



EDR⁺

**Endpoint Detection
& Response
+Overwatch**

EDR+ | Endgeräteschutz maximiert

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.

EDR+ setzt auf CrowdStrike Threat Detection mit KI und Machine Learning und zusätzlich auf das Overwatchteam um diese Bedrohungen zu identifizieren und zu neutralisieren, bevor diese dein System in Mitleidenschaft ziehen. Deine Endpoints werden durch Threathunter und Analysten überwacht. Hier agieren echte Menschen und können Angriffsverhalten effektiv einschätzen und verfolgen. Wird ein Angriff durch das System detektiert, welcher durch die Falcon Enterprise Plattform nicht automatisch entfernt werden kann, so erhält dein Administratorenteam in Echtzeit dedizierte Angriffsinformationen durch die Threathunter und kann sofort auf die Ereignisse reagieren.

Der Angreifer hat nicht mehr die Zeit um sich in deinem Netzwerk auszubreiten. Somit werden die Cyberrisiken für dich auf ein Minimum reduziert. Das Sicherheitsniveau steigt auf ein optimiertes neues Level.

Risiken, wie Ransomware Attacken und Malwarebedrohungen werden durch die Falcon Enterprise Plattform zuverlässig erkannt und eliminiert.

Das Onboarding der EDR+ 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”
- “Permanente Bedrohungssuche. Sicherheitsexperten spüren 24/7 auf”



EDR+ - CrowdStrike

Technologie neu gedacht

EDR+

Endpoint Detection
& Response
+Overwatch

Sicherheitskomponenten perfekt kombiniert



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 Discover

Falcon Discovery gibt Antworten auf deine IT-Hygiene. Sofortige Einblicke in deine Endgeräte-Umgebung.

Du erhältst Informationen über Anwendungs- und -Ressourcenbestand in Echtzeit und für die Vergangenheit und kannst die Compliance bei Administratoren- und Benutzerkonten sicherstellen.



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 melden.

Das Overwatch Team 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 erkannt werden.



Reiner SCT Authenticator

Unknackbare TOTP 2FA Authentisierung ohne Netzwerkverbindung.



Cyberversicherung

Rundumschutz durch kombinierte zusätzliche Cyberversicherung.

Das Restrisiko trotz aller Schutztechnologien wider erwartend doch einen Cybervorfall zu bekommen, wird durch eine individuell, auf deine Bedürfnisse, abgestimmte Cyberversicherung abgefangen.

**EDR+ - Lizenzpolitik
angepasst für kleine und
mittlere Unternehmen,
und perfekt kombiniert**

Was kann **EDR+** für mich tun?

EDR+

Endpoint Detection
& Response
+Overwatch

Entwickelt zur Abwehr von Sicherheitsvorfällen

CrowdStrike Falcon® Endpoint Protection Enterprise setzt den neuen Standard in der Endgerätesicherheit. Diese Lösung beruht auf der ersten und einzigen cloud-nativen Sicherheitsplattform, die nachweislich Sicherheitsverletzungen stoppt. Sie vereint Next-Gen Antivirus (NGAV), Endgeräteerkennung und Reaktion (EDR), Managed Threat Hunting und integrierte Threat Intelligence in einem einzigen Agenten, der über die Cloud bereitgestellt wird.

Ausfälle und Störungen vermeiden

KI-UNTERSTÜTZTES NGAV | Schützt vor dem gesamten Angriffsspektrum. Kombiniert die besten Präventionstechnologien: maschinelles Lernen, KI, Angriffsindikatoren (IOAs), Exploit-Blocking und vieles mehr. Die Lösung stoppt Angriffe mit bekannter und unbekannter Malware, Ransomware, Angriffe ohne Malware oder ohne Dateien, sowie versierte und verdeckte Angriffe nationalstaatlicher Akteure. Schützt die Endgeräte vollständig online und offline.

Überblick über dein System bekommen

INTELLIGENTES EDR | Verhindert unbemerkte Ausfälle durch die Erfassung von Rohereignissen zur automatischen Erkennung bösartiger Aktivitäten bei beispielloser Transparenz, proaktiver Bedrohungssuche und forensischer Analyse. Legt den gesamten Angriff im leicht anwendbaren CrowdScore Vorfalls-Arbeitsbereich dar, angereichert mit Kontextdaten und Bedrohungsinformationen. Stellt leistungsstarke Maßnahmen zur Eindämmung, Untersuchung und Behebung kompromittierter Systeme bereit.

Deine Cybersicherheit wieder im Griff haben

INTEGRIERTE THREAT INTELLIGENCE | Schafft Klarheit über die Bedrohungslage in deiner Umgebung, sodass du Abhilfemaßnahmen auf die Schwere der Bedrohung abstimmen und priorisieren kannst. Keine Mutmaßungen, sondern gezielte Reaktion auf Bedrohungen. Ermittelt automatisch Umfang und Auswirkung der in deiner Umgebung gefundenen Bedrohungen. Stellt ein breiteres Spektrum von Gefährdungsindikatoren bereit und ermöglicht somit einen schnelleren, besseren Schutz. Dein Administratorenteam ist immer im Bild über den Sicherheitszustand deiner Endpunkte.

Sicher alle Ziele erreichen

INT24/7 MANAGED THREAT HUNTING | Ein hochkarätiges Team von Sicherheitsexperten sucht proaktiv nach Bedrohungsaktivitäten in deiner Umgebung, analysiert diese und spricht anschließend Empfehlungen aus. So ist gewährleistet, dass dir keine Warnmeldungen von hoher Priorität entgehen. Die Alarm-Priorisierung weist auf akute Bedrohungen in deiner Umgebung hin. Falsch positive Meldungen werden aussortiert. Empfohlene Gegenmaßnahmen schaffen Klarheit über Angriffe.

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



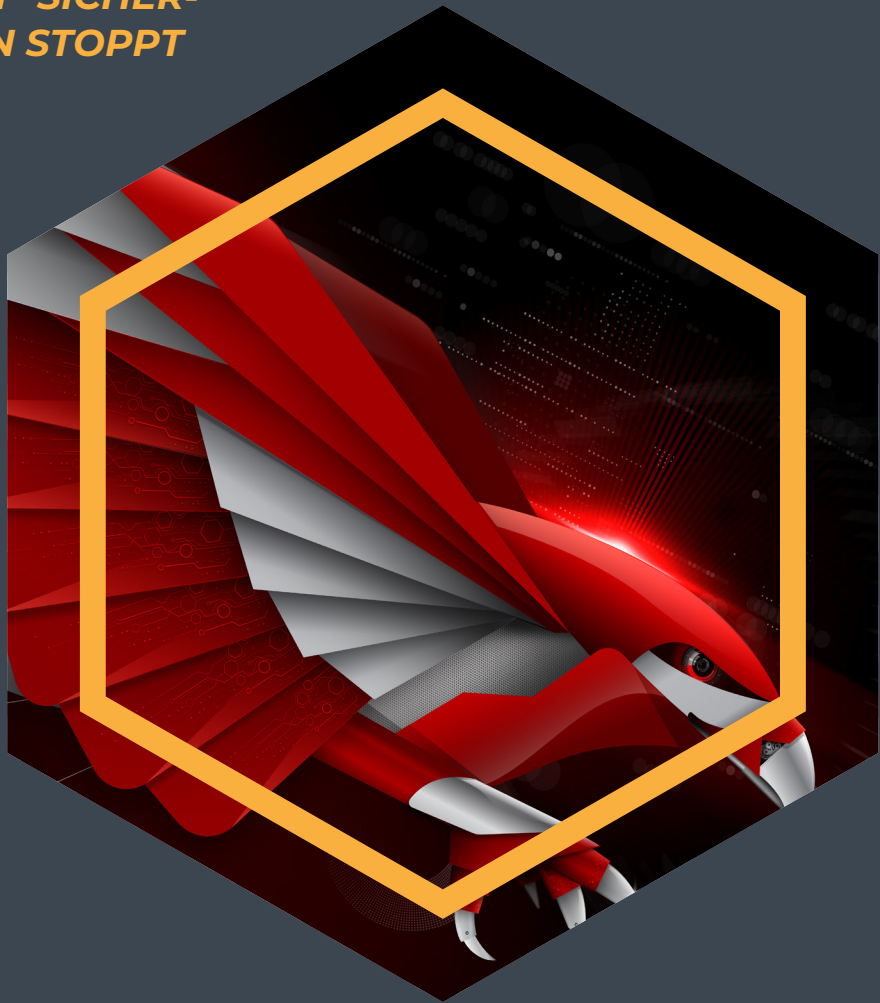
15 of the Top 20

der globalen Banken



17 of the Top 20

der wichtigsten Energieunternehmen



AV

comparatives

**99.5% BLOCKIERUNGSRATE BEI
MALWARE 100% EXPLOIT-
ERKENNUNG O 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.

EDR+ Features

Überblick der Komponenten und Vergleich

EDR+

Endpoint Detection
& Response
+Overwatch

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