
CROWDSTRIKE
Angriffe enden hier
Cloudbasierter Schutz für
Endgeräte,
Cloud-Workloads,
Identitäten und Daten

CrowdStrike Falcon

SCHÜTZEN SIE IHRE WICHTIGSTEN RISIKOBEREICHE: ENDGERÄTE, CLOUD, IDENTITÄTEN UND DATEN

Es hieß, dass es unmöglich sei, vollständigen cloudnativen Schutz mit einem einzigen schlanken Agenten zu bieten, ohne die Benutzer-Performance zu beeinträchtigen.

Doch CrowdStrike hat es möglich gemacht. Die cloudnative **CrowdStrike Falcon**-Plattform führt auf einzigartige Weise Technologie, Bedrohungsdaten und Expertise zu einer umfassenden, durchgängigen Sicherheitslösung zusammen, die die wichtigsten Risikobereiche von Unternehmen abdeckt: Endgeräte, Cloud-Workloads, Identitäten und Daten.

Mit der **CrowdStrike Security Cloud** und dem schlanken Falcon-Agenten, die Daten einmal erfassen und mehrmals nutzen, behebt die Falcon-Plattform zahlreiche Sicherheitsprobleme und reduziert gleichzeitig die Kosten und Komplexität.

Die **Falcon-Plattform** wächst immer weiter und bietet in diesen Bereichen branchenführenden Schutz:

- Endgerätesicherheit und erweiterte Erkennung und Reaktion (XDR)
- Cloud-Sicherheit
- Managed Services
- Threat Intelligence
- Identitätsschutz
- Sicherheits- und IT-Abläufe
- SIEM der nächsten Generation und Log-Management
- Datenschutz

Mit der Falcon-Plattform erhalten Kunden schnelle und skalierbare Bereitstellung, hervorragenden Schutz und hohe Leistung, geringere Komplexität sowie sofortige Wertschöpfung.

SCHUTZ, DER SIE WEITER BRINGT

Bedrohungen automatisch vorhersagen und in Echtzeit verhindern

Die **CrowdStrike Falcon®**-Plattform wurde funktionsorientiert in der Cloud entwickelt und schützt mit einem schlanken Agenten geschäftskritische Risikobereiche: Endgeräte, Cloud-Workloads, Identitäten und Daten.

Die Falcon-Plattform nutzt die CrowdStrike Security Cloud, um Echtzeit-Angriffsindikatoren, Threat Intelligence, sich weiterentwickelnde Vorgehensweisen von Angreifern sowie angereicherte Telemetriedaten aus dem gesamten Unternehmen auszuwerten. Dies ermöglicht die äußerst präzise Erkennung von Bedrohungen, automatisierte Schutz- und Behebungsmaßnahmen, tiefgreifende Bedrohungssuchen und Schwachstellenpriorisierung.

DER CROWDSTRIKE-UNTERSCHIED

Charlotte AI

Eine weitere Funktion aus CrowdStrikes generativem KI-Portfolio der Falcon-Plattform. Sie nutzt Petabytes an Daten von automatisierten CrowdStrike-Bedrohungsanalysen, die von Sicherheitsexperten ergänzt werden, um die Arbeitsabläufe von Analysten zu beschleunigen.

Ein schlanker Agent

Lässt sich reibungslos und im großen Maßstab bereitstellen und stoppt alle Angriffsarten – ohne die Speicherressourcen und das Endgerät durch geplante Scans zu belasten.

Cloudnative Plattform

Nutzt den Netzwerkeffekt der durch Crowdsourcing zusammengeführten Sicherheitsdaten. Gleichzeitig müssen keine lokalen Lösungen aufwändig verwaltet werden.

CrowdStrike Asset Graph

Behebt eines der derzeit komplexesten Kundenprobleme: die exakte Identifizierung von Assets, Identitäten und Konfigurationen bei allen Systemen, einschließlich Cloud, lokale und mobile Systeme, IoT und mehr. Diese Daten werden in einem Diagramm verknüpft.

Falcon Foundry

Ermöglicht Kunden und Partnern die einfache Erstellung benutzerdefinierter No-Code-Anwendungen, um mithilfe der Daten, Automatisierung und cloudskalierbaren Infrastruktur der Falcon-Plattform die größten Cybersicherheitsherausforderungen zu bewältigen.

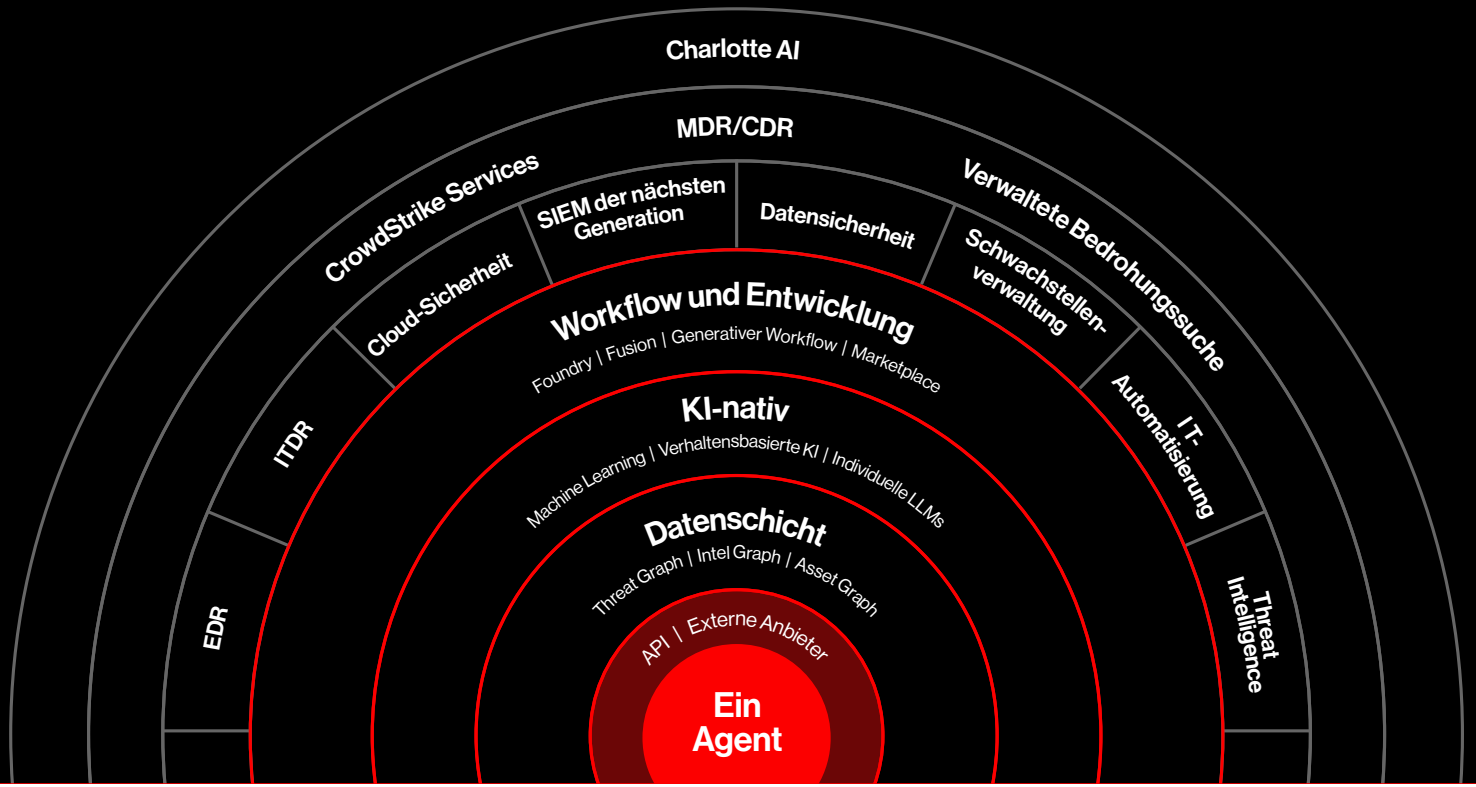
CrowdStrike Threat Graph

Nutzt cloudbasierte künstliche Intelligenz (KI), um Billionen Datenpunkte aus zahlreichen Telemetriedatenquellen zu korrelieren und Veränderungen bei den Taktiken der Bedrohungsakteure zu identifizieren. Diese werden im **CrowdStrike Threat Graph®** kartiert, um Bedrohungen bei CrowdStrike-Kunden auf der ganzen Welt automatisch und in Echtzeit zu verhindern.

Falcon Fusion

Stellt innerhalb der Falcon-Plattform integrierte SOAR-Funktionen (Security Orchestration Automation und Response) bereit. Dies ermöglicht die Sammlung kontextbezogener, angereicherter Daten und die Automatisierung von Sicherheitsvorgängen, Bedrohungsanalysen und Vorfallsreaktionen zur Begrenzung von Cyberbedrohungen und Schwachstellen – alles auf einer einzigen Plattform und über dieselbe Konsole.

Die CrowdStrike Falcon-Plattform



CROWDSTRIKE MARKETPLACE

CLOUDSKALIERBARES, OFFENES ÖKOSYSTEM

Technologiepartner-Marketplace für Unternehmen. Hier können geprüfte CrowdStrike- sowie Partneranwendungen gefunden, getestet, gekauft und bereitgestellt werden, die die CrowdStrike Falcon-Plattform erweitern, ohne zusätzliche Agenten zu benötigen oder die Komplexität zu erhöhen.

CROWDSTRIKE UNIVERSITY

SCHULUNGEN UND ZERTIFIZIERUNGEN

Bietet Online- und geleitete Schulungskurse und Zertifizierungen mit Schwerpunkt auf der Implementierung, Verwaltung, Entwicklung und Nutzung der CrowdStrike Falcon-Plattform.

CROWDSTRIKE ZERO TRUST

Setzt auf den drei kritischen Ebenen – Geräte, Identitäten und Daten – nativ sowie reibungslos Zero-Trust-Sicherheit durch. Dies umfasst Echtzeit-Bedrohungsschutz und die Erzwingung von IT-Richtlinien mithilfe von Identitäts-, Verhaltens- und Risikoanalysen, damit Kompromittierungen für alle Endgeräte, Workloads und Identitäten unterbunden werden.

Eine Plattform. Vollständiger Schutz.

ENDGERÄTESICHERHEIT

FALCON PREVENT | VIRENSCHUTZ DER NÄCHSTEN GENERATION
Schützt vor Bedrohungen aller Art, von Malware und Ransomware bis hin zu raffinierten Angriffen, und lässt sich innerhalb von Minuten bereitstellen, sodass Endgeräte sofort geschützt werden.

FALCON INSIGHT XDR | ERKENNUNG UND REAKTION FÜR ENDGERÄTE UND MEHR
Bietet branchenführende einheitliche endpunktbasierte Detektion und Reaktion (EDR) sowie erweiterte Erkennung und Reaktion (XDR) mit unternehmensweiter Transparenz, damit Angriffsaktivitäten automatisch erkannt und auf allen Endgeräten und wichtigen Angriffsflächen automatisiert abgewehrt werden können.

FALCON COMPLETE XDR | ERWEITERTE ERKENNUNG UND REAKTION ALS MANAGED SERVICE (MXDR)
Erweitert den branchenführenden MDR-Service von Falcon Complete mit domänenübergreifendem XDR-Schutz. Wird vom CrowdStrike-Expertenteam rund um die Uhr durchgeführt, einschließlich proaktiver Bedrohungssuche und nativen Bedrohungsanalysen.

FALCON FIREWALL MANAGEMENT | HOST-FIREWALL
Ermöglicht die einfache und zentrale Verwaltung für Host-Firewalls und dadurch die einfache Verwaltung und Kontrolle der Host-Firewall-Richtlinien.

FALCON DEVICE CONTROL | USB-SICHERHEIT
Bietet den Überblick und die detaillierte Kontrolle zur sicheren Nutzung von USB-Geräten im gesamten Unternehmen.

FALCON FOR MOBILE | ENDPUNKTBASIERTE DETEKTION UND REAKTION FÜR MOBILGERÄTE
Schützt vor Bedrohungen, die auf iOS- und Android-Geräte abzielen. Weitet XDR/EDR-Funktionen auf Ihre Mobilgeräte aus, einschließlich erweitertem Bedrohungsschutz und Echtzeit-Transparenz zu App- und Netzwerkaktivitäten.

THREAT INTELLIGENCE

FALCON INTELLIGENCE | AUTOMATISIERTE BEDROHUNGSANALYSE
Ergänzt die von der CrowdStrike Falcon-Plattform erkannten Ereignisse und Zwischenfälle mit Kontextinformationen und automatisiert die Analyse, damit Sicherheitsteams schneller bessere Entscheidungen treffen können.

FALCON INTELLIGENCE PREMIUM | CYBER-BEDROHUNGSANALYSEN
Bietet erstklassige Bedrohungsberichte, technische Malware-Analysen sowie Funktionen zur Bedrohungssuche, damit Unternehmen ihre Resilienz verbessern und raffinierte staatliche, kriminelle und hacktivistische Bedrohungsakteure abwehren können.

FALCON INTELLIGENCE ELITE | ZUGEWIESENER ANALYST
Optimiert die Investition in Falcon Intelligence Premium durch die Zuweisung eines CrowdStrike-Bedrohungsanalysten, dessen Aufgabe es ist, Ihr Unternehmen vor gezielten Angriffen zu schützen.

FALCON INTELLIGENCE RECON | DIGITALE BEDROHUNGSÜBERWACHUNG
Überwacht potenziell böswillige Aktivitäten im Open, Deep und Dark Web, sodass Marken, Mitarbeiter und sensible Daten besser geschützt werden können.

FALCON INTELLIGENCE RECON+ | VERWALTETE BEDROHUNGSÜBERWACHUNG
Ein CrowdStrike-Experte verwaltet die Überwachung, Triagierung, Bewertung und Behebung von Bedrohungen aus dem kriminellen Untergrund.

FALCON SANDBOX | MALWARE-ANALYSE
Legt den gesamten Ablauf des Angriffs mit tiefgreifenden Einblicken in alle Datei-, Netzwerk-, Speicher- und Prozessaktivitäten offen. Enthalten sind außerdem leicht verständliche Berichte, verwertbare IOCs und nahtlose Integrationen.

VERWALTETE SICHERHEIT

FALCON COMPLETE | VERWALTETE ERKENNUNG UND REAKTION (MDR)
Stoppt und beseitigt Bedrohungen innerhalb von Minuten, mit rund um die Uhr sichergestellter Verwaltung durch Experten, Überwachung und präziser Behebung, proaktiver Bedrohungssuche und integrierten Bedrohungsanalysen – alles gestützt auf die branchenweit stärkste Garantie zur Verhinderung von Kompromittierungen.

FALCON OVERWATCH™ | VERWALTETE BEDROHUNGSSUCHE
Ein Team aus hochqualifizierten Cybersicherheitsexperten hält innerhalb der Falcon-Plattform beständig Ausschau nach unauffälligen Anzeichen für raffinierte Angriffe, sodass Angreifern kein sicheres Versteck bleibt.

FALCON OVERWATCH™ ELITE | ZUGEWIESENER ANALYST FÜR VERWALTETE BEDROHUNGSSUCHE
Erweitert Ihr Team mit einem zugewiesenen CrowdStrike-Analysten für die Bedrohungssuche. Bietet dedizierte Kompetenzen, taktische tagesaktuelle Erkenntnisse zu Ihrer Bedrohungslandschaft sowie strategische Beratung, damit Sie Ihren Schutz kontinuierlich verbessern können.

COUNTER ADVERSARY OPERATIONS ELITE | DEDIZIERTER THREAT HUNTING-ANALYST
Der Ihnen zugewiesene Analyst identifiziert und stoppt Angreifer mithilfe hochentwickelter Untersuchungs- und Threat Hunting-Tools, die detaillierte Bedrohungsdaten nutzen, in Ihrer IT-Umgebung und darüber hinaus.

CLOUD-SICHERHEIT

FALCON CLOUD SECURITY
Bietet Angriffsschutz durch Bedrohungsanalysen, Erkennung und Reaktion, Laufzeitschutz für Workoads und Sicherheitsverwaltung für Cloud-Umgebungen wie AWS, Azure und Google Cloud Platform.

FALCON CLOUD SECURITY FOR CONTAINERS
Bietet Sicherheitsfunktionen und Kompromittierungsschutz für Cloud und Container, einschließlich Sicherheitsverwaltung für Cloud-Umgebungen, Bedrohungserkennung und -abwehr für lokale, hybride und Multi-Cloud-Umgebungen sowie Cloud-Workload-Schutz (z. B. Container-Sicherheit und Kubernetes-Schutz).

FALCON CLOUD SECURITY FOR MANAGED CONTAINERS
Gewährleistet den Schutz von Cloud und Containern und bietet Sicherheitsfunktionen wie Analysen, Erkennung und Abwehr von Bedrohungen sowie Container-Image- und Kubernetes-Schutz.

FALCON OVERWATCH™ CLOUD THREAT HUNTING | MANAGED SERVICES
Deckt Cloud-Bedrohungen auf, von individuellen Angriffspfaden mit komplexen Spuren von Cloud-IOAs und Indikatoren für Konfigurationsfehler (IOMs) bis zu verborgenen Aktivitäten von Bedrohungsakteuren in kritischer Cloud-Infrastruktur, einschließlich AWS, Azure und Google Cloud Platform.

FALCON COMPLETE CLOUD SECURITY | MDR FÜR CLOUD-WORKLOADS
Vollständig verwalteter Service für Cloud-Workload-Schutz, einschließlich Sicherheitsverwaltung, Bedrohungssuche, Überwachung und Reaktion für Cloud-Workloads rund um die Uhr, unterstützt durch die Garantie zur Verhinderung von Kompromittierungen.

SICHERHEITS- UND IT-ABLÄUFE

FALCON DISCOVER | IT-HYGIENE
Erkennt in Echtzeit in der gesamten Umgebung nicht autorisierte Konten, Systeme sowie Anwendungen und verschafft einen sofortigen Überblick für den Ausbau Ihrer Sicherheit.

FALCON SPOTLIGHT | SCHWACHSTELLENVERWALTUNG
Bietet Sicherheitsteams eine automatisierte und umfassende Verwaltung der Sicherheitslösung und ermöglicht so die schnellere Priorisierung durch integrierte Korrektur-Workflows ohne ressourcenintensive Scans.

FALCON EXPOSURE MANAGEMENT | VERWALTUNG VON SICHERHEITSLÜCKEN
Ermöglicht Sicherheitsteams die Priorisierung der schwerwiegendsten Gefahrenpotenziale sowie die proaktive Reduzierung der Möglichkeiten von Angreifern, eine Umgebung zu kompromittieren und sich lateral zu bewegen.

FALCON SURFACE | VERWALTUNG DER EXTERNEN ANGRIFFSFLÄCHE
Kontinuierliche Erkennung und Kartierung aller Assets mit Internetverbindungen, um potenzielle Schwachstellen schließen zu können. Umfasst geführte Behebungspläne zur Reduzierung der Angriffsfläche.

FALCON DATA PROTECTION | EINHEITLICHER DATENSCHUTZ
Bietet detaillierte Echtzeit-Transparenz dazu, was mit sensiblen Daten geschieht, um auf diese Weise Datendiebstahl zu stoppen. Umfasst Richtliniendurchsetzung, die automatisch Inhalte und nicht nur Dateien auswertet.

FALCON FILEVANTAGE | DATEIINTEGRITÄTS-ÜBERWACHUNG
Bietet umfassende und zentrale Echtzeit-Transparenz, um die Einhaltung von Compliance-Vorschriften deutlich zu verbessern und relevante Kontextdaten bereitzustellen.

FALCON FORENSICS | FORENSISCHE CYBERSICHERHEIT
Automatisiert die Erfassung punktueller und historischer Daten aus forensischen Untersuchungen zur zuverlässigen Analyse von Cybersicherheitsvorfällen.

FALCON FOR IT | AUTOMATISIERTE WORKFLOWS
Erweitert die Falcon-Plattform zur Automatisierung von IT- und Sicherheitsabläufen mit einem durchgängigen Lebenszyklus von der Sichtbarkeit zur Maßnahmenergreifung.

IDENTITÄTSSCHUTZ

FALCON IDENTITY THREAT DETECTION
Ermöglicht die hochpräzise Echtzeit-Erkennung identitätsbasierter Bedrohungen. Nutzt KI und Verhaltensanalysen, um hochgradig entscheidungsrelevante Informationen zur Abwehr moderner Angriffe wie Ransomware bereitzustellen.

FALCON IDENTITY THREAT PROTECTION
Bietet äußerst präzise Bedrohungserkennung und Echtzeitprävention von identitätsbasierten Angriffen durch eine Kombination aus hochentwickelter KI, Verhaltensanalysen sowie einem flexiblen Richtlinienmodul, das risikobasiert bedingten Zugriff gewährt.

FALCON COMPLETE IDENTITY THREAT PROTECTION
Eine, von einem CrowdStrike-Expertenteam bereitgestellte, vollständig verwaltete Identitätsschutzlösung, die rund um die Uhr die reibungslose Echtzeit-Abwehr von Identitätsbedrohungen, die Durchsetzung von IT-Richtlinien, die Überwachung und die Behebung ermöglicht.

SIEM DER NÄCHSTEN GENERATION

FALCON LOGSCALE | SIEM UND LOG-MANAGEMENT

Ermöglicht das schnelle Stoppen von Bedrohungsakteuren und die Reduzierung der SOC-Kosten, da branchenführende Erkennung, erstklassige Bedrohungsanalysen, blitzschnelle Suchen und KI-geführte Untersuchungen in einer cloudbasierten Plattform zusammengeführt werden.

CROWDSTRIKE SERVICES

Bietet rund um die Uhr Services für die Reaktion vor, während und nach Vorfällen. Ein qualifiziertes Team leistet Hilfestellung bei der Verteidigung gegen und Reaktion auf Sicherheitsvorfälle, um Kompromittierungen zu vermeiden und die Behebungsgeschwindigkeit zu optimieren.

VORKEHRUNG: BERATUNGSSERVICES

Realitätsnahe Simulationsübungen helfen, nötige Vorkehrungen zur Abwehr raffinierter Bedrohungsakteure zu treffen.

- TABLETOP-ÜBUNGEN
- ÜBUNGEN MIT ANGRIFFSSIMULATIONEN
- RED TEAM/BLUE TEAM-ÜBUNGEN
- PENETRATIONSTESTS

REAKTION: BREACH SERVICES

Liefern schnelle und präzise Hilfe zum Stoppen von Kompromittierungen, zur Untersuchung von Zwischenfällen und zum Wiederherstellung nach einem Angriff.

- REAKTION AUF ZWISCHENFÄLLE (IR)
- WIEDERHERSTELLUNG VON ENDGERÄTEN
- KOMPROMITTIERUNGSPRÜFUNG
- BEWERTUNG DER ANGRIFFSFLÄCHE
- NETZWERKSICHERHEITSÜBERWACHUNG

STÄHLUNG: BERATUNGSSERVICES

Helfen durch umsetzbare Empfehlungen, die Cybersicherheit zu verbessern und Schutzmaßnahmen zu verstärken.

- REIFEGRADBEWERTUNG FÜR CYBERSICHERHEIT
- CLOUD-SICHERHEITSBEWERTUNG
- BEWERTUNG DER TECHNISCHEN RISIKEN
- BEWERTUNG DES SOC
- BEWERTUNG DER AD-SICHERHEIT
- PROGRAMM ZUR VERBESSERUNG DER CYBERSICHERHEIT
- DETAILLIERTE BEWERTUNG DES SICHERHEITSPROGRAMMS

CLOUD SECURITY SERVICES

Helfen bei der Wiederherstellung nach einer Cloud-Datenkompromittierung und bei der Absicherung von Cloud-Plattformkonfigurationen.

- REAKTION AUF CLOUD-ZWISCHENFÄLLE
- BEWERTUNG DER CLOUD-SICHERHEIT
- KOMPROMITTIERUNGSPRÜFUNG DER CLOUD
- RED TEAM/BLUE TEAM-ÜBUNGEN FÜR DIE CLOUD
- OPERATIVE FALCON-SUPPORT-SERVICES FÜR CLOUD-SICHERHEIT

TECHNOLOGIE-SERVICES

Helfen, den Schutz von Unternehmen zu verbessern.

- ENDGERÄTESCHUTZ-SERVICES
- IDENTITÄTSSCHUTZ-SERVICES
- NETZWERKÜBERWACHUNGS-SERVICES
- LOG-MANAGEMENT-SERVICES
- OPERATIVE FALCON-SUPPORT-SERVICES
- FALCON GOLD STANDARD

Branchenweite Anerkennung von CrowdStrike

CrowdStrike setzt sich dafür ein, Unternehmen einen ganzheitlichen und zuverlässigen Schutz vor bekannten ebenso wie unbekannten Cyber-Angriffen zu bieten – egal ob mit oder ohne Malware-Komponente.
Das sagen Branchenanalysten über **CrowdStrike:**

- Im Gartner® Magic Quadrant™ für Endgeräteschutz-Plattformen (EPP) 2022 als führender Anbieter mit der Höchstplatzierung für die Vollständigkeit des Lösungsansatzes ausgezeichnet
- Auszeichnung als „Leader“ im Frost & Sullivan Radar™ für CNAPP 2023
- Auszeichnung als „Leader“ im Frost & Sullivan Radar™ für CWPP 2023
- Auszeichnung als „Leader“ im Forrester Wave™: Endpoint Security, 4. Quartal 2023
- Auszeichnung als „Leader“ im Forrester Wave™: External Threat Intelligence Service Providers, 3. Quartal 2023
- Auszeichnung als „Leader“ im Forrester Wave™: Endpoint Detection and Response Providers, 2. Quartal 2022
- Auszeichnung als „Leader“ im Forrester Wave™: Cybersecurity Incident Response Services (CIRS), 1. Quartal 2022
- Einstufung als „Strong Performer“ im Forrester Wave™: Cloud Workload Security, 1. Quartal 2022
- Auszeichnung als „Leader“ im IDC MarketScape™: Worldwide Modern Endpoint Security for Enterprise 2022 Vendor Assessment

CROWDSTRIKE