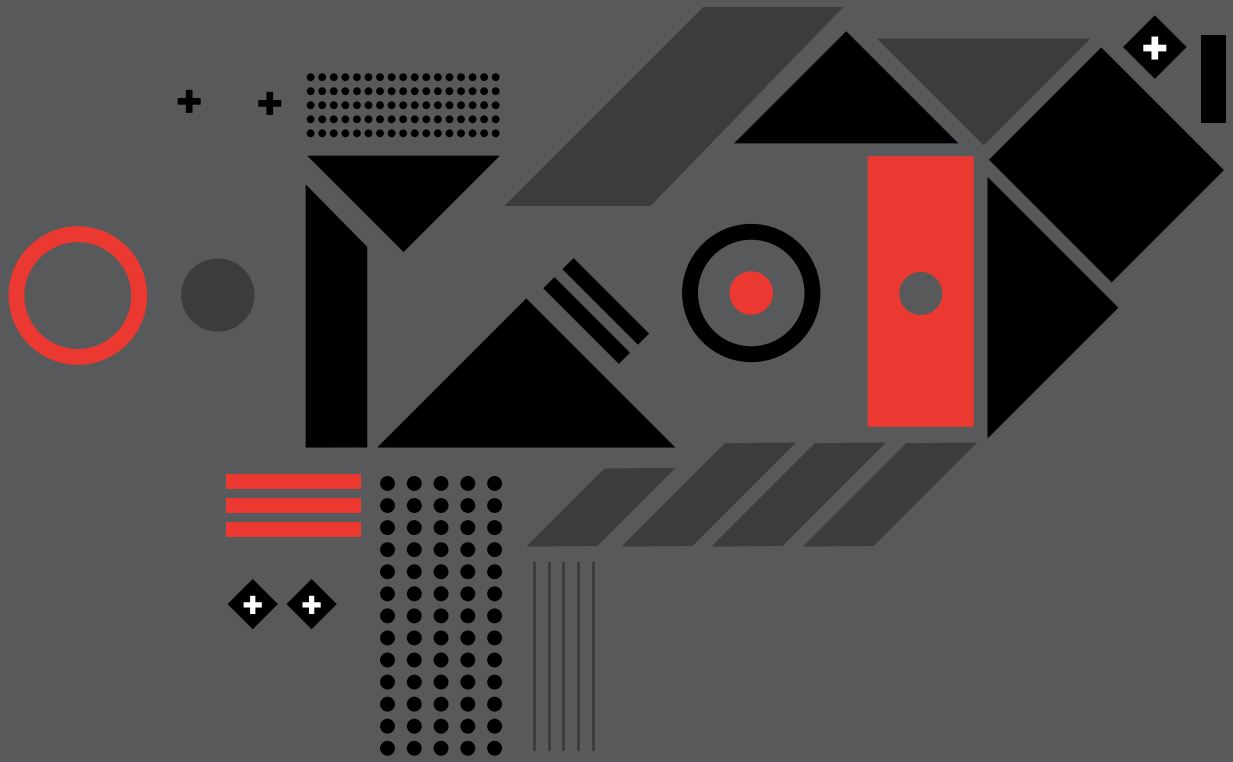
E-Book

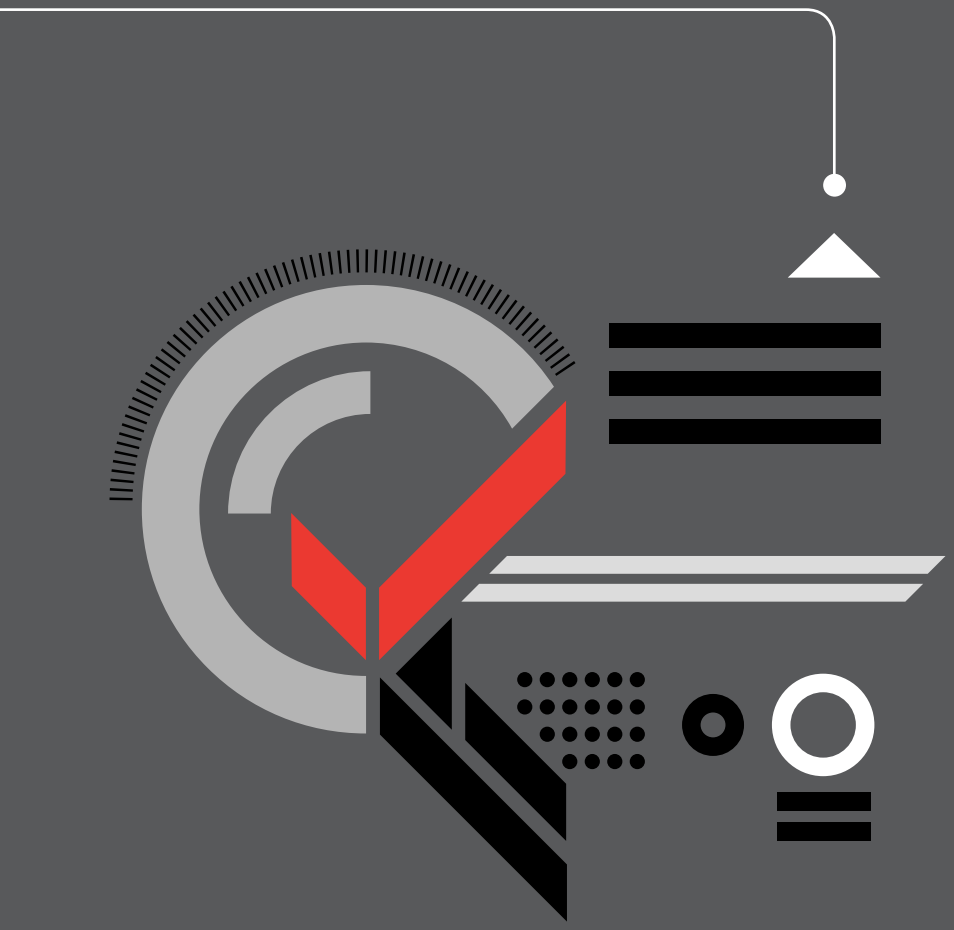


VON ÜBERALL AUS SICHER ARBEITEN

SCHÜTZEN SIE IHRE HYBRIDEN ARBEITSPLÄTZE, SICHERN SIE IHRE DATEN UND STÄRKEN SIE DIE RESILIENZ IHRES UNTERNEHMENS MIT DER CROWDSTRIKE FALCON-PLATTFORM AUF AMAZON WORKSPACES.

CROWDSTRIKE | aws

INHALTSVERZEICHNIS

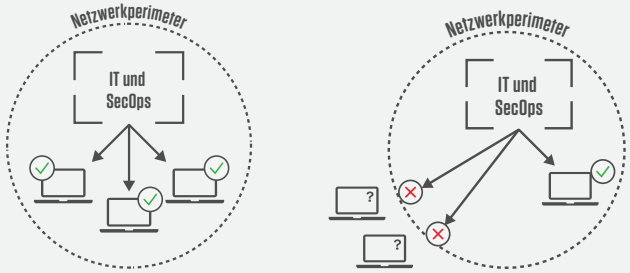


TELEARBEIT SCHWÄCHT PERIMETER

Hybrides Arbeiten wird uns erhalten bleiben. Das Modell, das am meisten Anklang findet, ist ein hybrides Modell, bei dem einige Mitarbeiter vollständig remote bleiben, während andere ins Büro zurückkehren und wiederum andere beides kombinieren und für einen Teil der Woche ins Büro kommen. In der heutigen Zeit des standortunabhängigen Arbeitens vervielfachen sich die Herausforderungen, wenn es darum geht, die Sicherheit aufrechtzuerhalten und die Resilienz des Unternehmens zu gewährleisten. Das alles geschieht zu einer Zeit, in der die meisten Unternehmen immer noch darum kämpfen, mit weniger mehr zu erreichen.

Beschleunigung der Cloud-Implementierung angesichts einer zunehmend hybrid arbeitenden Belegschaft

Viele Unternehmen, die verstärkt auf Hybridarbeit setzen, müssen die Implementierung von Cloud-Technologien beschleunigen. Dazu gehört auch der Wechsel von lokalen Cybersicherheitsmodellen zu Cloud-Lösungen. Nachdem Hybridarbeit mittlerweile den Normalfall darstellt, stellen diese Unternehmen fest, dass ihre neuen, unter zeitlichem und operativem Druck implementierten Ansätze, nicht genügen, um ihre hybrid arbeitenden Mitarbeiter – oder ihre Daten – langfristig zu schützen.



Dementsprechend implementieren weitsichtige Unternehmen einen cloudnativen Cybersicherheits-ansatz basierend auf einem Framework, das umfassenden Schutz an jedem Ort bietet.

Echtzeit-Schutz

Wehren Sie Bedrohungen ab, decken Sie verdächtige Aktivitäten auf und reagieren Sie auf Zwischenfälle – komplett in Echtzeit, ganz gleich, wo sich Ihre Benutzer oder Endgeräte befinden.

Cloudbasierte Bereitstellung

Vermeiden Sie Komplexität, vereinfachen Sie Ihre Sicherheits-lösungen und führen Sie die Bereitstellung in Rekordzeit durch. Mit Falcon Spotlight™ und Falcon Discover™ stehen Ihnen Schwachstellenverwaltung und IT-Hygiene sofort zur Verfügung.

Für jedes Gerät

Der einzelne schlanke Falcon-Agent funktioniert überall (einschließlich Cloud-Workloads und Rechenzentren) und schützt Benutzer auf unternehmenseigenen und privaten Geräten.

Sechs wichtige Faktoren für die Cybersicherheit von Remote-Mitarbeitern

1. Achten Sie darauf, dass Ihre Cybersicherheitsrichtlinie aktuell ist und Remote-Arbeit berücksichtigt.
2. Planen Sie für den Fall, dass BYOD-Geräte (Bring Your Own Device) sich mit Ihrem Unternehmensnetzwerk verbinden.
3. Beachten Sie, dass vertrauliche Daten über unsichere WLAN-Netzwerke abgerufen werden könnten.
4. Cybersicherheit und Transparenz sind unverzichtbar.
5. Kontinuierliche Benutzerschulungen und Kommunikation sind äußerst wichtig und sollten gewährleisten, dass Remote-Mitarbeiter schnell Unterstützung durch die IT-Abteilung erhalten können.
6. Krisenmanagement- und Zwischenfall-Reaktionspläne müssen von Remote-Mitarbeitern ausgeführt werden können.

SCHÜTZEN SIE HYBRIDES ARBEITEN MIT CROWDSTRIKE FALCON® UND AMAZON WORKSPACES

Schützen Sie Ihre Daten und die Identitäten Ihrer Mitarbeiter

Mit Amazon WorkSpaces können standortunabhängige Mitarbeiter eine sichere Desktop-as-a-Service-Lösung nutzen, die von überall aus Zugriff auf ihre Desktops bietet. Durch die Installation des CrowdStrike Falcon-Sensors in einer Amazon WorkSpaces-Umgebung verbessern Sie Ihre Sicherheitslage und reduzieren Risiken durch Cybersicherheitsbedrohungen.

Amazon WorkSpaces bietet eine Desktop-as-a-Service-Lösung für Hybrid-Mitarbeiter

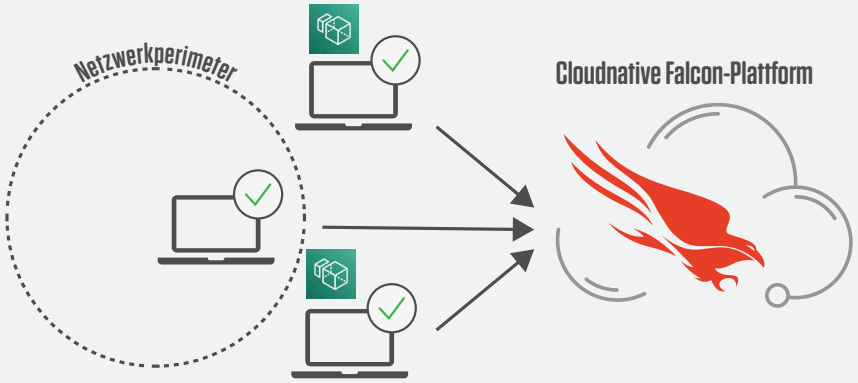
- Bereitstellung eines Cloud-Desktops, der überall mit einer Internetverbindung zugänglich ist
- Kann direkt auf verschiedensten Geräten wie PCs, Macs und iPads ausgeführt werden
- Vermeidet Verwaltungsaufgaben wie die Provisionierung, Bereitstellung und Verwaltung von Desktops

CrowdStrike Falcon-Plattform stoppt Angriffe dank reibungsloser Sicherheit und cloudnativem Endgeräteschutz

- Schnelle Installation aus der Cloud über eine SaaS-Lösung, die alle Geräte unabhängig von ihrem Standort absichert
- Nahtlose Implementierung von Sicherheitsmaßnahmen zur Absicherung sämtlicher potenzieller Arbeitsmodelle, ohne die Leistung zu beeinträchtigen
- Geringere Komplexität mit einer cloudbasierten SaaS-Lösung, die keine Hardware erfordert und die Betriebskosten senkt

DER CROWDSTRIKE-ANSATZ SCHÜTZT VOR ANGRIFFEN

Der schlanke Falcon-Sensor lässt sich einfach in der WorkSpaces-Umgebung von Endbenutzern installieren, um ein sicheres Arbeiten an jedem Ort zu ermöglichen. Gemeinsam verbessern diese cloudnativen Lösungen die Geschäftskontinuität, indem sie vor neuen Bedrohungen schützen, eine sichere Hybridlösung ermöglichen und dank reduziertem Aufwand die Kosten senken.



80 %
aller Angriffe sind mit kompromittierten Anmeldedaten verbunden

Keine Chance für böswillige Akteure

Angesichts neuer Bedrohungen, die Schwachstellen bei der hybrid arbeitenden Belegschaft ausnutzen, ist für zuverlässige Sicherheit die Kombination aus Amazon Virtual Private Network (VPC) sowie Endgerätesicherheit durch CrowdStrike Falcon® unverzichtbar. Schützen Sie Ihre Hybrid-Mitarbeiter mit einer Cybersicherheitslösung, die Machine Learning, künstliche Intelligenz und proaktive Bedrohungssuche kombiniert.

Reaktion, Wiederherstellung und Behebung per Fernzugriff

Falcon bietet Remote-Schutz zur Absicherung der Daten, Workloads und Geräte Ihrer Mitarbeiter unabhängig davon, wo diese arbeiten. Mit der leistungsstarken und cloudnativen Lösung können Sie Hosts schnell wiederherstellen.

Verlagerung der Kosten zur Steigerung der Resilienz

Desktops-as-a-Service per WorkSpaces und die cloudnative Architektur von CrowdStrike Falcon® benötigen erheblich weniger Hardware, Geräte und Software. Mit einem vollständig verwalteten Ansatz verringern Sie den Aufwand und verbessern die Resilienz Ihres Unternehmens.

SCHUTZ VOR RAFFINIERTEN ANGREIFERN

Im Zentrum jedes Cyberangriffs steht ein menschlicher Gegner. Diese Bedrohungsakteure entwickeln sich ständig weiter und nutzen relevante Ereignisse, um ihre Angriffe zu verschleiern.

CrowdStrike hat neue Bedrohungen stets im Visier und den Falcon-Sensor so konzipiert, dass er umfassende Details zu Schwachstellen aufdeckt. Da der Falcon-Sensor mit Amazon WorkSpaces integriert ist, entgeht Ihnen keine einzige Bedrohung für Ihre hybrid arbeitenden Mitarbeiter sowie Ihre Cloud-Daten.

Rundum abgesichert – von der Cloud bis zu Ihnen

Amazon WorkSpaces werden in Amazon VPCs bereitgestellt, die allen Benutzern Zugriff auf persistente und verschlüsselte Speichervolumen in der AWS Cloud bieten und mit AWS Key Management Service integriert sind. Auf dem lokalen Gerät werden keine Benutzerdaten gespeichert, was die Sicherheit von Benutzerdaten verbessert und die Angriffsfläche auch bei der hybrid arbeitenden Belegschaft minimiert.

Erkennung und Prävention in Echtzeit

CrowdStrike Falcon® nutzt Bedrohungsdaten von Threat Graph und bietet die effektivste Erkennung und Abwehr bekannter und unbekannter Bedrohungen in Echtzeit. Dadurch sind die Endgeräte rund um die Uhr vor allen Angreifern geschützt.

Dabei hat CrowdStrike Falcon® jedoch nicht nur Malware im Blick, sondern erkennt auch Kompromittierungsindikatoren (IOCs) sowie Angriffsindikatoren (IOAs).

BEST PRACTICES FÜR CYBERSICHERHEIT IN EINER HYBRIDWELT

Cybersicherheit erfordert für heutige standortunabhängige Arbeitsumgebungen einen anderen Ansatz. Zum Identifizieren von Systemen, Analysieren von Patches und Anzeigen von Schwachstellen benötigen Systeme zur Absicherung von Büro-Benutzern Scans mit hohem Bandbreitenbedarf. Wenn hybride Arbeitsszenarien ins Spiel kommen, ist das jedoch kaum mehr möglich. Mitarbeiter, die nicht ausschließlich im Büro arbeiten und mit verwalteten sowie nicht verwalteten Geräten auf Ihre Daten zugreifen, werden für die IT-Sicherheitsabteilung unsichtbar und schaffen neue Risiken, die die Behebung von Bedrohungen erschweren können.

Um die Cybersicherheitsprobleme des neuen Arbeitsmodells angehen zu können, geben CrowdStrike-Experten folgende Empfehlungen:

Unterstützung der Mitarbeiter und Nutzung verfügbarer Technologien

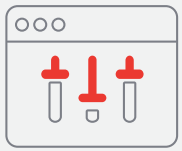
Um eine wirklich umfassende und effektive Cybersicherheitsstrategie entwickeln zu können, müssen Sie Ihre Richtlinien, Prozesse und Technologien in allen Geschäftsbereichen überprüfen. Bei den effektivsten Cybersicherheitsstrategien nutzen Fachleute hochentwickelte Technologielösungen (z. B. mit künstlicher Intelligenz, Machine Learning und anderen Arten von intelligenter Automatisierung), um ungewöhnliche Aktivitäten besser zu erkennen und die Reaktion und Beseitigung zu beschleunigen.

Sorgfältige Auswahl des Cloud-Anbieters

Wenn es darum geht, die Vorteile von Cloud-Technologie zu nutzen, ohne dabei die Sicherheit zu gefährden, tun sich große Unterschiede zwischen den Clouds auf. Bei der Entwicklung von Amazon Web Services (AWS) wurden die höchsten Standards der Datensicherheit eingehalten, sodass detaillierte Identitäten und Zugriffskontrollen hervorragende Transparenz gewährleisten. Die branchenführenden Schutz- und Erkennungsfunktionen von CrowdStrike für Amazon WorkSpaces unterstützen Ihre remote arbeitende Belegschaft, ohne die Geschäftskontinuität zu beeinträchtigen.

Reaktion, Wiederherstellung und Behebung per Fernzugriff

Angesichts unaufhörlicher Angriffe und Infiltrationsversuche müssen Sie sicherstellen, dass Sie über die Ressourcen und Fähigkeiten verfügen, um von überall aus reagieren zu können und Ihr Unternehmen zu schützen. Die cloudbasierte Architektur von Amazon WorkSpaces und CrowdStrike Falcon® gewährleistet mithilfe von Echtzeit-Sicherheitsfunktionen, dass Sie alle Workloads überall schützen können – selbst wenn diese sich außerhalb einer Firewall befinden.



Einfache Desktop-Bereitstellung

Als Cloud-Service erfordert Amazon WorkSpaces weniger Hardware mit Verwaltungsbedarf, zudem sind keine komplexen virtuellen Desktop-Infrastrukturbereitstellungen erforderlich, die sich nicht skalieren lassen. Amazon WorkSpaces ist in 13 AWS-Regionen verfügbar und bietet Zugriff auf leistungsstarke Cloud-Desktops überall dort, wo Ihre Teams arbeiten.

DER AUFBAU EINES SICHERHEITSNETZES BEGINNT MIT KOSTENKONTROLLE

Unternehmen auf der ganzen Welt sind mit einer unsicheren Situation konfrontiert. Um die geschäftliche Resilienz zu stärken und die Ausfallsicherheit zu verbessern, haben sie Wachstumsinitiativen angehalten, Budgets eingefroren und damit begonnen, Bargeldreserven aufzubauen. Mit Amazon WorkSpaces und CrowdStrike Falcon® haben Unternehmen jetzt eine Möglichkeit, Geschäftsprozesse auf sichere Weise bereitzustellen und dabei die Kosten zu senken.

Kostengünstige Cloud-Architektur

Dank der zentralen Verwaltung von Amazon WorkSpaces lässt sich der Zugriff von Remote-Mitarbeitern auf Cloud-Desktops skalieren. Für Ihre hybrid arbeitende Belegschaft müssen Sie keine Hardware oder Software beschaffen, vorbereiten und bereitstellen, um auf dem neuesten Stand zu bleiben sowie Zeit und Geld zu sparen. Außerdem vermeiden Sie mit Amazon WorkSpaces die Anschaffung zu vieler Desktop- und Laptop-Ressourcen, da Sie On-Demand-Zugriff auf Cloud-Desktops erhalten und Ihren Remote-Mitarbeitern auf diese Weise die benötigten Computing-, Arbeitsspeicher- sowie Speicherplatz-Ressourcen bereitstellen können. Die CrowdStrike Falcon-Plattform scannt alle Endpunkte, um ihre Sicherheit unabhängig von ihrem Standort und ohne Leistungseinbußen zu gewährleisten.

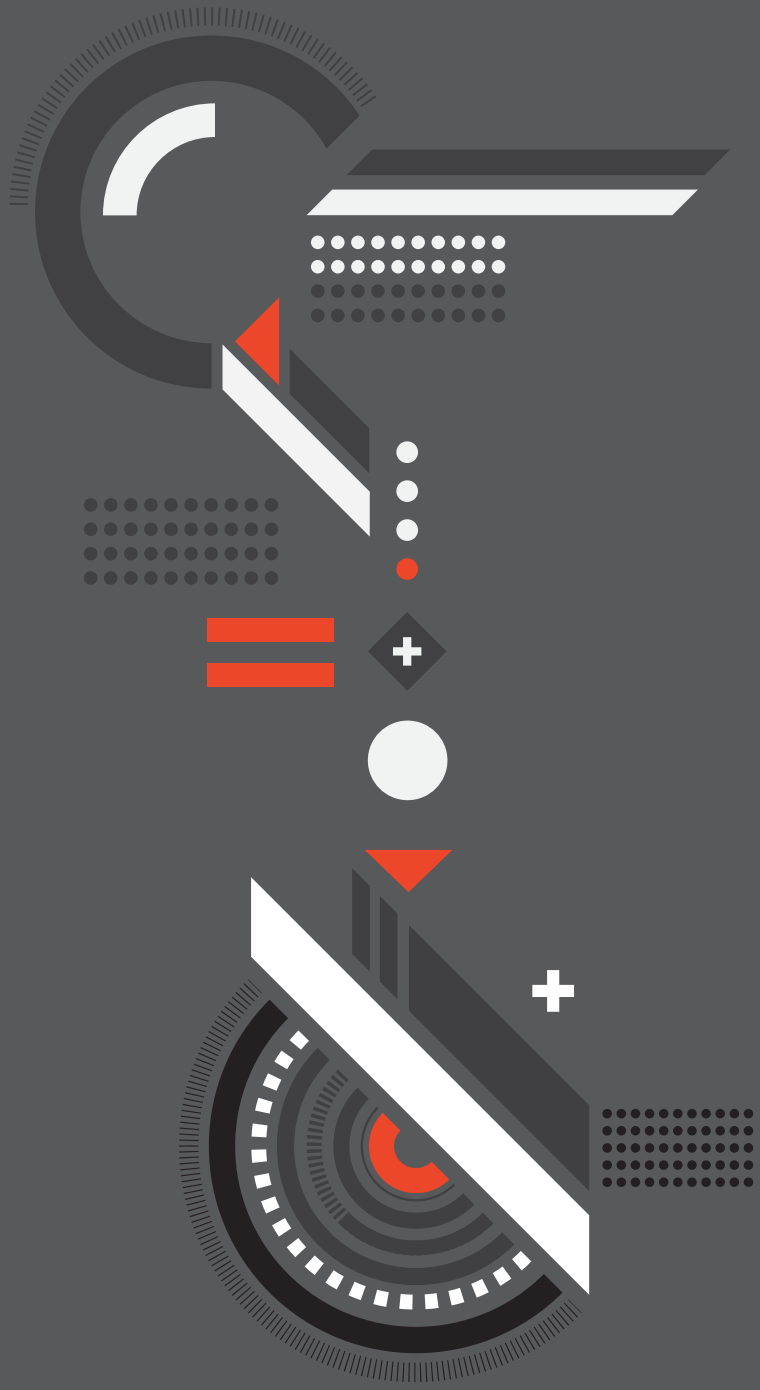
Weniger Aufwand durch vollständige Verwaltung

Durch die Bereitstellung von Falcon-Endgeräteschutz als vollständig verwalteten Service können Unternehmen ihre Cybersicherheit erheblich stärken. Mit dieser Rundum-sorglos-Lösung können Sie die Implementierung und Verwaltung der Endgerätesicherheit sowie die Vorfallreaktion dem bewährten CrowdStrike-Sicherheitsteam überlassen. Ihr Vorteil: Sofort optimierte Sicherheit ohne den Aufwand und die Kosten für die interne Verwaltung eines umfassenden Endgeräte-Sicherheitsprogramms.

SICHERN SIE IHRE ARBEIT VON ÜBERALL AUF DER WELT

CrowdStrike macht den Einstieg zum Kinderspiel. Um mehr über die Implementierung der CrowdStrike Falcon-Plattform bzw. Amazon WorkSpaces zu erfahren, **probieren Sie unsere 15-tägige kostenlose Testversion aus**.

Weitere Informationen zu CrowdStrike- und AWS-Lösungen erhalten Sie bei **CrowdStrike** oder im **AWS Marketplace**.



aws marketplace