IP FABRIC
AUTOMATED NETWORK ASSURANCE PLATFORM

IP Fabric | Sicherheit

Ein proaktiver Ansatz für die Netzwerksicherheit ist für Unternehmen unerlässlich. Je komplexer Ihr Netzwerk wird, desto größer wird auch die Angriffsfläche. Wenn Sie sich auf manuelle Prozesse verlassen, wird Ihr Netzwerk anfällig – das ist ein Risiko, das sich die meisten Unternehmen nicht leisten können.

Gartner
COOL VENDOR 2022

Ihre Herausforderung

Sie wünschten, Sie könnten Ihr Netzwerk einfach danach fragen, was Sie wissen möchten – als würden Sie Ihren Kollegen die Nachricht „Mittagessen um 12 Uhr“ senden?

Teams in Ihrem Unternehmen – sei es Sicherheit, Cloud, Infrastruktur oder Management – können normalerweise nicht auf relevante Daten zugreifen, ohne sich auf Ihr Netzwerkteam zu verlassen. Dies führt zu ineffizienten Prozessen und benachteiligt Mitarbeiter die nicht das gesamte Netzwerk in- und auswendig kennen.

Kennen Sie Ihr Netzwerk wie Ihre Westentasche?

Unsere Lösung

Mit der Netzwerk-Baseline von IP Fabric erhalten Sie ein verlässliches Netzwerkinventar, auf das alle Teams mühelos zugreifen können. Auf diese Weise können Sie überprüfen, ob Hardware, Software und Konfiguration Schwachstellen aufweisen, die Angreifer ausnutzen könnten.

Wir bieten eine klare und präzise Netzwerkübersicht.

Unsere Lösung

- Die Infrastruktur bleibt zweckmäßig (sie erreicht nicht unerwartet das Ende ihrer Lebensdauer).
- Die Konfiguration wird anhand von Best Practice und hinsichtlich der Einhaltung gesetzlicher Vorschriften validiert.
- Angemessene und korrekt angewandte Sicherheitsrichtlinien
- Schützen Sie Ihr hybrides Cloud-Netzwerk

IP Fabric | Sicherheit

80%

der Schwachstellen sind netzwerkbedingt. Zwei Drittel davon könnten durch eine Umstrukturierung eliminiert werden.

QUELLE: EdgeScan 2020 Vulnerability Report.

60%

der Sicherheitsverstöße betrafen Schwachstellen, für die ein Patch verfügbar war, aber nicht installiert wurde.

QUELLE: www.csoonline.com

80%

der Unternehmen haben Sicherheits- und Compliance-Probleme aufgrund der schlechten Zusammenarbeit zwischen Cloud-Teams und traditionellen Netzwerkinfrastruktur-Teams erlebt.

QUELLE: EMA Report 2021

Härten Sie Ihre Netzwerkinfrastruktur gegen Angriffe

Verwalten Sie die Netzwerkgeräten, welche die Weiterleitung sowie die Implementierung von Richtlinien steuern

Umfasst mein Netzwerk Geräte, die anfällig sein könnten?

Verwenden Sie eine Netzwerk-Baseline, um immer eine Antwort auf diese Frage zu haben. Die Point-in-Time-Snapshots von IP Fabric umfassen einen automatischen Erkennungsprozess und bieten umfassende Informationen über die Hardware, Software und Konfiguration Ihres Netzwerks, einschließlich Geräteinventar, Codeversion und mehr.

Nutzen Sie eine simple API-Anfrage, um die Daten, die IPF Ihnen zu Ihrer Netzwerkinfrastruktur liefert, anhand des CVE-Programms (Common Vulnerability and Exposure) zu validieren, um das Ausmaß der Schwachstellen in Ihrer Netzwerkinfrastruktur nachzuvollziehen.

Erfahren Sie mehr über das CVE-Programm.

Ist meine Infrastrukturkonfiguration vor Angriffen geschützt?

IP Fabric ermöglicht eine einfache Standardisierung der Verwaltungskonfiguration: Vereinheitlichen Sie die Authentifizierung, die Überwachungskonfiguration, die Ereignisprotokollierung sowie die Zugriffsmethoden mittels unseren Tests zur Zielverifizierung sowie End-to-End-Pfad-Suchen.

Die Entscheidungsfindung im Hinblick auf die Sicherheitsinformations- und Ereignisverwaltung wird durch eine übergreifende Ansicht des Netzwerks vereinfacht. Mithilfe der Netzwerkerkennung und -visualisierung von IP Fabric können Sie alle Engpässe im Netzwerk, wichtige Verteilungspunkte und vieles mehr in wenigen Minuten auf einen Blick erkennen.

Stellen Sie sicher, dass die Sicherheitsrichtlinien angemessen definiert und korrekt positioniert sind und von einem zentralen Punkt aus eingesetzt werden.

Zero-Trust-Netzwerkzugang

Ein wirksamer Zero-Trust-Sicherheitsansatz setzt voraus, dass die Außengrenzen des Netzwerks angemessen gesichert ist. IP Fabric hilft Ihnen, die Geräte oder Hosts in den Randbereichen Ihres Netzwerks zu identifizieren.

Segmentierung

Eine gut durchdachte Segmentierung Ihres Netzwerks – d. h. die Kontrolle darüber, wie der Datenverkehr durch Ihr Netzwerk fließt, indem eingeschränkt wird, wer oder was auf bestimmte Systeme zugreifen kann – kann Ihre die Leistung und Sicherheit Ihres Netzwerks verbessern. Nutzen Sie IP Fabric, um Ihre Segmentierungsrichtlinien zu validieren und mehr Kontrolle über Ihr Netzwerk zu erhalten.

Das Sicherheitsmodell von IP Fabric unterstützt auch das Hinzufügen einer weiteren Schutzebene durch Mikrosegmentierung (z. B. durch Hinzufügen von Informationen auf der Anwendungsebene), wodurch Sie die volle Transparenz über die Konfiguration und den Betrieb von Netzwerksegmenten erhalten.

Richtlinienautomatisierung

IP Fabric kann zusätzlich zu Ihren Tools zur Automatisierung von Sicherheitsrichtlinien eingesetzt werden, damit Sie einen tieferen Einblick in das Verhalten Ihres Netzwerks erhalten. Automatische Benachrichtigung von Tools über Änderungen und Prüfung, ob die Änderungen die gewünschte Wirkung zeigen.

Cloud-Sicherheit

IP Fabric unterstützt die Durchsetzung von Sicherheitsrichtlinien in der Cloud ebenso wie in Ihren On-Premise-Netzwerken. Ein hybrides Netzwerk sollte niemals Kompromisse bezüglich der Sicherheit erfordern.

IP Fabric führt alles zusammen: Ihre Infrastruktur und die Informationen zu den Sicherheitsrichtlinien befinden sich an einem Ort. Dies ermöglicht kontextbezogene, automatisierte Netzwerkeinblicke auf Knopfdruck.

Kundenmeinungen

Wie S&P Global die Lösungen von IP Fabric in ihrer Netzwerkbetriebsstrategie einsetzt:

> Wenn Sie ein globales Netzwerk aufgebaut und programmierbar gemacht haben und sich auf die Benutzeroberfläche konzentrieren, erhöhen Sie Ihr Sicherheitsrisiko immens. [Zusammen mit IP Fabric] haben wir unseren Ansatz geändert und konzentrieren uns nun auf den Schutz des Netzwerkperimeters mit Zero-Trust-Modellen.

Guruprasad Ramamoorthy,
Global Head of Network Architecture bei S&P Global

Weitere Ressourcen

- Lesen Sie hier mehr über Zero Trust, Segmentierung und Richtlinienautomatisierung.
- Blog-Beitrag: „How vulnerable is my network“
- Blog-Serie: Network Security Assurance – Teil 1 | Teil 2 | Teil 3
- Mehr über das CVE-Programm
- Podcast: How S&P Global built a Network Observability Platform with IP Fabric

ÜBER **IP FABRIC**

IP Fabric bietet Network Assurance für große Unternehmen, indem wir einen digitalen Zwilling der gesamten Netzwerkinfrastruktur erstellen. Dieser enthält Informationen zu allen Technologien und Protokollen in Ihrem Netzwerk und bietet die Möglichkeit, Weiterleitungs- und Sicherheitsszenarien zu simulieren. Das Netzwerkmodell von IP Fabric wird auch als „Network Source of Truth“ (verlässliche Quelle für Netzwerkdaten) für Netzwerkautomatisierungsinitiativen eingesetzt und stellt mittels API sämtliche Informationen des Netzwerks zur Verfügung. IP Fabric wurde von Gartner als „Cool Vendor“ im Bereich Netzwerkautomatisierung im Jahr 2022 anerkannt.

Nehmen Sie uns beim Wort:

FORDERN SIE EINE DEMO AN

Fordern Sie eine Demo an und erfahren Sie mehr darüber, wie Sie die Sichtbarkeit Ihres Netzwerks erhöhen und Zeit einsparen können.

IP FABRIC
AUTOMATED NETWORK ASSURANCE PLATFORM

115 Broadway, 5th Floor
New York, NY, 10006
United States

info@ipfabric.io

Kateřinská 466/40
Prague - 12000
Czech Republic

sales@ipfabric.io

ipfabric.io