

Schutz, Management und Kontrolle für den Benutzerzugriff auf Daten

Forcepoint mit Identitäts- und Zugriffsmanagement (IAM) von Okta



Herausforderung

- › Transparente Informationen über das Benutzerverhalten von Mitarbeitern im Unternehmen, die sich von verschiedenen Orten oder von verschiedenen Geräten aus anmelden.

Lösung

- › FBA nutzt Verhaltensdaten, um das Risiko zu minimieren.
- › DEP ermöglicht einen sicheren Zugriff auf Cloud- und lokale Umgebungen.
- › Okta Identity Cloud gewährleistet sichere Passwörter und authentifiziert und schützt die Anmeldedaten für Anwendungen in Cloud-Umgebungen durch SSO.

Ergebnis

- › Nutzen Sie Ihre bestehenden Investitionen in Forcepoint, um Vorfälle in Folge eines gehackten Zugriffs zu erkennen, zu verwalten und zu beseitigen.

Wenn die digitale Transformation die Cyber-Sicherheit überholt, entstehen Schlupflöcher, über die böswillige Personen ungeschützte Netzwerke angreifen können. Ein wirkungsvolles Cyber-Sicherheitskonzept beginnt deshalb mit der Identifizierung jedes einzelnen Benutzers – unabhängig von dessen Standort – und der permanenten Bewertung des von ihm ausgehenden Risikos, um so einen sicheren Zugriff zu gewährleisten. Forcepoint arbeitet mit Okta zusammen, um integrierte, für die Cloud konzipierte IAM-Services (Identity Access Management) nach dem Zero-Trust-Prinzip bereitzustellen. Diese bieten eine dynamische, lückenlose Sicherheit, indem sie die Benutzeridentität ermitteln, und schützen vor Sicherheitsrisiken für Anwendungen und Benutzer.

Forcepoint Behavioral Analytics (FBA) und Forcepoint Dynamic Edge Protection (DEP)

Das Wissen um die Identität und das Verhalten der Benutzer sind zwei entscheidende Faktoren, um den Zugriff von Benutzern mit hohem Risiko auf Netzwerkdaten und Unternehmensressourcen zu verhindern. Die FBA- und DEP-Lösungen arbeiten Hand in Hand, um Sicherheitslücken zu schließen und die Compliance zu optimieren. Dies steigert die Produktivität – sowohl die der Sicherheitsanalysten, da Fehlalarme vermieden werden, als auch die der Anwender, da sie einen schnelleren Zugriff auf Cloud-Anwendungen erhalten.

Forcepoint DEP bietet Management und Schutz für Web-, Cloud- und private Anwendungen

DEP ermöglicht, allen Mitarbeitern – egal ob diese zu Hause, im Büro oder unterwegs arbeiten – einen kontrollierten Zugriff auf Web-, Cloud- und interne Anwendungen bereitzustellen und sie vor komplexen Bedrohungen und Datenverlusten zu schützen.

DEP-Lösung

- Das Cloud Security Gateway (CSG) sichert den Benutzerzugriff auf SaaS-Anwendungen und das öffentliche Internet.
- Private Access (PA) bietet einen Zero-Trust-Remote-Zugriff auf private Anwendungen ohne die Nachteile von VPNs.

FBA-Lösung

Die Verhaltensanalysen von Forcepoint (Forcepoint Behavioral Analytics oder kurz FBA) liefern Einblicke in riskante Verhaltensweisen und Personen, indem die Interaktionen zwischen Menschen, Daten, Geräten und Anwendungen ausgewertet werden.

- **Aussagekräftige Inhalte:** Unterschiedliche Datenquellen werden zu einem Gesamtbild zusammengefügt. Zum Entschlüsseln der Absichten werden dabei neben ergänzenden SIEM-, Endpunkt- und Mitarbeiterdaten auch Kommunikationsinhalte herangezogen.

- **Hybrid-Analysen:** Verschiedene Arten von verhaltens- und inhaltsbasierten Analysen werden angewendet, die vorrangig nach Änderungen, Mustern und Anomalien suchen, um Angriffe besser zu erkennen.
- **Suche und Erkennung:** Leistungsstarke Werkzeuge für die forensische Suche und Erkennung werden über eine kontextbasierte Benutzeroberfläche bereitgestellt, die eine kontinuierliche Überwachung und eingehende Untersuchung ermöglichen.
- **Intuitiver Workflow:** Die aktiv bereitgestellten Berichte lassen sich vollständig in den Workflow der Mitarbeiter und in bestehende Kundeninformationsarchitekturen integrieren, um die betriebliche Effizienz zu optimieren.

Okta Identity Cloud-Plattform

Die Okta-Plattform liefert eine vollständige Identitätsebene für jede Anwendung und bildet die Grundlage für sichere Verbindungen zwischen Mensch und Technologie. Okta macht sich die Vorteile der Cloud zunutze und ermöglicht es den Mitarbeitern, jederzeit und von jedem Gerät aus auf Anwendungen zuzugreifen, während gleichzeitig umfassende Sicherheitsmaßnahmen angewendet werden.

Die Okta-Produktfamilie umfasst die Basisprodukte Okta Single Sign-On (SSO) und Okta Adaptive Single Sign-On sowie eine Vielzahl verfügbarer Add-ons – darunter

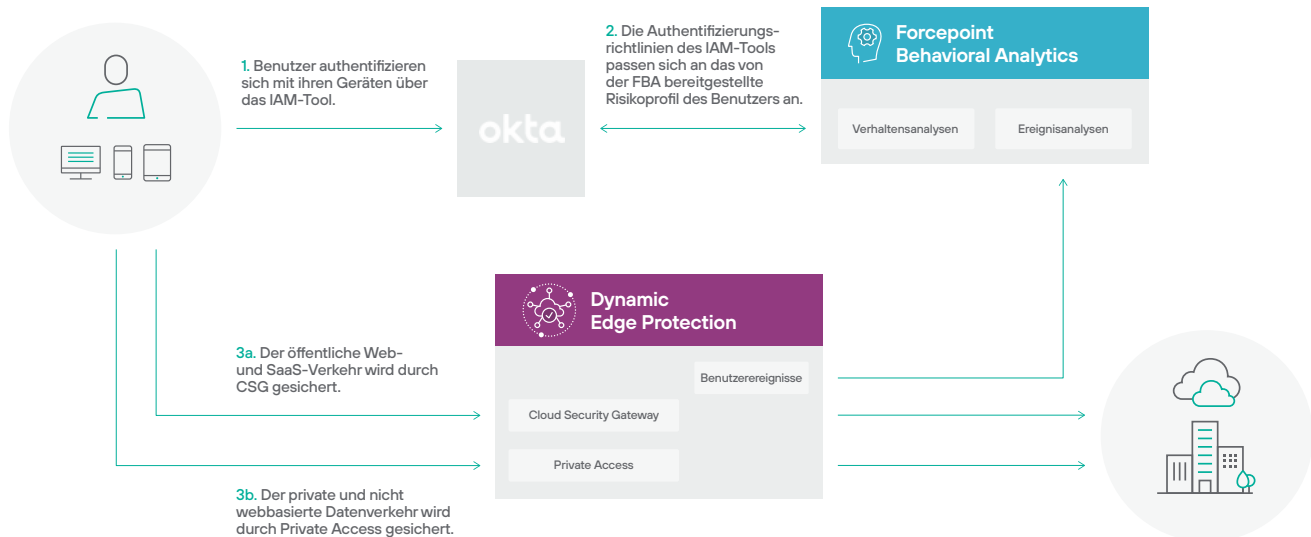
Universal Director, Adaptive Multi-Factor Authentication und API Access Management –, die eine umfassende adaptive und kontextbezogene Authentifizierung ermöglichen.

Gemeinsam mehr erreichen: Forcepoint Zero-Trust-Dienste kombiniert mit Okta Identity Cloud

Durch die Kombination von FBA mit der Okta-Plattform entsteht eine Komplettlösung für Identität, Sicherheit und Risikoschutz. Benutzer können die kontextbezogene und adaptive Authentifizierung von Okta auf ihren eigenen Geräten oder auf vom Unternehmen bereitgestellten Geräten nutzen. Von Okta erstellte Systemprotokolle werden von FBA und DEP eingelesen, um Ereignisse und Benutzerverhalten zu analysieren. Anschließend wird ihnen eine Risikobewertung zugewiesen, die unter Verwendung der Benutzer- und Gruppen-ID von Okta gespeichert wird.

Für Konten, die eine hohe Risikobewertung erhielten, kann Okta die Mitgliedschaft dahingehend ändern, dass eine aktive Sitzung beendet, SSO verhindert und eine Neuansmeldung erzwungen wird. Jeder neue Anmeldeversuch durchläuft denselben Prozess, bei dem der Zugriff basierend auf dem Risiko des Benutzers analysiert wird. Benutzer, denen Zugriff erteilt wird, können im Anschluss sicher auf Datenverkehr im Web zugreifen, der durch Forcepoint DEP Zero-Trust-Dienste geschützt wird.

Diagramm der IAM-Integration



forcepoint.com/contact