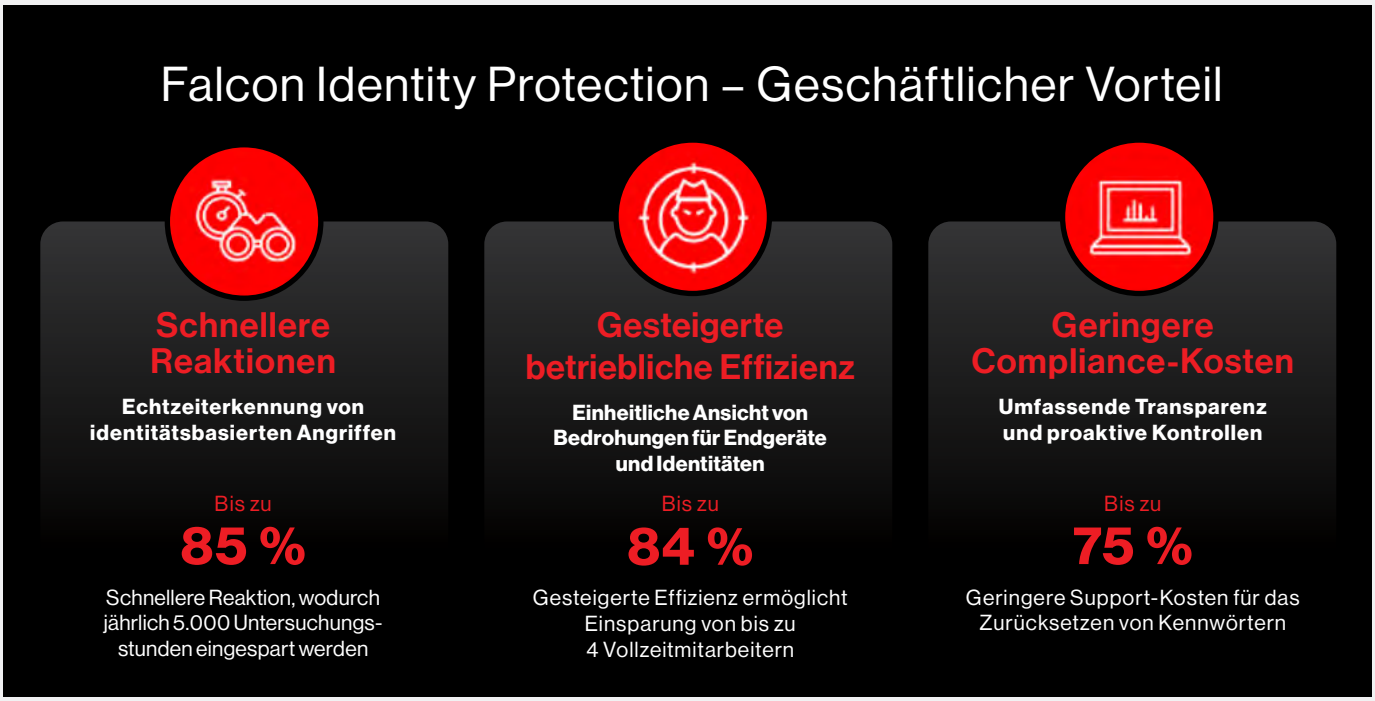
CROWDSTRIKE

Die wichtigsten Gründe, warum Sie Falcon Identity Threat Protection jetzt in Ihr Cyberabwehr-Portfolio aufnehmen sollten

Identitätsbasierte Angriffe sind heute die größte Cybersicherheitsbedrohung für Unternehmen. Fakt ist: Bei mehr als 80 % aller Cyberzwischenfälle werden gültige Anmeldedaten für den Netzwerkzugang missbraucht.

CrowdStrike Falcon® Identity Threat Protection, ein Modul der CrowdStrike Falcon®-Plattform, erkennt und stoppt identitätsbezogene Kompromittierungen in einer komplexen hybriden Identitätslandschaft in Echtzeit – mit einem einzigen Sensor und einer einheitlichen Bedrohungsübersicht, sodass Sie Angriffe auf Endgeräte, Workloads, Identitäten und Daten korrelieren können. Welche geschäftlichen Vorteile können Sie erwarten, wenn Sie Ihr Cyberabwehr-Portfolio noch heute mit Identitätsschutz ergänzen?



1. Bis zu 85 % schnellere Reaktionen auf Bedrohungen

Die Reaktionen des Sicherheitsteams werden nicht nur durch herkömmliche Endgerätelösungen ausgebremst, die Identitätsbedrohungen übersehen, sondern auch durch den aktuellen Ansatz, bei dem Bedrohungen mit mehreren Einzellösungen (AD-Hygienetools, Windows-Ereignisprotokolle, PAM, UEBA, SIEM und mehr) manuell für alle Endgeräte und Identitäten korreliert werden. Mit der einheitlichen CrowdStrike Falcon-Plattform können Kunden von Falcon Identity Threat Protection vollständige Angriffspfade erkennen und Bedrohungen in einer einzigen Konsole korrelieren. Dies ermöglicht **bis zu 85 % schnellere Reaktionen** sowie Echtzeitschutz und spart jährlich tausende Untersuchungsstunden in Folge von Kompromittierungen ein.

2. Um bis zu 84 % gesteigerte betriebliche Effizienz

CrowdStrike Falcon ist **eine cloudnative Lösung mit einem einzigen Sensor**, der überall in der Kundenumgebung bereitgestellt werden kann und die Erfassung von Telemetriedaten (auf Endgeräten oder aus Identitäten) vereinfacht. Ein großes Einzelhandelsunternehmen **konsolidierte mit Falcon Identity Threat Protection mehr als fünf Tools (typisch für viele Unternehmen)** zur Verwaltung von Identitätsbedrohungen in einer Lösung. Die Konsolidierung des Sicherheitskontrollzentrums durch eine Plattform und einen Sensor macht eigenständige Tools und Agenten überflüssig, was zu direkten Einsparungen von Tool- und Betriebskosten führt. Da zudem die Protokolle nicht mehr getrennt erfasst werden müssen, kann die Gesamtzahl der Wartungsstunden durch Echtzeiterkennung reduziert und die **betriebliche Effizienz um bis zu 84 % gesteigert** werden, wodurch etwa vier Vollzeitmitarbeiter eingespart werden können.

3. Um bis 75 % geringere Compliance- und Supportkosten

Dank des umfassenden Überblicks über kompromittierte Kennwörter, übermäßig privilegierte Konten und Missbrauch von Service Accounts können Kunden die Active Directory-Hygiene vorbeugend verbessern sowie proaktive Kontrollen einrichten und damit Compliance-Kosten senken. In einem Fall berichtete ein CISO von **75 % weniger Kennwortzurücksetzungen durch den Support und der Einsparung der damit verbundenen Kosten**. Zudem verringerten sich die Phishing-Anfälligkeit um 8 % und unnötige Benutzerzugriffsrechte um 32 %. Ein großer Telekommunikationsanbieter berichtete, dass sich die Einhaltung der Cybersecurity Maturity Model Certification (CMMC) durch den Einsatz von Falcon Identity Threat Protection und dem dadurch umfassenderen Einsatz von Multifaktor-Authentifizierung (MFA) – auch bei Legacy-Anwendungen – verbessert hat.

4. Um 57 % geringeres Risiko für Kompromittierungen durch gestohlene Anmeldedaten

Da bei acht von zehn Angriffen gestohlene oder kompromittierte Anmeldedaten genutzt werden, wird durch ein geringeres Risiko für gestohlene Anmeldedaten die allgemeine Sicherheit unmittelbar verbessert. Falcon Identity Threat Protection kann identitätsbezogene Bedrohungen erkennen und ermöglicht Kunden, riskante Konten sowie mögliche Angriffspfade in der gesamten Umgebung zu identifizieren und somit die Angriffsfläche zu minimieren. Kürzlich teilte der CISO einer Hotelkette mit, dass Falcon Identity Threat Protection auf Anhieb 250.000 mögliche Angriffspfade in der Unternehmensumgebung aufgedeckt hat und 93 % davon mit drei Konfigurationsänderungen behoben werden konnten. CrowdStrike-Geschäftswert-Analysen haben gezeigt, dass sich **das Risiko für Kompromittierungen durch gestohlene Anmeldedaten um bis zu 57 % verringert**. Dies wurde ebenfalls durch Penetrationstests bei Kunden demonstriert, die bei den gleichen Tests vor der Bereitstellung von Falcon Identity Threat Protection durchgefallen waren.

5. Verbesserte Cyber-Versicherbarkeit und geringere Prämien

Da schwache Identitätssicherheitskontrollen nach wie vor von Angreifern ausgenutzt werden, **weisen Cyber-Versicherungsunternehmen darauf hin**, dass die Kontrollen verbessert werden müssen, um Cyberrisiken zu minimieren. Ransomware ist ein wichtiger Faktor für Cyberversicherungen, weshalb die Versicherer immer wieder auf folgende Voraussetzungen für die Cyber-Versicherbarkeit hinweisen: Absicherung des Active Directory, Durchsetzung von Multifaktor-Authentifizierung für alle Anwendungen (auch für ältere), Schutz von privilegierten Konten und Service Accounts sowie Einsatz von endpunktbasierter Detektion und Reaktion (EDR). Kunden, die Falcon Identity Threat Protection nutzen, berichten von Vorteilen für ihre Cyberversicherung und geringeren Prämien.

Das sagen CrowdStrike-Kunden

„Nachdem wir Falcon Identity Threat Protection bereitgestellt hatten, führten wir einen weiteren Penetrationstest durch und erkannten sofort die Vorteile der verbesserten Transparenz."

Ryan Melle
SVP, CISO, Berkshire Bank
(**Anwenderbericht lesen**)

„Seit der Bereitstellung von Falcon Identity Threat Protection haben wir einen deutlich besseren Überblick über Anmeldedaten, privilegierte Identitäten sowie verschiedene Angriffspfade und wissen, welche Schutzmaßnahmen wir ergreifen können."

Steven Townsley
Head of Information Security, Mercedes-AMG Petronas Formel 1-Team
(**Video ansehen**)

„Zwei Stunden nach der Bereitstellung von Falcon Identity Threat Protection haben wir zehn privilegierte Konten mit kompromittierten Kennwörtern identifiziert und gleich darauf zurückgesetzt."

CISO eines US-Countys im Raum Washington, D.C.
(**Blog-Artikel lesen**)

„Wir haben den Wert von Falcon Identity Threat Protection bereits in der ersten Minute erkannt, als wir 250.000 mögliche Angriffspfade identifizieren und 93 % davon mit nur drei Konfigurationsänderungen beheben konnten."

CISO einer internationalen Hotelkette

„Es ist deutlich komfortabler, den Großteil des SOC über ein einziges Fenster zu verwalten, als 13 verschiedene Konsolen und Seiten zu studieren, um etwas zu analysieren und aufzuspüren."

CISO eines Agrar- und Lebensmittelunternehmens

Identitätsschutz ist nicht optional, sondern unverzichtbar

Der CrowdStrike Global Threat Report 2023 zeigt, dass Identitätsangriffe zunehmen und **die Zahl der Access-Broker-Inserate im Dark Web im Jahr 2022 um 112 % gestiegen** ist. Microsoft Active Directory, das von über 90 % der Unternehmen genutzt wird, bleibt weiterhin die am häufigsten missbrauchte Schwachstelle für Angriffe.[1] Eine aktuelle Metadatenanalyse von mehreren Millionen Konten (darunter menschliche, privilegierte sowie Service Accounts) durch CrowdStrike ergab, dass tatsächlich **50 % der Unternehmen privilegierte Konten mit kompromittierten Kennwörtern nutzen**.

Erschwerend kommt hinzu, dass Identitätskompromittierungen bekanntermaßen schwer zu erkennen sind und eine **Identifizierung ohne die richtigen Tools im Durchschnitt etwa 250 Tage dauert**[2]. In dieser Zeit können sich die Angreifer unbemerkt lateral in der Umgebung bewegen und verheerende Angriffe ausführen. Laut dem CrowdStrike Global Threat Report 2023 betrug die **durchschnittliche Zeit bis zum Ausbruch im Jahr 2022 nur 84 Minuten**. Angesichts dessen können es sich die Unternehmen nicht leisten, erst bei einer schwerwiegenden Identitätskompromittierung zu reagieren. Zudem sind die Angreifer möglicherweise bereits in Ihrer Umgebung, ohne dass Sie es bemerkt haben.

Identitätsorientierte Bedrohungen zu ignorieren kann schwerwiegende Folgen wie die vollständige Domänenkompromittierung der AD-Infrastruktur, lähmende Ransomware-Angriffe und verheerende Geschäftsunterbrechungen haben. Laut IBM und dem Ponemon Institute belaufen sich die **weltweiten Durchschnittskosten einer Datenkompromittierung auf 4,35 Millionen US-Dollar (in den USA liegen sie bei 9,44 Millionen US-Dollar)**.[3] Da bei **80 % aller Angriffe** gestohlene oder kompromittierte Zugangsdaten zum Einsatz kommen, wirkt sich die Implementierung einer Identitätsschutzlösung sofort positiv aus und bietet Ihnen potenzielle Kosteneinsparungen in Millionenhöhe. Zudem schützt sie Ihre Marke und Ihren Ruf vor irreversiblen Schäden.

Die Angreifer werden nicht warten, bis Sie vorbereitet sind. Stoppen Sie Kompromittierungen jetzt mit Falcon Identity Threat Protection.

Kontaktieren Sie Ihren CrowdStrike-Kundenvertreter oder fordern Sie Ihre kostenlose Active Directory-Risikoüberprüfung an.

[1] Frost & Sullivan: „Active Directory Holds the Keys to your Kingdom, but is it Secure?".

[2] IBM und Ponemon Institute: „Cost of a Data Breach Report 2022".

[3] IBM und Ponemon Institute: „Cost of a Data Breach Report 2022".

* Die erwarteten und tatsächlichen Ergebnisse können nicht garantiert werden und können von Kunde zu Kunde variieren. Die erwarteten Vorteile 1, 2 und 4 basieren auf aggregierten Durchschnittswerten aus über 100 BVAs (Business Value Assessments, engl. für „Geschäftswert-Analysen") und BVR-Fällen (Business Value Realized, englisch für „erzielter Geschäftswert"), die von 2018 bis Dezember 2022 vom CrowdStrike-Business Value-Team bei CrowdStrike Enterprise-Kunden durchgeführt wurden. BVAs sind prognostizierte Renditeanalysen, die auf dem Wert der CrowdStrike-Lösung im Vergleich zur vorhandenen Lösung des Kunden basieren. BVRs sind Analysen der erzielten Rendite bei Kunden, die CrowdStrike-Lösungen über einen Zeitraum von mehr als sechs Monaten nutzen. Die Analysen werden mithilfe von Kundenfeedback und aufgezeichneten Telemetriedaten erstellt. Der erwartete Vorteil 3 basiert auf Daten, die von einem Kunden direkt an CrowdStrike übermittelt wurden.

Über CrowdStrike

CrowdStrike (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit einer der weltweit fortschrittlichsten cloudnativen Plattformen für Endgeräte- und Workloadschutz sowie Identität und Daten die Sicherheit geschäftskritischer Unternehmensbereiche neu.

Die CrowdStrike Falcon®-Plattform nutzt die CrowdStrike Security Cloud und erstklassige KI, um Echtzeit-Angriffsindikatoren, Bedrohungsanalysen, veränderte Vorgehensweisen von Angreifern sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen auszuwerten. Dadurch kann die CrowdStrike-Plattform äußerst präzise Bedrohungen erkennen, automatisierte Schutz- und Behebungsmaßnahmen bereitstellen, zuverlässige Bedrohungssuchen durchführen und Schwachstellen priorisieren.

CrowdStrike Falcon® wurde für den Cloud-Einsatz entwickelt und nutzt einen einzigen schlanken Agenten, um schnelle und skalierbare Bereitstellung, hervorragende Schutzwirkung und Geschwindigkeit, geringere Komplexität sowie sofortige Rendite zu ermöglichen.

CrowdStrike: **We stop breaches.**

Folgen Sie uns: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Kostenlose Testversion

Weitere Informationen unter **www.crowdstrike.de**