CROWDSTRIKE FALCON:
DER NEUE STANDARD BEI ENDGERÄTESCHUTZ

ENDGERÄTESICHERHEIT MIT EINEM EINFACHEN UND DENNOCH LEISTUNGSFÄHIGEN ANSATZ

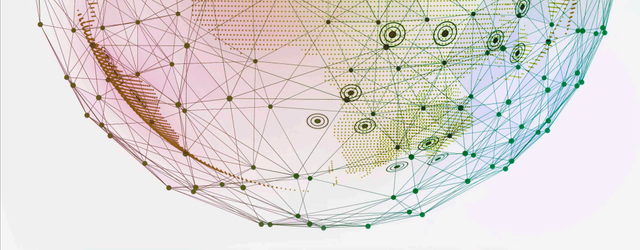
Der schlanke Agent von CrowdStrike Falcon und die leistungsstarke Cloud arbeiten nahtlos zusammen, um Echtzeitschutz und Transparenz zu bieten – **selbst dann, wenn der Agent nicht mit dem Internet verbunden ist**. CrowdStrike Falcon liefert zuverlässigen Bedrohungsschutz und kombiniert hierfür künstliche Intelligenz (KI) und Machine Learning (ML) mit hochentwickelten Funktionen für Erkennung und Reaktion sowie integrierten Bedrohungsdaten. All das wird über eine besonders intuitive Verwaltungskonsole gesteuert.

GRÜNDE FÜR CROWDSTRIKE FALCON

VOLLSTÄNDIGER SCHUTZ
Sofortige und effektive Erkennung sowie Abwehr aller Angriffstypen – mit und ohne Malware-Komponenten – unabhängig davon, ob Sie on- oder offline sind.

UNÜBERTROFFENE TRANSPARENZ
Ein „Protokollführer" für Ihre Endgeräte, der nichts übersieht. Erkennen und untersuchen Sie aktuelle und frühere Endgeräteaktivitäten innerhalb von Sekunden.

MAXIMALE BENUTZER-FREUNDLICHKEIT
Eine Cloud-basierte Plattform, die mit nur einem schlanken Agenten unkompliziert bereitgestellt, konfiguriert und gewartet werden kann.



CROWDSTRIKE: GETESTET UND BEWÄHRT

Mit CrowdStrike haben Sie die Sicherheit, dass Ihr Unternehmen zuverlässig vor bekannten ebenso wie unbekannten Cyber-Angriffen geschützt ist – egal ob mit oder ohne Malware-Komponenten. Diese Einschätzung von CrowdStrike Falcon wird von unabhängigen Experten bestätigt:

„VISIONÄR"
Gartner Magic Quadrant für Endgeräteschutz-Plattformen – Januar 2017

„STRONG PERFORMER"
Forrester Wave: Endgerätesicherheit – Oktober 2016

„GEPRÜFTES SICHERHEITSPRODUKT FÜR UNTERNEHMEN"
AV Comparatives – Dezember 2016

CROWDSTRIKE-FIRMENHAUPTSITZ
15440 Laguna Canyon Road, Suite 250, Irvine, California 92618 | +1 (888) 512-8906
info@crowdstrike.com | sales@crowdstrike.com | crowdstrike.com
Opfer einer Datenkompromittierung geworden? Kontaktieren Sie uns unter +1 (855) 276-9347 oder services@crowdstrike.com.

CROWDSTRIKE

STOPPT KOMPROMITTIERUNGEN

Cloud-basierter Endgeräteschutz

CROWDSTRIKE FALCON:
DAS „UNMÖGLICHE" MÖGLICH MACHEN

Es hieß, dass es unmöglich sei, mit einem schlanken Agenten vollständigen Endgeräteschutz zu bieten, ohne die Benutzer-Performance zu beeinträchtigen. Wir haben das Gegenteil bewiesen. Die bisher unerreichte Echtzeit-Transparenz, -Schutzwirkung und -Reaktionsfähigkeit von CrowdStrike Falcon **bietet folgende Möglichkeiten:**

➤ Verhinderung verbreiteter sowie besonders raffinierter Angriffe unabhängig davon, ob Malware eingesetzt wird und ob Ihre Endgeräte on- oder offline sind.

➤ Echtzeit-Überblick über Endgeräte und Informationen über Anwendungen sowie Prozesse, die an beliebiger Stelle in Ihrer Umgebung ausgeführt werden. So wird gewährleistet, dass keine Bedrohung übersehen wird und stets die passende Reaktion erfolgt.

➤ Proaktive Suche nach hochentwickelten Bedrohungen – schneller und effektiver als je zuvor.

➤ Schutz für Endgeräte auf allen verbreiteten Plattformen, einschließlich Endgeräten mit Windows, OS X und Linux, Rechenzentrum-Server, virtuellen Maschinen sowie Cloud-Plattformen wie AWS, Azure und Google.

➤ Wechsel von veraltetem Virenschutz zu einer Lösung der nächsten Generation, die unabhängig getestet und als effektiver Ersatz für Virenschutz zertifiziert wurde.

CROWDSTRIKE-LÖSUNGEN

FALCON DISCOVER
IT-Hygiene

Falcon Discover erkennt in Echtzeit nicht autorisierte Systeme sowie Anwendungen überall in Ihrer Umgebung und ermöglicht so schnellere Problembehebungen und damit mehr Sicherheit.

FALCON PREVENT
Virenschutz der nächsten Generation (NGAV)

Falcon Prevent schützt vor Angriffen mit und ohne Malware-Komponenten. Die Lösung wurde von unabhängigen Experten getestet sowie zertifiziert und kann herkömmlichen Virenschutz im Unternehmen ersetzen.

FALCON INSIGHT
Endgeräte-Erkennung und Reaktion (EDR)

Falcon Insight bietet kontinuierliche und umfassende Endgeräte-Transparenz – einschließlich Erkennung, Reaktion und Forensik –, damit keine Bedrohungen übersehen und potenzielle Kompromittierungen abgewehrt werden können.

FALCON OVERWATCH
Verwaltete Bedrohungssuche

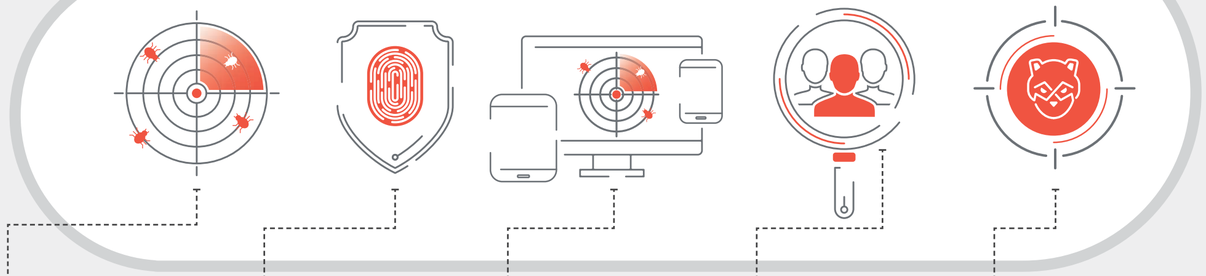
Das rund um die Uhr aktive Falcon OverWatch-Team ergänzt nahtlos Ihre internen Sicherheitsressourcen, damit schädliche Aktivitäten so früh wie möglich aufgedeckt werden und böswillige Akteure keine Chance haben.

FALCON INTELLIGENCE
Bedrohungsanalyse

Falcon Intelligence überwacht die weltweiten Aktivitäten krimineller Akteure und liefert individuelle sowie umsetzbare Berichte und Analysen, die Sie problemlos zur Verbesserung Ihrer Sicherheitslage nutzen können.

CLOUD-BASIERTER ENDGERÄTESCHUTZ

FALCON PLATFORM



IT-HYGIENE
Sie müssen auf alle Angriffsformen vorbereitet sein, aber Sie können nur das abwehren, was Sie auch sehen. Ihr Unternehmen benötigt umfassende Echtzeittransparenz, um alle verwalteten und nicht verwalteten Endgeräte zu erkennen und ein Inventar aller Anwendungen in Ihrer Umgebung zu erstellen. Nur so können Sie potenzielle Bedrohungsvektoren sofort erkennen und beseitigen.

VIRENSCHUTZ DER NÄCHSTEN GENERATION (NGAV)
Zum Schutz vor Angriffen mit und ohne Malware-Komponenten benötigen Sie umfassenden und bewährten Virenschutz der nächsten Generation, der mehrere Schutztechnologien nutzt, z. B. Machine Learning, Exploit-Blockierung sowie Verhaltensanalysen basierend auf erweiterten Angriffsindikatoren (IOA).

ENDGERÄTE-ERKENNUNG UND REAKTION (EDR)
Dank kontinuierlicher und umfassender EDR mit der Möglichkeit, aktuelle und frühere Endgeräteaktivitäten innerhalb von 5 Sekunden zu finden, kennen Sie die Ereignisse auf Ihren Endgeräten und können daher sicher sein, dass Ihnen nichts entgeht. So haben Angreifer keine Chance, sich zu verstecken.

VERWALTETE BEDROHUNGSSUCHE
Es genügt nicht, nur die am höchsten entwickelte Schutztechnologie einzusetzen. Um raffinierte Angreifer abzuwehren, benötigen Sie ein dediziertes Team, das rund um die Uhr proaktiv nach verdächtigem Verhalten sucht und bei der Identifizierung neuer und zukünftiger Bedrohungen auf den „Schwarmansatz“ setzt.

BEDROHUNGSANALYSE
Sie können nur das schützen, was Sie als gefährdet einstufen. Dank Bedrohungsanalysen verstehen Sie die Motive von Angreifern, kennen deren Vorgehensweisen und können effektive Maßnahmen implementieren, mit denen Sie erfolgreiche Kompromittierungen verhindern können.

CROWDSTRIKE-SERVICES:

INCIDENT RESPONSE SERVICES

Die umfassenden CrowdStrike-Services für Reaktionen vor und nach Zwischenfällen sind rund um die Uhr verfügbar und unterstützen Sie vor, während und nach Kompromittierungen. Diese besonders erfahrenen Teams besitzen die nötigen Kompetenzen, damit Sie Ihr Unternehmen vor Sicherheitszwischenfällen schützen, Kompromittierungen verhindern und Ihre Reaktionsgeschwindigkeit erhöhen können.

PROACTIVE SERVICES

Das Service-Team von CrowdStrike arbeitet auf Wunsch mit Ihnen zusammen, um Bedrohungen vorherzusehen, Ihr Netzwerk auf die Abwehr von Eindringungsversuchen vorzubereiten und die Möglichkeiten Ihres Teams zur Abwehr von Cyber-Angriffen zu verbessern. Proactive Services umfassen Kompromittierungsbewertung, Penetrationstests der nächsten Generation und Notfallübungen, aber auch Entwicklungsprogramme für Zwischenfallreaktionen (IR) und Sicherheitskontrollzentren (Security Operations Center, SOC).