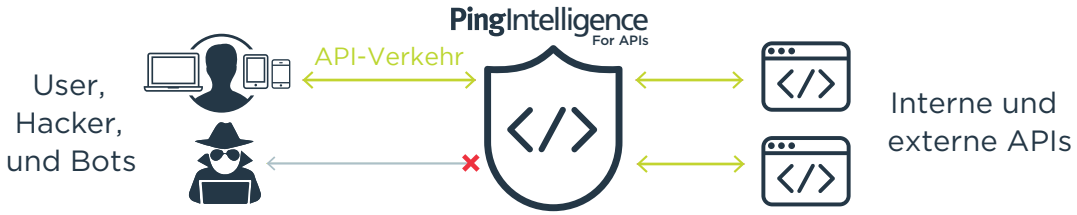
PingIntelligence For APIs

DATENBLATT

API-basierte Digital-Transformation-Initiativen sorgen zunehmend dafür, dass Geschäftslogik und Daten für interne und externe Benutzer leicht zugänglich sind. Allerdings öffnen APIs auch neue Einfallstore für Hacker und Cyberkriminelle, die es auf Daten und Systeme abgesehen haben. Vordefinierte Regeln, Richtlinien und Angriffssignaturen können mit dieser dynamischen Bedrohungslandschaft kaum Schritt halten. PingIntelligence for APIs nutzt künstliche Intelligenz (KI), um aktive APIs bereitzustellen, Cyberangriffe auf APIs zu identifizieren und automatisch zu stoppen und detaillierte Berichte zu sämtlichen API-Aktivitäten bereitzustellen. Mit speziell für die API-Sicherheit konzipierten KI-Modellen stellt PingIntelligence for APIs Cybersicherheitsfunktionen sowie umfassende Informationen zum API-Verkehr in bestehenden API-Gateways und anwendungsserverbasierten API-Umgebungen bereit.

PingIntelligence for APIs ist in der Lage, verdächtiges Verhalten in APIs sowie Daten und Anwendungen, die über APIs bereitgestellt werden, zu erkennen und Angriffe in Ihrer API-Umgebung automatisch zu stoppen. Zum Beispiel werden Versuche, Anmeldesysteme mit gestohlenen Tokens oder Credential-Stuffing-Angriffen mithilfe von Botnets zu umgehen, als Cyberangriffe erkannt. Auch anderes ungewöhnliches Verhalten, wie der Versuch, Daten herauszuschleusen, zu verändern oder zu löschen, wird in Echtzeit unterbunden und gemeldet.



PingIntelligence for APIs ermöglicht einen umfassenden Einblick in sämtliche API-Aktivitäten und blockiert Cyberangriffe in allen API-Infrastrukturen.

FUNKTIONEN

- Automatisierte API-Erkennung
- Identifizierung von API-Bedrohungen und automatisierte Abwehr
- API-Verschleierung und Honeypots
- Umfassender Einblick in den API-Verkehr und Reporting
- Verschiedene Implementierungsoptionen
- Unterstützung hybrider IT-Umgebungen
- Selbstlernendes System (es müssen keine Richtlinien und Regeln erstellt werden)

VORTEILE

- Identifizierung unbekannter und inaktiver APIs
- Abwehr von API-Angriffen im Unternehmen
- Schutz der Daten vor Diebstahl und Löschung
- Schutz der APIs vor Störungen oder Deaktivierung
- Unmittelbare Erkennung und Abwehr von Hacker-Angriffen
- Bereitstellung detaillierter forensischer und Compliance-Berichte

PINGINTELLIGENCE-LÖSUNGEN
Cybersicherheit für interne und externe APIs

PingIntelligence for APIs nutzt KI-Modelle und Big-Data-Analysen, um kontinuierlich sämtliche API-Aktivitäten zu prüfen und Berichte dazu zu erstellen. Darüber hinaus ist die Lösung in der Lage, verdächtiges Traffic-Verhalten in API-Umgebungen automatisch zu erkennen. Cyberkriminelle wissen, wie sie statische Sicherheitsregeln umgehen können. Doch dagegen lässt sich etwas tun: PingIntelligence wurde speziell entwickelt, um sich schnell ändernde, dynamische und eigens auf APIs ausgerichtete Angriffe zu erkennen und darauf zu reagieren – ohne Richtlinien, Regeln oder Code schreiben zu müssen.

AUTOMATISIERTE API-ERKENNUNG: Identifizieren Sie auf dynamische Weise versehentlich bereitgestellte bzw. vergessene oder unbekannte APIs in Ihrer Umgebung. Generieren Sie detaillierte Berichte zur Aktivität dieser APIs und halten Sie nach Angriffen auf deren Daten und Anwendungen Ausschau.

API-VERSCHLEIERUNG: Mithilfe von Schein-APIs (Honeypots) können Sie Hacker-Aktivitäten unmittelbar aufdecken. Da autorisierte Clients normalerweise nie auf Schein-APIs zugreifen, sollte der API-Verschleierungsmechanismus umgehend den Angriff erkennen und den Zugriff auf Produktions-APIs verhindern.

DOS-/DDOS-ANGRIFFE: PingIntelligence ist in der Lage, gezielte Denial-of-Service(DoS)- und Distributed-Denial-of-Service(DDoS)-Angriffe auf einzelne APIs zu erkennen und darauf zu reagieren. Dies gilt auch für raffinierte Botnet- und Memory-Flooding-Angriffe, die eine Erkennung vermeiden, indem sie einen bestimmten mengenmäßigen Grenzwert nicht überschreiten.

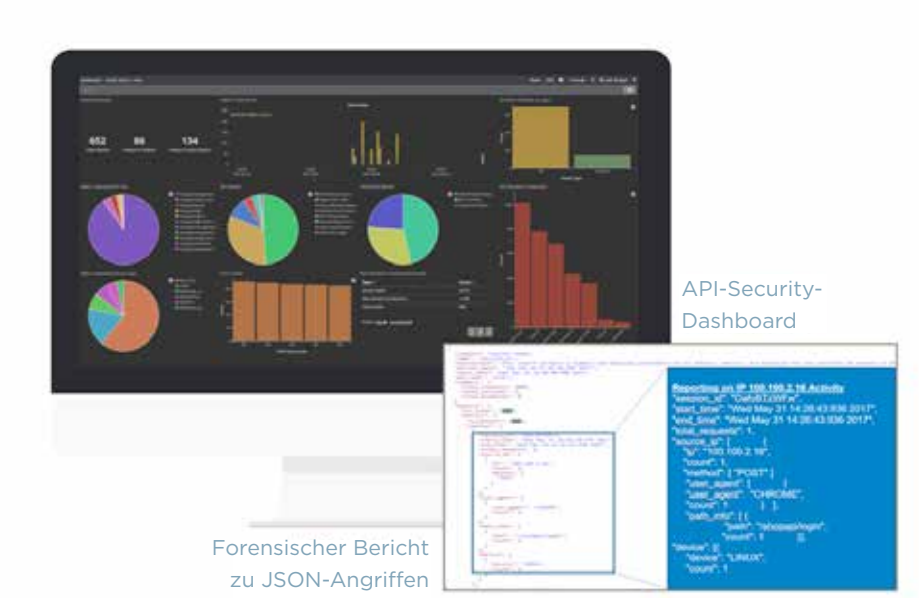
AUTHENTIFIZIERUNGS-/AUTORISIERUNGSANGRIFFE: API-Clients durchlaufen bestimmte Authentifizierungsschritte, sodass PingIntelligence Versuche identifizieren kann, Anmeldesysteme mithilfe von Credential-Stuffing, gestohlenen Cookies oder Token und anderen Methoden zu umgehen, um auf API-Services zuzugreifen.

ANGRIFFE AUF ANWENDUNGEN, SYSTEME UND DATEN: Das Client-Verhalten sowie Anfrage-/Antwort-Flows können je nach API stark variieren. PingIntelligence ist in der Lage, Abweichungen von der Norm zu erkennen und das Herausschleusen, Löschen und Ändern von Daten sowie API-Angriffe, bei denen bösartige Inhalte eingeschleust werden, zu identifizieren.

REPORTING UND MONITORING VON API-VERKEHR UND -ANGRIFFEN

Mit PingIntelligence können Sie sämtliche API-Aktivitäten überwachen – einschließlich aller Befehle und Methoden, die in Sitzungen verwendet werden. Dashboards bieten Ihnen eine grafische Übersicht zu Angriffen, Anomalien und Kennzahlen in der gesamten API-Umgebung. So lassen sich identifizierte APIs, laufende Angriffsaktivitäten und ungewöhnliche Ereignisse leichter nachverfolgen. Die Dashboards lassen sich entweder einzeln implementieren oder über PingIntelligence-REST-APIs in eine interne Prozesskonsole integrieren.

Darüber hinaus können Sicherheitsanalysten forensische Berichte zur Untersuchung historischer Aktivitäten generieren – z. B. um etwa alle APIs und Pfade, auf die ein Hacker im Vorfeld eines Angriffs zugegriffen hat, einzusehen. Für regulierte Branchen ist zu Compliance-Zwecken auch ein detailliertes Reporting aller API-Aktivitäten im Zusammenhang mit Datenbank- und Dateisystemzugriff, Line-of-Business-Anwendungen oder Kontrollsysteme verfügbar.



Integrierte Dashboards und Berichte erlauben die Überwachung der API-Aktivität.

FLEXIBLE IMPLEMENTIERUNG

PingIntelligence for APIs wurde für eine einfache Integration mit Ihrem API-Gateway und eine flexible Implementierung in Kombination mit der Ping Identity-Plattform konzipiert. Zusätzliche Flexibilität beim Architekturdesign bieten sowohl die Inline- als auch die Sideband-Implementierung. Auf diese Weise kann die IT das Modell auswählen, das am besten zu ihrer Umgebung passt. Das Inline-Modell bietet ein hochleistungsfähiges Reverse Proxy, das sämtliche Anwendungen schützt. Alternativ bietet die Sideband-Implementierung mit einem API-Gateway oder PingAccess dieselben KI-basierten Angriffserkennungsmechanismen und umfassenden Einblicke wie die Inline-Option, ohne dass Modifikationen am Netzwerk oder an der Infrastruktur nötig sind.

INLINE-IMPLEMENTIERUNG VON PINGINTELLIGENCE FOR APIs MIT EINEM API-GATEWAY

SIDEBAND-IMPLEMENTIERUNG VON PINGINTELLIGENCE FOR APIs MIT EINEM API-GATEWAY

SIDEBAND-IMPLEMENTIERUNG VON PINGINTELLIGENCE FOR APIs MIT PINGACCESS

SCHUTZ INTERNER UND EXTERNER APIs

Die PingIntelligence-Lösung schützt Sie vor Cyberangriffen und bietet einen umfassenden Überblick über alle API-Aktivitäten auf bestehenden API-Gateways sowie in APIs, die direkt auf Appservern wie Node.JS, WebLogic, Tomcat und WebSphere implementiert sind – egal ob lokal, in der Cloud oder einer Kombination davon. Mit Implementierungsoptionen wie virtuellen Geräten, Docker-Containern und Bare-Metal-Umgebungen unterstützt PingIntelligence automatisierte Installations- und Management-Skripts in gängigen Datencenter- und Cloud-Umgebungen wie AWS.

FLEXIBLE SKALIERUNG

Sie können Ihre API-Sicherheitsinfrastruktur dynamisch erweitern und verkleinern, um hohe Verkehrslasten zu bewältigen und gleichzeitig die Kosten unter Kontrolle zu halten. Profitieren Sie von der automatischen Weitergabe wichtiger Sicherheitsinformationen in hybriden IT-Umgebungen. Dank Echtzeitsynchronisierung und einer konsequenten Regeldurchsetzung an allen Standorten können Sie sich so gegen API-Angriffe auf mehrere Datencenter schützen.

#3341 | 08.23 | Digital v14