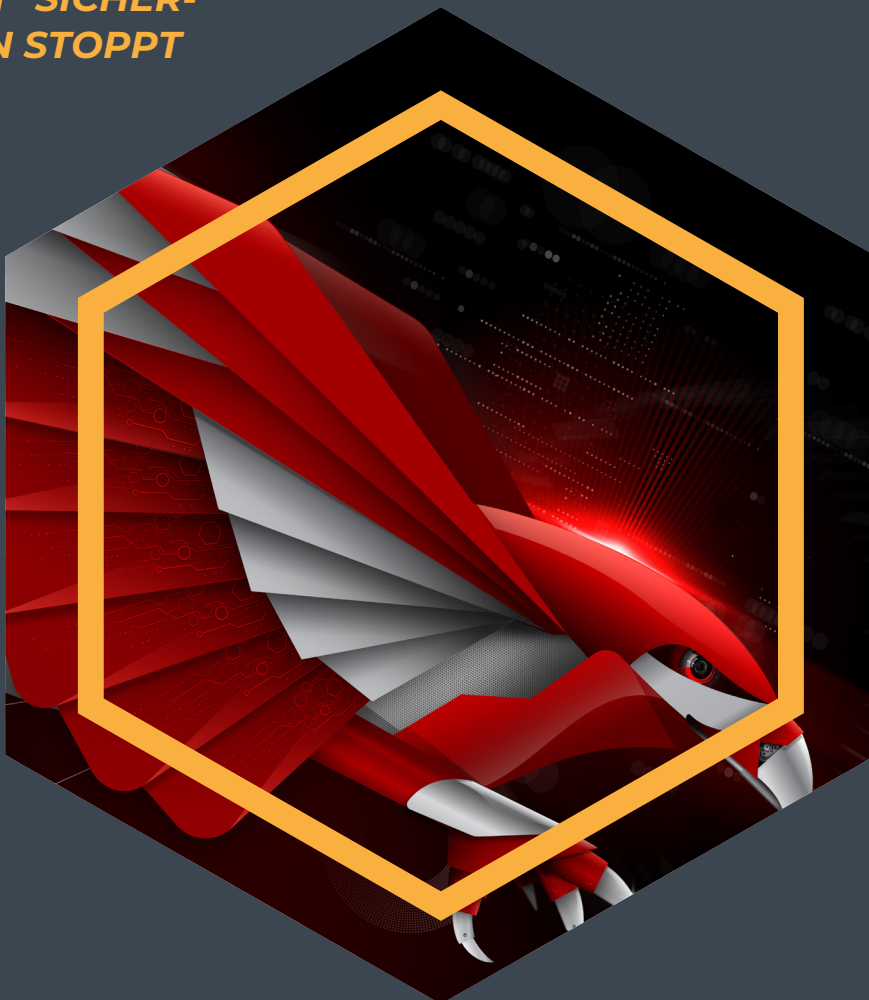
15 of the Top 20

der globalen Banken



17 of the Top 20

der wichtigsten Energieunternehmen



AV

comparatives

**99.5% BLOCKIERUNGSRATE BEI
MALWARE 100% EXPLOIT-
ERKENNUNG 0 FEHLALARME**

SE Labs

**MACHINE LEARNING ENGINE 100%
BLOCKIERUNGSRATE BEI
MALWARE KEINE FEHLALARME**

MITRE

**ATT&CK FRAMEWORK GEGNER-
EMULATION VOLLSTÄNDIGER
SCHUTZ**



**VENDOR MEMBER GRUNDLAGE:
STANDARDS GRUNDLAGE: TESTS**

CrowdStrike® Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Endgeräteschutzplattform die Sicherheit im Cloud-Zeitalter neu. Die Plattform CrowdStrike Falcon® verfügt über eine einzigartige, Cloud-basierte, schlanke Agentenarchitektur, die von künstlicher Intelligenz (KI) unterstützt wird und unternehmensweit für Schutz und Transparenz in Echtzeit sorgt. So werden Angriffe auf Endgeräte sowohl innerhalb als auch außerhalb des Netzwerks verhindert. Mit Hilfe des firmeneigenen CrowdStrike Threat Graph® korreliert CrowdStrike Falcon weltweit und in Echtzeit über 2,5 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eine der weltweit fortschrittlichsten Datenplattformen für Cyber-Sicherheit.

MDR Features

Überblick der Komponenten und Vergleich

MDR

Managed Endpoint
Detection & Response
Falcon Complete

EDR

EDR+

MDR

Endpoint Security Features

- Falcon Endpoint Protection Enterprise
- Falcon Insight EDR
- Falcon Prevent (NGAV) Application
- Falcon Device Control

- Falcon Endpoint Protection Enterprise
- Falcon Insight EDR
- Falcon Prevent (NGAV) Application
- Falcon Device Control

- Falcon Endpoint Protection Enterprise
- Falcon Insight EDR
- Falcon Prevent (NGAV) Application
- Falcon Device Control

Threat Intelligence Features

- Falcon Threat Graph Standard
-
- EDR beinhaltet kein Threat hunting durch das Overwatchteam.

- Falcon Threat Graph Standard
- Falcon Overwatch Service
- Das Team von Overwatch sucht unermüdlich nach Bedrohungen und meldet diese, sobald sie erkannt werden: Es sind die 1 % aus 1 % der Bedrohungen, die normalerweise im Verborgenen bleiben und zu Datendiebstählen führen, wenn sie nicht frühzeitig entdeckt werden.

- Falcon Threat Graph Standard
- Falcon Overwatch Service
- Falcon Complete Service
- Vollumfängliche Threatanalyse. Das Team von Overwatch sucht unermüdlich nach Bedrohungen und stoppt diese, sobald sie erkannt werden: Es sind die 1 % aus 1 % der Bedrohungen, die normalerweise im Verborgenen bleiben und zu Datendiebstählen führen, wenn sie nicht frühzeitig entdeckt werden.

Security & IT Ops Features

- Falcon Discover

- Falcon Discover

- Falcon Discover

Incident Response Features

-
-
- EDR beinhaltet keine Incident Response Features. Im Störfall übernimmt dein eigenes Administrationsteam die Identifizierung und die Beseitigung.

-
-
- EDR+ beinhaltet keine Incident Response Features. Im Störfall übernimmt dein eigenes Administrationsteam die Identifizierung und die Beseitigung.

- Falcon Complete Service
- Falcon Incident Response Service
- Falcon Complete beinhaltet den IR Service: Das IR-Team wird während der gesamten Reaktion auf den Vorfall durch das CrowdStrike Intelligence-Team unterstützt. Als Pionier in der Gegneranalyse hilft es, in der Umgebung vorhandene Gegner zu identifizieren, sodass das IR-Team den Vorfall schnell und effizient eindämmen kann.

Remediation Features

-
-
- EDR beinhaltet keine Remediation Features. Die Wiederherstellung übernimmt dein eigenes Administrationsteam.

-
-
- EDR+ beinhaltet keine Remediation Features. Die Wiederherstellung übernimmt dein eigenes Administrationsteam.

- Falcon Complete Service
- Falcon Endpoint Recovery Service
- Sofortige Beseitigung der Bedrohungsakteure und Verhinderung weiterer Versuche, die Umgebung zu kompromittieren. Schnelle Identifizierung von Persistenzvektoren und Massenbeseitigung von bösartigen Artefakten mit Schnelligkeit und Präzision. Stellen Sie den normalen Geschäftsbetrieb effizient und effektiv wieder her, ohne dass Sie Geräte neu sichern oder neu ausgeben müssen.

Breach Prevention and Warranty Features

- Individuell angepasste Cyberversicherung
- Das Restrisiko eines Cybervorfalles wird durch eine individuelle angepasste Cyberversicherung abgedeckt. Voraussetzung hierfür ist die Erfassung deines Sicherheitsstatus.

- Individuell angepasste Cyberversicherung
- Das Restrisiko eines Cybervorfalles wird durch eine individuelle angepasste Cyberversicherung abgedeckt. Voraussetzung hierfür ist die Erfassung deines Sicherheitsstatus.

- Falcon Complete Breach Warranty
- CrowdStrike bietet Falcon Complete™-Kunden eine Garantie, die bei einem Vorfall in der durch CrowdStrike Falcon Complete geschützten Umgebung bis zu \$ 1 Million für Sicherheitsverletzungsabwehrkosten abdeckt. Gewährleistungsanspruch besteht dann, wenn der Sicherheitsvorfall durch unbefugten Zugriff eines Dritten auf das Betriebssystem eines durch Falcon Complete geschützten Endgeräts in Form von Verlust, Zerstörung und/oder irreversible Verschlüsselung von Kundendaten erfolgt, von denen der Kunde vernünftigerweise annimmt, dass ihr Wert \$ 5.000 übersteigt.



MISSION:
CYBERSECURITY
POSSIBLE



Global MSSP
Partner

Diese Informationsbroschüre dient lediglich zur Information. Der Umfang oder der technische Inhalt der beschriebenen Pakete kann unter Umständen variieren. Alle Markenlogos, Informationen oder Texte wurden mit freundlicher Unterstützung der Markeninhaber oder Hersteller zur Verfügung gestellt. Die Cyberversicherung wird nach Anfrage beim Versicherer individuell berechnet. Grundvoraussetzung ist ein Fragebogen zum Sicherheitsstatus des jeweiligen Unternehmens. Änderungen und Anpassungen behalten wir uns vor.



WWW.ITELIS.COM



WIR STOPPEN CYBERBEDROHUNGEN

itelis OHG
Slavertrift 1
32657 Lemgo
info@itelis.com



100% Service
Ein Berater ist für dich da

05261.777.977