

Schutz, Management und Kontrolle für den Benutzerzugriff auf Daten

Forcepoint mit Identitäts- und Zugriffsmanagement von Ping



Herausforderung

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

Lösung

- › Das Benutzerverhalten wird von Forcepoint analysiert und mit einer Risikobewertung versehen. Im Falle einer hohen Risikobewertung kann Ping die Ergebnisse analysieren und zusätzliche Kontrollen durchsetzen, wie z. B. eine mehrstufige Authentifizierung.

Ergebnis

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

Durch die digitale Transformation können Schlupflöcher entstehen, über die böswillige Personen ungeschützte Netzwerke angreifen können. Sicherheitsbeauftragte haben die Aufgabe, die vielen neuen Möglichkeiten des ortsunabhängigen Arbeitens abzusichern und Daten zu schützen – unabhängig davon, wo und wie sie genutzt werden. Es beginnt damit, das Benutzerisiko und den Zugriff auf Umgebungen innerhalb einer Organisation zu bestimmen. Forcepoint arbeitet mit Ping zusammen, um integrierte, für die Cloud konzipierte Services nach dem Zero-Trust-Prinzip bereitzustellen. Diese bieten eine lückenlose Sicherheit, indem sie die Benutzeridentität ermitteln, und schützen vor Sicherheitsrisiken für Anwendungen und Benutzer.

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

Das Wissen um die Identität und das Verhalten der Benutzer sind entscheidende Faktoren, um bedrohliches Verhalten zu erkennen, bevor Benutzer auf Netzwerkdaten und Unternehmensressourcen zugreifen. Die FBA- und DEP-Lösungen arbeiten Hand in Hand, um Sicherheitslücken zu schließen und die Compliance zu optimieren, sodass eine gesteigerte Produktivität erzielt wird.

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

Die DEP-Lösung ermöglicht es, allen Mitarbeitern – unabhängig davon, wo diese arbeiten – einen kontrollierten Zugriff auf Web-, Cloud- und private Anwendungen bereitzustellen und sie vor komplexen Bedrohungen und Datenverlust 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 interne 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.

PingFederate Single-Sign-On

PingFederate ist eine moderne Lösung für das Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM), die für komplexe Anforderungen in Unternehmen entwickelt wurde. Durch die Integration von Identitäts- und Anwendungssilos innerhalb des Unternehmens, zwischen Partnern und in der Cloud bietet PingFederate folgende Möglichkeiten:

- SSO und Identitätsverbund
- Registrierung, Profilverwaltung und Kennwörterücksetzung
- Adaptive Authentifizierungsrichtlinien
- Anmeldung über soziale Medien und Kontoverknüpfung

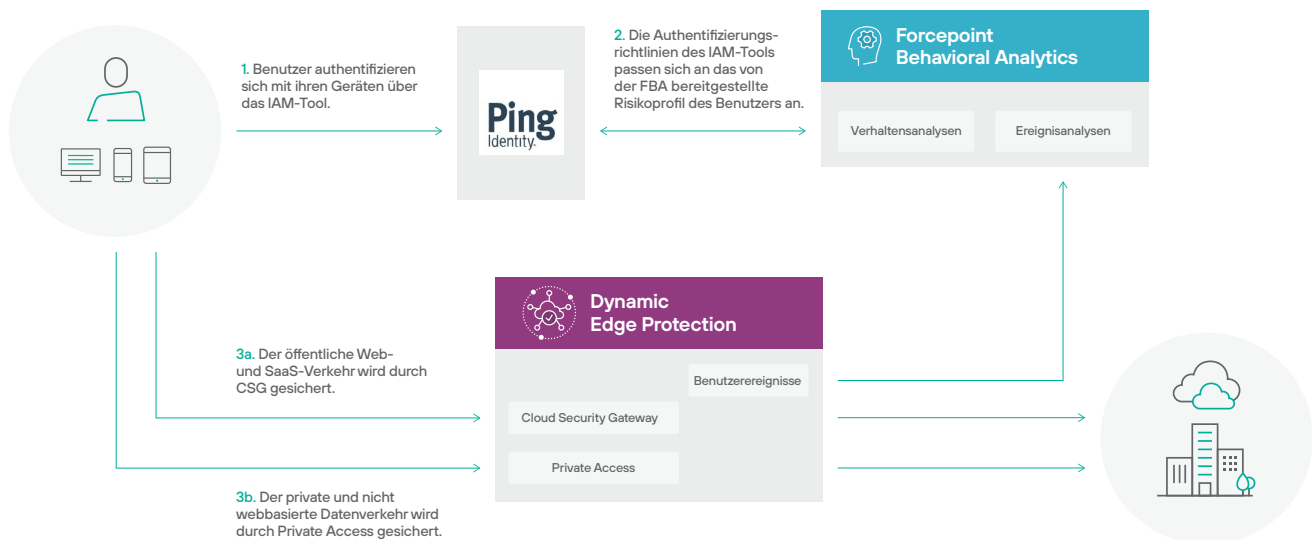
PingFederate ermöglicht einen benutzerfreundlichen, sicheren Zugriff auf praktisch alle Anwendungen, einschließlich SaaS-, Web-, Mobil- und Legacy-Anwendungen. Durch Richtlinienkontrollen wird ein optimales Gleichgewicht zwischen Sicherheit und Komfort für eine breite Palette von Anwendungsfällen erreicht.

Gemeinsam mehr erreichen: Forcepoint Zero-Trust-Dienste kombiniert mit PingFederate

Durch die Kombination der DEP-Lösung mit PingFederate entsteht eine Komplettlösung für Identität, Sicherheit und Risikoschutz. Benutzer können die kontextbezogene und adaptive Authentifizierung von PingFederate auf ihren eigenen Geräten oder auf vom Unternehmen bereitgestellten Geräten nutzen. Von PingFederate 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 PingFederate gespeichert wird.

Für Konten, die eine hohe Risikobewertung erhielten, kann PingFederate 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 Architektur



forcepoint.com/contact