

# FALCON PREVENT – VIRENSCHUTZ DER NÄCHSTEN GENERATION (NGAV)

Dieser ideale Ersatz für Antivirenlösungen kombiniert die wirksamsten Präventionstechnologien mit einfacher Handhabung und zeigt Angriffe klar und deutlich auf

## BRANCHENWEIT ANERKANNTER ERSATZ FÜR HERKÖMMLICHE ANTIVIREN-LÖSUNGEN

Für Unternehmen und Institutionen, die mit der Ineffizienz und Komplexität ihrer herkömmlichen Antivirenlösungen zu kämpfen haben, ist CrowdStrike® Falcon Prevent™ die richtige Wahl. Falcon Prevent überzeugt durch überlegenen Schutz mit einem einzigen, schlanken Agent, der ohne ständige Signatur-Updates, lokale Verwaltungsinfrastrukturen oder komplexe Integrationen auskommt. Selbst die größten Organisationen sind mit Falcon Prevent in wenigen Minuten einsatzbereit.

**Zertifiziert als Ersatz für herkömmliche Antiviren-Produkte** – Unabhängige Tests von AV-Comparatives und SE Labs belegen die Wirksamkeit von Falcon Prevent. Zudem wurde Falcon Prevent nach den Anforderungen gemäß PCI, HIPAA, NIST und FFIEC validiert.

**Auszeichnung als „Leader“ im Gartner im Magic Quadrant (MQ) für Endpoint Protection Platforms (EPP) 2019 – Neben der Positionierung als „Leader“** – d. h. als führendes Unternehmen – erhielt CrowdStrike die höchste Bewertung für die „Vollständigkeit der Vision“. Der Marktforschungsbericht von Gartner umfasst Kriterien wie Innovation, Marketing- und Produktstrategien, Strategien für vertikale Branchen und geografische Strategien sowie die Schlüssigkeit des Geschäftsmodells insgesamt.

### ENTSCHEIDENDE VORTEILE

Schützt gegen Angriffe jeder Art

Vereinfacht den Betrieb dank signaturlosem Schutz und Bereitstellung als Software-as-a-Service (SaaS)

Ist in wenigen Minuten implementiert und sofort einsatzbereit

Ersetzt herkömmliche AV-Lösungen schnell und zuverlässig

Lässt sich während der Migration problemlos parallel zu einer vorhandenen AV-Lösung betreiben

Zeigt Angriffe vollständig auf

## FALCON X ELITE

# WICHTIGE LEISTUNGSMERKMALE

## HOCHMODERNE PRÄVENTIONSTECHNIKEN

Falcon Prevent schützt Endgeräte gegen Angriffe aller Art: von gängiger Malware bis hin zu ausgeklügelten Strategien – sogar, wenn die Geräte offline sind.

- Maschinelles Lernen und künstliche Intelligenz blockieren bekannte und unbekannt Malware, Adware sowie potenziell unerwünschte Programme
- Verhaltensbasierte Angriffsindikatoren (IOAs) verhindern versierte Angriffe; auch Ransomware und Angriffe ohne Dateien oder Malware
- Exploit Blocking stoppt die Ausführung und Verbreitung von Bedrohungen über nicht gepatchte Schwachstellen
- Präventive Bedrohungsaufklärung sperrt alle als bössartig bekannten Aktivitäten
- Über benutzerdefinierte Angriffsindikatoren lassen sich spezielle Verhaltensweisen definieren, die blockiert werden sollen
- Blockierte Dateien werden unter Quarantäne gestellt, wo sie für weitere Ermittlungen zugänglich sind
- Die skriptbasierte Ausführungsüberwachung inspiziert und blockiert bössartige Makros in Microsoft-Office-Anwendungen

## VOLLE ANGRIFSTRANSparenZ AUF EINEN BLICK

Mit den Kontextinformationen zu Alarmen schafft Falcon Prevent eine beispiellose Transparenz:

- Jeder Alarm erfolgt unter Angabe von Details, Kontext und Verlauf
- Der gesamte Angriff wird in einem leicht verständlichen Prozessbaum samt Kontextdaten und Bedrohungsinformationen dargestellt
- Der Abgleich der Warnmeldungen mit dem ATT&CK®-Framework von MITRE (Adversarial Tactics, Techniques, and Common Knowledge) macht auch komplexe Ereignisse auf einen Blick verständlich
- Erkennungsdetails werden 90 Tagelang aufbewahrt

**Testen Sie jetzt kostenlos  
den Virenschutz der  
nächsten Generation**

Erfahren Sie mehr unter [www.crowdstrike.de](http://www.crowdstrike.de)  
© 2020 CrowdStrike, Inc. Alle Rechte vorbehalten.

## INTEGRIERTE BEDROHUNGSaufKLÄRUNG

- Sie ermitteln automatisch Umfang und Auswirkung der in Ihrer Umgebung gefundenen Bedrohungen.
- Sie stellen fest, ob Sie im Visier sind, wer Sie im Visier hat und wie Sie sich besser schützen und aufstellen können
- Sie können Falcon Prevent in CrowdStrike Falcon X™ integrieren, um:
  - die Bedrohungslage in Ihrer Umgebung vollständig zu verstehen und geeignete Abhilfemaßnahmen zu ergreifen
  - auf Erkenntnisse und Analysen zu Malware zuzugreifen
  - Maßnahmen einfach zu priorisieren dank fundierter Bewertung des Bedrohungsgrads
  - sofortige Schritte zur Wiederherstellung und Behebung von Vorfällen mit detaillierter Bedrohungsanalyse zu ergreifen

## EINFACH, SCHNELL UND SCHLANK

Die cloud-native CrowdStrike Falcon®-Plattform und der schlanke Falcon-Agent beseitigen Komplexitäten und vereinfachen die Sicherheitsabläufe an den Endgeräten.

- Falcon arbeitet ohne ständige Signatur-Updates, komplizierte Integrationen oder spezielle Geräte vor Ort
- Der schlanke Agent belastet die Endgeräte kaum – ganz gleich, ob es sich um die Erstinstallation oder den täglichen Einsatz handelt. Nach Installation ist kein Neustart erforderlich
- Der minimale CPU-Overhead holt verlorene Systemleistung und Endbenutzerproduktivität zurück
- Die Lösung arbeitet auf Anhieb, ist in wenigen Minuten implementiert und sofort einsatzbereit
- Falcon Prevent ist dank cloud-nativer Architektur und SaaS-Bereitstellung stets auf dem aktuellen Stand
- Falcon unterstützt eine Vielzahl von Plattformen, einschließlich Windows, Windows Server, macOS und Linux

**HAFTUNGSausschluss:** Gartner spricht keine Empfehlung für die in seinen Marktforschungspublikationen genannten Anbieter, Produkte oder Services aus. Gartner empfiehlt Anwendern nicht, nur solche Anbieter auszuwählen, die die höchsten Einstufungen erhalten haben. Die Marktforschungspublikationen von Gartner geben die Ansichten der Marktforschungsabteilung von Gartner wieder und sind nicht als Tatsachenbehauptungen auszulegen. Gartner schließt jede stillschweigende oder ausdrückliche Gewähr im Hinblick auf diesen Marktbericht aus, einschließlich der Zusicherung der Marktgängigkeit oder Eignung für einen bestimmten Zweck.

## FALCON PREVENT: AV-ERSATZ LEICHT GEMACHT

Besserer Schutz

Schnelle und einfache Bereitstellung

Optimale Leistung

Geringere Komplexität

## 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 Echtzeitsorgt. 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 weltweit fortschrittlichsten Datenplattformen für Cyber-Sicherheit.

