CROWDSTRIKE

FALCON ZERO TRUST

MIT RISIKOBASIERTER AUTHENTIFIZIERUNG DATENDIEBSTAHL WIRKSAM VERHINDERN

KOMFORTABLER IDENTITÄTSSCHUTZ FÜR MEHRERE VERZEICHNISDIENSTE VOR ORT UND IN DER CLOUD

CrowdStrike Falcon Zero Trust sorgt für eine komfortable Umsetzung des Zero-Trust-Sicherheitsmodells mit Bedrohungsprävention in Echtzeit und Durchsetzung von IT-Richtlinien anhand von Identitäts-, Verhaltens- und Risikoanalysen. 80 % der Datendiebstähle gehen mit kompromittierten Zugangsdaten einher. Segmentierung der Identitäten, automatische Durchsetzung von Richtlinien und ein risikobasierter, bedingter Zugang zur Verifizierung des Authentifizierungsverkehrs können Gefahren wirksam reduzieren und gleichzeitig zur Senkung der IT-Komplexität beitragen. Schon mehr als 100 große Unternehmen schützen so insgesamt die Identität von mehr als 4 Millionen Mitarbeitern in hybriden Umgebungen.

WICHTIGE PRODUKTMERKMALE

SEGMENTIEREN

Erkennen Sie Sicherheitslücken in Identitätsspeichern durch einen detaillierten und kontinuierlichen Einblick in Konten und Aktivitäten und versetzen Sie Ihre IAM- und Sicherheitsverantwortlichen in die Lage, die damit verbundenen Risiken besser zu bewerten.

Kontinuierliche Sichtbarkeit über mehrere Verzeichnisdienste hinweg – Verschaffen Sie sich einen fundierten Einblick in den Umfang und die Auswirkungen von Zugangsberechtigungen für Identitäten in Microsoft Active Directory und Azure AD.

Automatische Klassifizierung aller Konten – Klassifizieren Sie Identitäten automatisch als hybride (Identitäten, die sich vor Ort und in der Cloud AD befinden) und als reine Cloud-Identitäten (Identitäten, die sich nur auf Azure AD befinden), und segmentieren Sie die Konten nach Personenkonten, Servicekonten, freigegebenen (gemeinsamen) und privilegierten Konten.

WESENTLICHE VORTEILE

- Mehrwert von Anfang an
- Einheitliche Sichtbarkeit und Kontrolle des Zugangs zu Anwendungen, Ressourcen und Identitätsspeichern in hybriden Umgebungen
- Reduzierung der mittleren Erkennungs- und Behebungszeit (MTTD/R) sowie höhere Effizienz und kürzere Antwortzeiten von SOC-Analysten, da die mühsame und fehleranfällige Sichtung komplexer Protokolle entfällt
- Bessere Alarmqualität und genauere Ergebnisse, indem echte Vorfälle beim Zugang mit Identitätsprüfung erkannt und automatisch gelöst werden
- Durchsetzung konsistenter risikobasierter Richtlinien nach dem Zero-Trust-Modell (Aktionen: Blockieren, Erlauben, Prüfen oder verstärkte Prüfung durch Multi-Faktor-Authentifizierung) ohne Reibungsverluste
- Geringere Kosten für die Protokollspeicherung, da nur relevante Authentifizierungsprotokolle gespeichert werden
- Höhere Rentabilität der Investitionen in Multi-Faktor-Authentifizierung durch Ausweitung auf Legacy-Anwendungen und Tools

FALCON CLOUD WORKLOAD PROTECTION

Konfigurierbare Übersicht zur Sicherheitsaufstellung – Analysieren Sie Benutzerrisiken und Verhaltensänderungen im zeitlichen Verlauf, wie beispielsweise die Häufung von Kontosperren, risikobehaftete Endgeräte, kompromittierte Kennwörter usw. So verschaffen Sie sich einen Überblick über die Angriffsfläche Ihrer Organisation.

AUTOMATISIEREN

Erkennen Sie Identitätsbedrohungen in Echtzeit, ohne Protokolle durcharbeiten zu müssen. So vermeiden Sie riskante Mutmaßungen und können sich auf Authentifizierungsaufgaben konzentrieren, die auf über 100 Verhaltensanalysen und Risikofaktoren für jedes Konto basieren.

Schutz hybrider Identitätsspeicher:
Bewerten Sie kontinuierlich die Konfiguration von Verzeichnisdiensten, z. B. Group Policy Objects (GPO), LDAP-Konfigurationen und riskanten Protokollen. Analysieren Sie alle vor Ort und in hybriden Identitätsspeichern geführten Konten. Untersuchen Sie den laufenden Authentifizierungsverkehr, einschließlich verschlüsselter Protokolle (z. B. LDAP/S).

Keine Protokolle, Bedrohungserkennung in Echtzeit:
Nehmen Sie eine kontinuierliche Bewertung von Identitätsereignissen in Echtzeit vor und ordnen Sie diese automatisch Bedrohungen und böswilligen Aktivitäten zu, ohne Protokolle einsehen zu müssen. Die vorkonfigurierten Erkennungsregeln in Falcon Zero Trust auf Basis von Machine Learning machen es möglich. Mit erweiterter Analytik und patentierten Machine-Learning-Technologien decken Sie Ausspähungsaktivitäten auf (Tools wie BloodHound oder SharpHound sowie Angriffe auf LDPA und Zugangsdaten), Seitwärtsbewegungen (z. B. RDP, Pass the Hash (PtH), Mimikatz, ungewöhnliche Endgeräte-Nutzung, ungewöhnliche Service-Logins usw.) und Persistenzmechanismen (z. B. Golden-Ticket-Angriffe, Eskalation von Rechten usw.).

Intuitive Bedrohungssuche:
Ermitteln Sie schneller mit zentralem Zugriff auf detaillierte Aktivitäten jedes Kontos über hybride Identitätsspeicher hinweg, ohne komplexe, string-basierte Abfragen durchführen zu müssen. Wählen Sie aus mehreren vordefinierten Suchkriterien: Authentifizierungsereignisse, Verwendung unverschlüsselter Protokolle, Benutzerrollen, IP-Reputation, Risikobewertungen und vieles mehr. Erstellen und speichern Sie bei Bedarf Ihre eigenen Suchkriterien, um Rohereignisse proaktiv zu sichten und in Form periodischer Berichte per E-Mail zu versenden.

Umfassende API-Abdeckung:
Erweitern Sie die Risikoeinstufung und vertrauenswürdigen Informationen der Falcon-Plattform mit minimalem Aufwand über API-basierte Konnektoren auf andere Anwendungen (z. B. ADFS, SSO, IT-Systeme und mehr als 50 Integrationen).

REIBUNGSLOSE UMSETZUNG DES ZERO-TRUST-MODELLS

Unterstützung der Identitätsebene mehrerer Verzeichnisdienste
CrowdStrike Falcon Zero Trust unterstützt Microsoft Active Directory, Azure Active Directory und lässt sich in SSO- und Federation-Lösungen integrieren, wie beispielsweise ADFS, PingFederate und Okta.

Umfassende Unterstützung der Multi-Faktor-Authentifizierung
CrowdStrike Falcon Zero Trust unterstützt mehrere MFA-Lösungen, darunter Azure MFA, PingID, RSA CAS, Duo, Okta und viele weitere.

Erweiterte Protokollabdeckung
CrowdStrike Falcon Falcon Zero Trust verleiht detaillierte Einblicke und Kontrolle über verschlüsselte Protokolle wie NTLM und LDAPS, die mit herkömmlichen Tools wie SIEM und UEBA nur schwer zu erkennen sind.

Umfassende API-Abdeckung
CrowdStrike Falcon Zero Trust unterstützt mehr als 50 Integrationen mit API-basierten Konnektoren, die eine einfache Einbindung in IDaaS/SSO-, SIEM-, SOAR-, Ticketing- und Asset-Management-Lösungen ermöglichen.

ÜBERPRÜFEN

Schützen Sie den Benutzerzugang zu Anwendungen, Tools und Ressourcen ohne Reibungsverluste. Stellen Sie eine einheitliche Anmeldepraxis für reale Benutzer sicher. Verstärken Sie automatisch die Authentifizierung, wenn das Risiko steigt.

Komfortable Identitätsüberprüfung mit flexiblen Richtlinien:
Definieren und erzwingen Sie Richtlinien anhand einfacher Regeln mit der adaptiven Analyse von Falcon Zero Trust. Dadurch entfällt die Notwendigkeit, komplexe statische Bedingungen für jeden Benutzer zu erstellen. Die Regeln beruhen auf Authentifizierungsmustern, Verhaltensgrundmustern und individuellen Risikobewertungen. So werden Identitäten mithilfe von MFA verifiziert und der Zugriff auf Identitätsspeicher und Anwendungen wird gesichert. Gleichzeitig wird die Anmeldepraxis für Benutzer verbessert, d. h. die Identitätsverifizierung wird nur dann ausgelöst, wenn das Risiko steigt oder wenn eine Abweichung vom normalen Verhalten vorliegt.

Verbesserte Sicherheitslage mit erweiterter Multi-Faktor-Authentifizierung (MFA) –
Erweitern Sie die Identitätsüberprüfung/MFA auf jede Ressource oder Anwendung, einschließlich älterer/proprietärer Systeme und Tools, die bislang nicht in MFA integriert werden konnten. Dies betrifft beispielsweise Desktops, die nicht von cloud-basierten MFA-Lösungen abgedeckt werden, und Tools wie PowerShell sowie Protokolle wie RDP über NTLM. Reduzieren Sie damit Ihre Angriffsfläche.

Automatische Behebung von Sicherheitsvorfällen:
Beheben Sie mit den konfigurierbaren Durchsetzungsrichtlinien der Falcon-Plattform die vom Benutzer autorisierten Vorfälle mithilfe von Identitätsprüfungsmethoden (2FA/MFA). So können sich Ihre Sicherheitsanalysten auf die wichtigen Sicherheitsvorfälle konzentrieren. Darüber hinaus haben Sie die Möglichkeit, diese Vorfälle durch die unkomplizierte API-Integration in SOAR- und Ticketing-Plattformen zu beheben.

ÜBER CROWDSTRIKE

CrowdStrike ist der führende Anbieter beim cloudbasierten Endgeräteschutz. Die Plattform CrowdStrike Falcon® sorgt auf Anhieb für Transparenz und Schutz im gesamten Unternehmen und verhindert Angriffe auf Endgeräte innerhalb und außerhalb des Netzwerks – unterstützt durch verwaltete Bedrohungssuche rund um die Uhr.
Es gäbe noch viel darüber zu sagen, wie CrowdStrike Falcon den Endgeräteschutz neu definiert. Aber unter dem Strich sollten Sie vor allem eines über CrowdStrike wissen:
Wir stoppen Datendiebstahl.

Testen Sie jetzt kostenlos den Virenschutz der nächsten Generation

Erfahren Sie mehr unter **www.crowdstrike.de**