CROWDSTRIKE

FALCON COMPLETE: BEWÄHRTE, PROFESSIONELLE MDR-LÖSUNG

DER OPTIMIERTE SCHUTZ FÜR ALLE IHRE SYSTEME ZU JEDER ZEIT

EINLEITUNG

Mangelnde Ressourcen und Fachkenntnisse im Bereich der Cybersicherheit können dazu führen, dass Organisationen sich mit der optimalen Nutzung der erworbenen Sicherheitstechnologien schwer tun. Dadurch entstehen unnötige Schwachstellen. Dies wiederum kann zu Vorfällen und daraus resultierenden Maßnahmen führen, die hätten verhindert werden können, wenn die Sicherheitstechnologien richtig konfiguriert und auf dem neuesten Stand gehalten worden wären. Oder wenn die Warnhinweise, die einem solchen Vorfall vorausgingen, frühzeitig bemerkt worden wären, um Schaden abzuwenden.

CrowdStrike® Falcon Complete™ ist eine MDR-Lösung (verwaltete Erkennung und Reaktion, die diese Herausforderungen für CrowdStrike Falcon®-Kunden löst, indem sie die Effektivität der Falcon-Plattform mit der Effizienz eines engagierten Teams von Sicherheitsexperten verbindet. Falcon Complete legt den Fokus auf die Verwaltung und Überwachung Ihrer Endgerätesicherheit und wehrt Bedrohungen mit Schnelligkeit und Präzision für Sie ab.

Falcon Complete ist die sofort einsatzfertige Lösung für Organisationen, die über keine üppigen Sicherheitsbudgets verfügen. Der Schutz vor den heutigen Bedrohungen verlangt nach der ständigen Wachsamkeit von ausgewiesenen Fachleuten. Doch die Kosten für den Aufbau eines umfassenden Sicherheitsprogramms, das rund um die Uhr mit Sicherheitsexperten besetzt ist, können viele Organisationen nicht stemmen. Aber selbst für Organisationen, die über die finanziellen Mittel für interne Programme verfügen, ist der Rückgriff auf das Falcon Complete Team oft der schnellste und einfachste Weg zu einem umfassenden und ausgereiften Endgerätesicherheitsprogramm.

CrowdStrike ist von Falcon Complete so überzeugt, dass wir eine Garantie in Höhe von bis zu 1 Million US-Dollar gegen Datendiebstahl[1] in einer von uns geschützten Umgebung abgeben.

Falcon Complete ist eine Ergänzung zu Ihrer Investition in die Falcon-Technologie. Mit den engagierten Fachleuten und ausgereiften Prozessen, die Sie benötigen, um Sicherheitsverletzungen zu stoppen, wo und wann immer sie auftreten.

Dieses Whitepaper geht den Herausforderungen an eine optimale Nutzung Ihrer Endgerätesicherheitslösung nach und zeigt auf, wie das Team von Falcon Complete in besonderer Weise geeignet ist, diese Herausforderungen zu lösen.

> **Falcon Complete legt den Fokus auf die Verwaltung und Überwachung Ihrer Endgerätesicherheit und wehrt Bedrohungen mit Schnelligkeit und Präzision für Sie ab.**

1 Es gelten Einschränkungen. Einzelheiten entnehmen Sie bitte den Falcon Complete FAQ zur Garantie gegen Sicherheitsverletzungen.

GEMEINSAME HERAUSFORDERUNGEN ZUR OPTIMIERUNG DER SICHERHEITSAUFSTELLUNG

Unternehmen und Institutionen stehen bei der Implementierung eines Endgeräte-sicherheitsprogramms üblicherweise vor einigen Herausforderungen, die den Einsatz von MDR-Diensten – wie Falcon Complete – sinnvoll machen:

- **Schwierigkeiten bei der Handhabung der Technologie.** Jede Sicherheitslösung erfordert ein regelmäßiges proaktives Management, wenn ein angemessener Schutz erreicht werden soll. Nur so ist sichergestellt, dass die Lösung richtig eingesetzt und richtig konfiguriert wird und alle Endgeräte schützen kann. IT-Teams verfügen jedoch oft nicht über die dafür nötigen Tools oder Personalstärke. Außerdem fehlen ggf. Zeit und Erfahrung, um die Sicherheitsrichtlinien so zu konfigurieren, dass sie den gegebenen Anforderungen entsprechen und dass die Endgeräte wirklich geschützt sind. Dies kann dazu führen, dass die Endgerätelösung nur unvollständig bereitgestellt und lückenhaft konfiguriert wird, was die Organisation anfällig für Sicherheitsverletzungen macht.

- **Mangelndes Vermögen, zuverlässig und rechtzeitig auf Bedrohungen zu reagieren und Sicherheitsverletzungen zu verhindern.** Sicherheitswarnungen weisen auf mögliche Bedrohungen hin, sodass das IT-Team rechtzeitig reagieren kann, bevor der Schaden eintritt. Diese Warnungen nutzen aber nur dann, wenn sie von Fachleuten früh genug gelesen und überprüft werden. Der Umgang mit Warnmeldungen erfordert Zeit, Energie und Fachwissen. Diese wichtigen Sicherheitsressourcen stehen vielen Organisationen gar nicht zur Verfügung. Der Umgang mit der oft großen Zahl von Alarmen, die von einer Endgerätesicherheitslösung erzeugt werden, kann selbst Unternehmen überfordern, die ein eigenes Sicherheitsteam oder ein SOC (Security Operation Center) unterhalten. Die damit verbundenen Ermüdungserscheinungen führen dazu, dass Alarme nicht ausgewertet werden, was Angreifern Tür und Tor öffnet.

- **Schwierigkeiten bei der ordnungsgemäßen Behebung von Sicherheitsvorfällen.** Die schnelle und zielgerichtete Behebung von Vorfällen verlangt Fertigkeiten und Erfahrung. Doch verfügen viele Organisationen weder über die Zeit noch das Fachwissen, um Art und Ausmaß eines Vorfalls vollständig zu analysieren, sobald sich dieser ereignet. Das kann dazu führen, dass Mitarbeiter aus IT und Sicherheit wochenlang versuchen, einen Vorfall zu bereinigen, dabei unnötige und aufwendige Maßnahmen durchführen, wie beispielsweise ein Re-Imaging, und schließlich davon ausgehen, dass die Umgebung bereinigt wurde, obwohl das nicht der Fall ist.

> **“Bis 2024 werden 25 % der Organisationen MDR-Dienste in Anspruch nehmen, gegenüber weniger als 5 % derzeit. Bis 2024 werden 40 % der mittelständischen Unternehmen MDR-Dienste als einzigen verwalteten Sicherheitsdienst nutzen.”**
>
> **Gartner Research**
> Market Guide for Managed Detection and Response Services, 15. Juli [2]

2 Craig Lawson, Toby Bussa, Sid Deshpande, Pete Shoard, Kelly Kavanagh, „Market Guide for Managed Detection and Response Services“ 15. Juli 2019

DAS TEAM VON FALCON COMPLETE: ADMINISTRATION, ÜBERWACHUNG UND REAKTION DURCH FACHLEUTE – 24/7

Falcon Complete ergänzt die bewährten Schutztechnologien von CrowdStrike mit den Mitarbeitern, dem Know-how und den Prozessen, die für eine praxisorientierte Endgerätesicherheit erforderlich sind.

Falcon Complete baut auf der CrowdStrike Falcon-Plattform auf und ist die umfassendste Lösung von CrowdStrike für den Endgeräteschutz. Die Lösung bietet unübertroffene Sicherheit, indem sie Falcon Prevent™ als Virenschutz der neuesten Generation (NGAV), Falcon Insight™ für die Endgeräteerkennung und Reaktion (EDR) und Falcon OverWatch™ für die verwaltete Bedrohungssuche mit dem Fachwissen und dem 24/7-Einsatz des Teams von Falcon Complete ergänzt. Das Team verwaltet und überwacht aktiv die Falcon-Plattform für Kunden und behebt bei Bedarf Vorfälle per Fernzugriff. Das Team von Falcon Complete implementiert und unterhält ein effektives und ausgereiftes Endgerätesicherheitsprogramm, ohne dass der Kunde mit den Schwierigkeiten, dem Aufwand und den Kosten kämpfen muss, die mit dem internen Aufbau eines solchen Programms verbunden wären.

EIN HOCHQUALIFIZIERTES UND MOTIVIERTES TEAM

Das Team von Falcon Complete ist für die Verwaltung und Überwachung der Falcon-Plattform sowie für die Reaktion auf erkannte Bedrohungen zuständig. Es setzt sich zusammen aus Sicherheitsfachleuten, die Erfahrung in der Behandlung von Vorfällen, der Reaktion auf Vorfälle, der Forensik, der SOC-Analyse und der IT-Administration haben. Das Team ist weltweit präsent. Die Mitglieder sitzen in den Vereinigten Staaten, in Großbritannien und in Australien, was eine echte 24/7-Abdeckung ermöglicht.

Dank der jahrelangen Erfahrung mit Zwischenfällen und der Reaktion darauf konnten diese Fachleute ihre Fähigkeiten ständig verbessern. Das macht sie ebenso hocheffizient wie effektiv. Da sich die Teammitglieder kontinuierlich auf die Verwaltung der Falcon-Plattform konzentrieren, haben sie eine Art „Muskelgedächtnis“ entwickelt, das für die schnelle Triage und Reaktion auf Bedrohungen erforderlich ist. Dies ist ein wichtiger Faktor, der sie von anderen Sicherheitspraktikern unterscheidet, die ggf. viele Funktionen ausfüllen müssen und mit einer Unzahl von IT-Zuständigkeiten und Sicherheitstechnologien betraut sind, sodass sie einen bestimmten Bereich oft gar nicht umfassend beherrschen können.

Tatsächlich haben sich viele der Teammitglieder dafür entschieden, dem Falcon Complete Team beizutreten, weil sie dort ihre Fähigkeiten täglich anwenden und verfeinern können, was bei der Arbeit für eine einzige Organisation nicht immer möglich ist. Die Mitglieder des Teams von Falcon Complete können sich auf die Tätigkeiten konzentrieren, die ihnen am besten zusagen, wie beispielsweise die Bearbeitung von Vorfällen, die Malware-Analyse oder die Beseitigung von Bedrohungen. Dieses Umfeld ist auch der Grund, warum CrowdStrike die besten Talente aus aller Welt anzieht und auch hält.

Alle Mitglieder des Teams sind nach CCFA und CCFR zertifiziert. Das macht sie äußerst versiert im Umgang mit der Falcon-Plattform und bestens vertraut mit deren Werkzeugen und der Datenstruktur. Es weiß daher, wie eine schnelle Triage durchzuführen ist. Vielen Kunden ist dies gar nicht möglich, weil sie nicht über die nötige Erfahrung oder Intuition verfügen.

Das Falcon Complete Team pflegt zudem eine enge Beziehung zu anderen Sicherheitsfachleuten von CrowdStrike. Die Zusammenarbeit mit dem CrowdStrike Intelligence Team eröffnet den Zugang zu einem großen Pool an Informationen über Cyber-Bedrohungen. Der Zugang zu diesen Echtzeitinformationen hat viele Vorteile: Schnellere, präzisere und zeitnahe Entdeckungen; die Antizipation möglicher Angriffe; die Formulierung detaillierterer und umfassenderer Empfehlungen und die bessere Behandlung, Lösung und Behebung von Vorfällen.

DAS TEAM VON FALCON COMPLETE

Die Fachleute für die CrowdStrike Falcon-Plattform: CrowdStrike Certified Falcon Responder (CCFR) und CrowdStrike Certified Falcon Administrator (CCFA)

Die Fachleute für die Abwehr von Sicherheitsvorfällen: Mehrjährige Erfahrung in der digitalen Forensik und in der Abwehr von Sicherheitsvorfällen

Immer wachsam — 24/7/365

VERWALTUNG, ÜBERWACHUNG UND REAKTION AUF BEDROHUNGEN

Das Team von Falcon Complete ist in drei Hauptbereichen tätig: Verwaltung der Falcon-Plattform, Überwachung der Plattform und Reaktion auf Bedrohungen. Gemeinsam ergibt sich daraus eine umfassende Sicherheit ab dem ersten Tag.

Onboarding: Eine echte Partnerschaft mit Ihnen

Ein Falcon Complete-Kunde zu werden, ist ein schneller und effizienter Prozess und dauert für ein typisches Unternehmen nur wenige Tage. Der Onboarding-Prozess beginnt damit, dass das Falcon Complete Team gemeinsam mit Ihnen die geeignete Sicherheitsaufstellung für Ihre Umgebung bestimmt und in einem „Betriebsmodell" dokumentiert. Das Betriebsmodell hält schriftlich fest, wie Falcon konfiguriert werden muss und wie das Team nach den Vorstellungen des Kunden auf Bedrohungen reagieren soll. Es bestimmt, wie das Team erkannte Bedrohungen priorisiert und wie es unter bestimmten Umständen darauf reagiert oder Probleme an Sie zur Genehmigung eskaliert. Dadurch ist die Koordination zwischen dem Team von Falcon Complete und Ihnen gewährleistet – ebenso wie die Transparenz der Zuständigkeiten.

Damit Ihre Sicherheitsaufstellung ermittelt werden kann, erhalten Sie eine kurze Checkliste, die die gewünschte Sicherheitsstrategie und Ihre wichtigsten Anliegen aus übergeordneter Sicht aufzeigt. Das Falcon Complete Team setzt diese Informationen in die passende Sicherheitsaufstellung um, einschließlich der Konfiguration der Falcon-Plattform.

Zur schnellen und unkomplizierten Gestaltung dieses Prozesses spricht das Falcon Complete Team grundlegende Empfehlungen aus. Diese Empfehlungen beziehen sich auf verschiedene Ebenen der Sicherheitsaufstellung: aktiv, moderat oder vorsichtig.

- **Aktiv** bedeutet, dass die Präventionsrichtlinien der Falcon-Plattform recht restriktiv sind. Diese Richtlinien folgen den Empfehlungen von CrowdStrike und den vordefinierten Plänen mit festgelegten Gegenmaßnahmen, zu denen der Kunde das Falcon Complete Team autorisiert hat, wenn Bedrohungen in der Umgebung des Kunden festgestellt werden. Bei einer aktiven Sicherheitsaufstellung ist die Prävention also eingeschaltet, sodass das Team im Falle eines Falles unverzüglich und aus der Ferne reagieren kann.
- Bei der **moderaten** Sicherheitsaufstellung sind einige Präventionsrichtlinien nicht eingeschaltet, aber das Team kann trotzdem einige vordefinierte Maßnahmen ergreifen, mit Ausnahme von Reaktionen, die für die IT disruptiv wirken können, wie beispielsweise das Trennen (Isolieren) eines Geräts.
- Bei einer **vorsichtigen** Sicherheitsaufstellung überwacht das Team lediglich erkannte Bedrohungen. Hier sind nur die Präventionen mit höchstem Konfidenzniveau aktiviert. Bei einem Vorfall ergreift das Team nicht automatisch Abhilfemaßnahmen. Dies ist eine Option für Bereiche des Netzwerks, in denen der Kunde möchte, dass das Falcon Complete Team nicht tätig wird.

Anhand dieser einfachen Wahlmöglichkeiten kann das Team eine maßgeschneiderte Endgerätesicherheitsstrategie erstellen und verschiedene Aufstellungen auf verschiedene Teile der Umgebung anwenden. Die Organisation könnte beispielsweise eine aggressive Sicherheitsaufstellung zum Schutz ihrer Arbeitsplätze wünschen, denn von dort kommen die meisten Warnungen und dort beginnen die meisten Eindringversuche. Möglicherweise wünscht der Kunde aber für bestimmte Systeme aufgrund interner Anforderungen an das Änderungsmanagement oder anderer Bedenken eine vorsichtigere Sicherheitshaltung. Zur Implementierung eines solchen maßgeschneiderten Modells kann das Falcon Complete Team in Zusammenarbeit mit dem Kunden die Umgebung logisch gruppieren.

Alle diese Eingaben werden während des Onboarding-Prozesses gesammelt. Zum Abschluss dieses Prozesses erstellt das Team ein Betriebsmodell, mit einer definierten Sicherheitshaltung, die auf Ihre Organisation zugeschnitten ist. Das Team ergreift dann die zur Umsetzung des Modells erforderlichen Maßnahmen. Es konfiguriert beispielsweise die Präventionsrichtlinien oder definiert die Gegenmaßnahmen, die das Team in verschiedenen Situationen ergreifen wird. Das Onboarding kann bei den meisten Organisationen innerhalb weniger Tage abgeschlossen werden.

> **„Für ein typisches Unternehmen ist das Onboarding schnell und effizient und dauert nur wenige Tage. "**

Fortlaufende Verwaltung:
Der oben beschriebene Prozess ist keine einmalige Angelegenheit. Ihre Anforderungen können sich ändern. Auch das Produkt selbst entwickelt sich weiter. Das Team trifft sich daher regelmäßig mit Ihnen. So ist sichergestellt, dass das Betriebsmodell und seine Umsetzung stets auf dem neuesten Stand bleiben. Dabei behält das Team Veränderungen in Ihrer Umgebung sorgfältig im Auge. Wird beispielsweise der Falcon-Agent auf neuen Endgeräten implementiert, dann prüft und gewährleistet das Falcon Complete Team, dass geeignete logische Gruppen zur Verwaltung dieser Endgeräte vorhanden sind und dass die Endgeräte den Gruppen korrekt zugeordnet werden. So ist sichergestellt, dass neue Agents den richtigen Gruppen hinzugefügt werden und dass darauf die vereinbarten Präventionsmaßnahmen angewandt werden.

Zudem sucht das Team nach nicht verwalteten Geräten und zugehörigen Risiken. Hierzu setzt es die Falcon Discover™-Technologie als Teil von Falcon Complete ein. Änderungen in der Anzahl der eingesetzten Endgeräte, wie z. B. umfangreiche Neuinstallationen, werden ebenfalls überwacht. Zudem wird regelmäßig überprüft, ob alle Agents auf dem neuesten Stand sind und ob die richtigen Präventionsstrategien angewendet werden. Das gewährleistet zu jeder Zeit eine intakte Agent-Population und ein optimales Schutzniveau.

“

Eine regelmäßige Überprüfung, ob alle Agents auf dem neuesten Stand sind und ob die richtigen Präventionsstrategien angewendet werden, gewährleistet zu jeder Zeit eine intakte Agent-Population und ein optimales Schutzniveau.

Die Verwaltung der Falcon-Plattform ohne und mit Falcon Complete

Ohne Falcon Complete	Mit Verwaltung durch das Falcon Complete Team
• Probleme mit der Sichtbarkeit und Kontrolle nicht verwalteter Systeme • Ungeschützte, exponierte Systeme bleiben an den Rändern unbemerkt	• Umfassende Kontrolle nicht verwalteter Systeme • Falcon Complete unterstützt den Kunden dabei, dass alle Assets richtig gruppiert, eingeordnet und geschützt sind
• Verzögerungen bei der Aktualisierung der Falcon-Agents • Maschinen mit einem veralteten Falcon-Agent arbeiten möglicherweise nicht mit den neuesten Schutztechniken	• Enge Kontrolle über den Falcon-Agent • Falcon Complete stellt sicher, dass der aktuelle Falcon-Agent installiert ist, und bietet so den besten verfügbaren Schutz
• Zahlreiche Richtlinien ohne einheitliche Anwendung • Im Laufe der Zeit entwickelt sich ein Flickenteppich von Richtlinien. Das schafft Unklarheiten, erschwert die Untersuchung zu Bedrohungen und hinterlässt möglicherweise gefährliche Schutzlücken	• Rigoroses Konfigurationsmanagement • Bewährte Richtlinien nach Best Practices werden systematisch auf alle Systeme angewandt
ERGEBNIS: individuell abgestimmter Schutz für alle Ihre Systeme zu jeder Zeit	

Überwachen der Falcon-Plattform

Das Team von Falcon Complete überwacht die Falcon-Plattform 24 Stunden am Tag und sieben Tage die Woche auf neue Sicherheitswarnungen. Jede Entdeckung, unabhängig vom Schweregrad, wird vom Team untersucht. Eine Priorisierung setzt die Kenntnis der ursprünglichen Quelle der Erkennung voraus. Wenn die Machine Learning Engine von Falcon beispielsweise feststellt, dass eine Datei bösartig ist, untersucht das Team, wann diese Datei zum ersten Mal auf das Endgerät gebracht wurde und welcher Prozess sie in das System geschrieben hat. Das Team verfolgt dann den Prozessbaum zurück, um herauszufinden, wie die Ereigniskette gestartet wurde, welches Benutzerkonto mit diesen Prozessen verbunden war und wie der Benutzer angemeldet war. Das Team untersucht, ob sich die bösartige Datei auch auf anderen Systemen befand, um festzustellen, ob der Angriff mehrere Endgeräte getroffen hat oder auf ein Gerät beschränkt ist. Diese Fragen klärt das Team in den ersten Minuten nach einer Entdeckung.

Es profitiert dabei von seinem direkten Zugang zu anderen CrowdStrike-Teams. So arbeitet das Falcon Complete Team eng mit Falcon OverWatch zusammen – dem Team, das für die proaktive Suche nach Bedrohungen zuständig ist. Es nutzt zudem seine internen Beziehungen zu CrowdStrike Services, CrowdStrike Intelligence und CrowdStrike Support. Bei jeder Entdeckung kann das Team somit einen schnellen und effektiven Prozess der Triage, Eindämmung, Beseitigung und Wiederherstellung verfolgen.

Dieser effiziente und umfassende Prozess ermöglicht es dem Team, jede Erkennung zu behandeln und verlässlich festzustellen, ob es sich um einen falsch-positiven Befund handelt, ob der Vorfall auf ein einziges Endgerät beschränkt ist oder ob bereits eine Weiterverbreitung stattgefunden hat. Diese Erkenntnisse bestimmen die weitere Vorgehensweise des Teams.

Das Team von Falcon Complete überwacht die Falcon Plattform 24 Stunden am Tag und sieben Tage die Woche auf neue Sicherheitswarnungen. Jede Entdeckung, unabhängig vom Schweregrad, wird vom Team untersucht.

Überwachen ohne und mit Falcon Complete

Ohne Falcon Complete	Mit Überwachung durch das Falcon Complete Team
• 8 Stunden/Tag aktive Überwachung • Angreifer halten sich nicht an Geschäftszeiten oder Feiertage. Bedrohungen, die außerhalb der Geschäftszeiten auftreten, werden nicht selten erst am nächsten Arbeitstag bearbeitet	• 24 Stunden/Tag aktive Überwachung • Die Überwachung durch Falcon Complete erfolgt ständig. So ist sichergestellt, dass aufkommende Bedrohungen unverzüglich in Echtzeit bearbeitet werden
• Die Mehrzahl der Entdeckungen bleibt ungeprüft • Weniger schwere Entdeckungen, u. a. erfolgreich blockierte Malware, werden oft ignoriert, sind jedoch potenziell ein Zeichen für künftige Angriffe	• Jede Entdeckung wird von Fachleuten geprüft • Falcon Complete untersucht alle kritischen, hoch-, mittel- und niedrigschwelligen Entdeckungen zeitnah und stellt sicher, dass Eindringversuche zum frühestmöglichen Zeitpunkt erkannt werden
• 6 Stunden: Durchschnittliche Zeit bis zur Reaktion[3] • Die Reaktion verzögert sich, weil den Teams oft das notwendige Wissen, die Bedrohungsinformationen und die Erfahrung fehlen	• 10 Minuten: Durchschnittliche Zeit bis zur Reaktion[4] • Falcon Complete erstellt und aktualisiert einen systematischen Musterleitfaden, damit sichergestellt ist, dass alle Bedrohungen schnell und effizient untersucht werden
ERGEBNIS: Bedrohungsüberwachung durch Experten rund um die Uhr und Reaktion auf Angriffe innerhalb weniger Minuten bei deren Auftreten	

3 Vanson Bourne, „The 2019 Global Security Attitude Survey“, November 2019

4 Mittlere Zeit von Falcon Complete für die Untersuchung und Reaktion auf Sicherheitsvorfälle, gemessen über die erste Jahreshälfte 2020. Individuelle Untersuchungs- und Antwortzeiten können abweichen.

Reaktion auf Bedrohungen

Der dritte Bereich, den das Falcon Complete Team bearbeitet, betrifft die Reaktion auf Bedrohungen. Wenn ein Ereignis mit kritischem, hohem oder mittlerem Schweregrad erkannt wird, prüft das Team zunächst, dass es sich um eine wirkliche Bedrohung handelt.

Stellt das Team fest, dass kein Fehlalarm vorliegt, folgt es dem mit dem Kunden entwickelten Musterleitfaden und reagiert gemäß den Anforderungen. Dazu können Eindämmungsmaßnahmen zählen, wie das Blockieren eines Hashwerts oder des Netzwerks, in dem sich das betroffene Gerät befindet. Dank dem Falcon-Agent können diese Maßnahmen unverzüglich ergriffen werden. Falls erforderlich, macht sich das Team an die Behebung. Dabei kann es aus der Ferne auf ein Endgerät mit dem Ziel zugreifen, einen laufenden Angriff zu unterbrechen, ein kompromittiertes Endgerät zu bereinigen oder Malware-Artefakte zu entfernen. Das ist ein entscheidender Vorteil für den Kunden. Denn das Team weist nicht nur auf ein Problem hin. Vielmehr löst das Falcon Complete Team das Problem vollständig, sodass sich der Kunde nicht darum zu kümmern braucht. Das erspart ihm beispielsweise das Re-Imaging von Systemen.

Falls es sich um eine Falschmeldung handelt, sorgt das Team dafür, dass keine unnötigen Aktionen ausgelöst werden. Hier wird für jeden Kunden und jede Lage der beste Ansatz gewählt. So ermittelt das Falcon Complete Team beispielsweise, ob Whitelisting, Ausschlüsse oder die Zusammenarbeit mit dem CrowdStrike Support und dem Security Response Team geboten ist, damit neue Muster erstellt und künftig keine weiteren Falschmeldungen ausgelöst werden.

> **“**
>
> **Das Falcon Complete Team löst das Problem vollständig, sodass sich der Kunde nicht darum zu kümmern braucht. Das erspart ihm beispielsweise das Re-Imaging von Systemen.**

Reaktion ohne und mit Falcon Complete

Ohne Falcon Complete	Mit Reaktion durch das Falcon Complete Team
• 6-8 Stunden: Zeitaufwand der IT für ein Re-Imaging des Systems • Re-Imaging ist die gängigste Abhilfe – zuverlässig, aber arbeitsintensiv	• 45 Minuten: Zeitaufwand für die Durchführung der Präzisionsbereinigung[4] • Die Experten von Falcon Complete führen präzise Eingriffe aus der Ferne durch; ein Re-Imaging kann oft entfallen
• 6-8 Stunden: Ausfallzeit für Endbenutzer aufgrund von Re-Imaging • Re-Imaging ist nicht nur teuer, sondern beeinträchtigt auch die Benutzerproduktivität stark und kann wertvolle forensische Beweise vernichten	• 0 Minuten: Normalerweise keine Ausfallzeit für den Endbenutzer während der Präzisionsbereinigung • Das Falcon Complete Team kann oft Abhilfemaßnahmen durchführen, ohne dass die Benutzer überhaupt etwas davon mitbekommen
• Ungewissheit • Sobald die erste Reaktion abgeschlossen ist, muss sich die IT möglicherweise mit dem nächsten Vorfall beschäftigen, ohne sicherstellen zu können, dass die Bedrohung nicht wiederkommt	• Vertrauen • Falcon Complete führt bei jedem Eindringversuch eine umfassende Analyse durch und ermöglicht so eine vollständige und abschließende Bereinigung, unterstützt durch die CrowdStrike-Garantie gegen Sicherheitsverletzungen
ERGEBNIS: Präzisionsmaßnahmen beseitigen Bedrohungen schnell und abschließend	

Falcon Complete oder MSS-Provider?

Viele Organisationen stellen sich die Frage: „Brauche ich Falcon Complete überhaupt, wenn ich doch mit einem Managed Security Service Provider (MSS-Provider) arbeite?“ Das Leistungsangebot von MSS-Providern kann sehr unterschiedlich sein. Im Allgemeinen widmen sich diese Provider der umfassenden Überwachung und Verwaltung von Sicherheitswerkzeugen in einem Unternehmen. Dazu gehört üblicherweise die grundlegende Priorisierung von Sicherheitswarnungen zusammen mit einer Vielzahl anderer Services, wie Technologie-Management und -Upgrades, Compliance und Schwachstellenmanagement.

Falcon Complete beruht auf einem völlig anderen Schwerpunkt. Falcon Complete ist eine schnelle, sofort einsatzfertige integrative Lösung, die sich durch höchste Fachkompetenz für die CrowdStrike Falcon-Plattform auszeichnet. Die Mission von Falcon Complete zielt konsequent darauf ab, Bedrohungen zu überwachen und abzuwehren. Und das mit maximaler Effektivität und in kürzester Zeit. Aufgrund dieser Fokussierung bietet Falcon Complete einen sofortigen Nutzen zu geringen Kosten innerhalb eines sehr kurzen Zeitfensters – mit der branchenweit umfassendsten Garantie gegen Sicherheitsverletzungen.

“

Die Mission von Falcon Complete zielt konsequent darauf ab, Bedrohungen zu überwachen und abzuwehren. Und das mit maximaler Effektivität und in kürzester Zeit.

Falcon Complete vs. MSS-Provider

Phase	Aktivität	Falcon Complete	MSS-Provider
Verwalten	Fachleute für die CrowdStrike Falcon-Plattform	x	
	Unterstützt bei der Identifizierung und Beseitigung nicht verwalteter Systeme	x	
	Sorgt für aktuelle Version der Falcon-Sensoren an geschützten Endpunkten	x	
	Konfiguriert und optimiert kontinuierlich die Falcon-Richtlinien	x	
	Gewährleistet, dass alle Systeme ordnungsgemäß gruppiert und durch die Falcon-Plattform hinreichend geschützt sind	x	
	Umfasst proaktive Check-ins und Reporting	x	x
Überwachen	Überwachung der Falcon-Plattform 24/7/365	x	x
	Untersucht kritische und hochsensible Erkennungen	x	x
	Untersucht Erkennungen von mittlerer und geringer Schwere	x	?
	Umfasst eine proaktive Bedrohungssuche durch Fachleute	x	?
	Profitiert vom Zugriff auf die Experten von CrowdStrike Intelligence und OverWatch	x	
Abwehren	Bestimmt die Abwehrstrategie	x	x
	Berät zu Abwehrmaßnahmen	x	x
	Isoliert kompromittierte Systeme proaktiv	x	
	Führt gezielte Abhilfemaßnahmen durch	x	
	Erstellt nach dem Eindringversuch eine Zusammenfassung mit Sicherheitsempfehlungen	x	
	Stellt Service-Level-Agreements (SLAs) für Untersuchung und Reaktion bereit	x	x
	Umfasst eine Garantie gegen Sicherheitsverletzungen	x	

SOFORTIGE PRAKTISCHE UNTERSTÜTZUNG FÜR UNSERE KUNDEN

AUF ANHIEB EINSATZBEREIT

Die Verwaltung aller Aspekte der Endgerätesicherheit durch CrowdStrike hat einen ganz offensichtlichen Vorteil: Time-to-Value. Unternehmen und Institutionen, die versuchen, ein Security Operations Center in Eigenregie aufzubauen, das schnell und effektiv auf Bedrohungen reagiert und diese beseitigt, wissen, dass der Weg dahin lang, komplex und teuer ist. Von der Suche und Einstellung des geeigneten Personals und dem Erwerb der entsprechenden Technologie bis hin zur Festlegung von Richtlinien und der Definition von Prozessen zur Reaktion auf Vorfälle können Monate, wenn nicht Jahre vergehen.

Zudem wird derartigen Programmen oft eine geringere Priorität eingeräumt als anderen dringenden IT-Projekten. Das führt zu langwierigen Implementierungen und macht Organisationen verwundbar. Auch die Kosten können ein Thema sein. Für die personelle Abdeckung eines Betriebs rund um die Uhr sind mindestens vier Vollzeitbeschäftigte erforderlich. Das macht die erforderliche Sicherheitsreife für viele Unternehmen unerreichbar. Und für diejenigen, die tatsächlich über diese Mittel verfügen, ist es immer noch eine Herausforderung, das notwendige Fachwissen zu finden und zu halten. Einen Mitarbeiter zu rekrutieren, zu schulen und zu halten, der ausreichend qualifiziert ist, um gegen die versierten und hochgerüsteten Gegner zu bestehen, mit denen Organisationen heute konfrontiert sind, kann enorm schwierig werden. Schließlich leidet die Branche im Allgemeinen ohnehin unter einem Mangel an qualifizierten Sicherheitsexperten.

Im Unterschied dazu zeichnet sich das Falcon Complete Team durch sofortige Time-to-Value aus: Der Kunde profitiert auf Anhieb von erfahrenen Sicherheitsexperten, die mit seinen Spezialisten zusammenarbeiten und die Verwaltung der Falcon-Plattform für den Endgeräteschutz übernehmen. Für jeden neuen Kunden erarbeitet das Falcon Complete Team Empfehlungen und ein erprobtes Betriebsmodell. Das umfasst einen maßgeschneiderten Musterleitfaden und ein voll einsatzfähiges 24/7-Team. Dessen Arbeit kann beginnen, sobald das Onboarding des Kunden abgeschlossen ist.

ERGEBNISSE STATT HAUSAUFGABEN

Ein weiterer wichtiger Vorteil des Falcon Complete Teams ist die Fernbehebung. Wenn Endgeräte kompromittiert werden, ergreift das Falcon Complete Team gezielt Maßnahmen zur Lösung des Vorfalls, ohne dass sich der Kunde darum kümmern muss. Diese besonderen Fähigkeiten ermöglichen es dem Team, effizient, schnell und sicher auf Zwischenfälle zu reagieren. Viele Organisationen tun sich derart schwer, solche Fähigkeiten zu entwickeln, dass sie lieber ein komplettes Re-Imaging ihrer Systeme einplanen, falls diese als infiziert oder kompromittiert gelten.

Ein Re-Imaging kann eine effektive Lösung sein, ist aber auch kostspielig. Darüber hinaus ist es sowohl für IT-Abteilungen als auch für die Endbenutzer mit empfindlichen Belastungen bzw. zeitlichen Einbußen verbunden, wenn sie ihre Notebooks beim Helpdesk abgeben. Der Helpdesk ist seinerseits gezwungen, viel Zeit für das Re-Imaging aufzuwenden, damit die Endgeräte wieder als vertrauenswürdige Arbeitsumgebung dienen können.

Auch hier zahlt sich die hohe Kompetenz des Falcon Complete Teams aus: Es analysiert den Umfang und die Details eines Vorfalls vollständig und schnell und schafft zuverlässig Abhilfe, ohne sozusagen als Standardlösung auf ein Re-Imaging zu verweisen.

Das Team führt die zum Verständnis des Vorfalls erforderlichen Analysen durch. Handelt es sich beispielsweise um eine Malware-Infektion oder ist es ein Angreifer, der in der Umgebung eine versteckte Hintertür hinterlassen hat? Das Team nutzt dieselben Fähigkeiten, die bei einer vollständigen Untersuchung zum Einsatz kämen. Es wendet sie jedoch taktisch auf ein einzelnes System an, um den Verlauf des Angriffs, die verwendeten Persistenzmethoden und die Art der Hintertür oder der Malware zu verstehen, die vom Angreifer für den Zugriff auf das System verwendet wurde. Sobald sich das Team ein umfassendes Bild des Angriffs gemacht hat, kann es Hintertüren aus der Ferne entfernen, Malware bereinigen, Persistenzmethoden eliminieren und bösartige Prozesse im Speicher stoppen. Im Vergleich zu Antiviren-Lösungen oder automatisierten Prozessen kann das Team hier weitaus umfassender tätig werden.

Dies ist für solche Kunden eine enorme Entlastung, die normalerweise ein Re-Imaging durchführen würden, obwohl eine so extreme Maßnahme gar nicht erforderlich wäre. Die Kunden könnten bei den meisten Systemen auf ein Re-Imaging verzichten. Vorausgesetzt, sie haben das Falcon Complete Team an ihrer Seite, das die richtigen Analysen durchführt und die richtigen Maßnahmen ergreift. So lassen sich Zwischenfälle wesentlich eleganter und weniger störend beheben. Das eigentliche Problem wird kosteneffektiv behoben, und zwar weitaus effizienter als bei einem Re-Imaging.

FAZIT

Falcon Complete verhilft Ihrer Organisation zu einem ausgereiften Endgerätesicherheitsprogramm; mit einer Geschwindigkeit, Erschwinglichkeit und Wirksamkeit, die nur sehr wenige Organisationen auf sich gestellt oder auch mit Hilfe Dritter erreichen können.

Durch die Verlagerung des mit Endgerätesicherheit verbundenen administrativen Aufwands nach CrowdStrike sparen Organisationen viel Zeit, die sie für den Aufbau und die Pflege eines Endgerätesicherheitsprogramms oder für die Bearbeitung von Warnmeldungen und die Reaktion auf Vorfälle aufwenden müssten.

Durch Einbindung eines Teams, das auf den Einsatz und die Verwaltung der CrowdStrike Falcon-Plattform spezialisiert ist, erreichen Organisationen jeder Größe sofort den höchsten Reifegrad in ihrer Endgerätesicherheitsstrategie.

Damit verbessern sich ihr gesamtes Cybersicherheitsprogramm und die damit verbundene Sicherheitsaufstellung auf Anhieb.

Und mit dem Falcon Complete Team an ihrer Seite profitieren Organisationen zudem von einem unschätzbaren Vorteil: Der beruhigenden Gewissheit, geschützt zu sein.

Kunden können darauf vertrauen, dass die in ihrem Bereich besten Sicherheitsexperten die Endgeräte ihrer Kunden rund um die Uhr überwachen – auch an Wochenenden, in der Nacht oder wenn man selbst mit anderen Dingen beschäftigt ist. Kunden von Falcon Complete können sich darauf verlassen, dass das Falcon Complete Team die nötigen Maßnahmen zur Behebung von Vorfällen ergreift, ohne dass sie selbst aktiv werden müssen.

ÜBER CROWDSTRIKE

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 3 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eine der weltweitfortschrittlichsten Datenplattformen für Cyber-Sicherheit.

Mit CrowdStrike profitieren Kunden von besserem Schutz, besserer Leistung und sofortiger Time-to-Value – und das alles auf der cloud-nativen Falcon-Plattform.

Über CrowdStrike sollten Sie vor allem eines wissen: **Wir stoppen Datendiebstahl.**

Erfahren Sie mehr über Falcon Complete