illumio

KURZVORSTELLUNG

Implementierung von Zero Trust mit Illumio

Viele Unternehmen kämpfen mit der zunehmenden Komplexität ihrer Infrastruktur und schwenken nun auf ein Zero Trust Modell, ein neues Modell das konsistente Sicherheit für alle Umgebungen gewährleisten kann. Dieses Whitepaper zeigt, wie die Illumio Adaptive Security Platform® (ASP) ein Zero-Trust-Framework überhaupt erst ermöglicht.

Gründe für Zero Trust

Die wachsende Komplexität von Cloud-, Multi-Cloud- und Hybrid-Cloud-Umgebungen hat in Verbindung mit der sich schnell entwickelnden Bedrohungslage dazu geführt, dass herkömmliche Netzwerksicherheit mit den Anforderungen nicht mehr Schritt halten kann. Immer komplexere Anwendungen und fehlende Transparenz führen zu blinden Flecken, unzureichender Erkennung und unzureichenden Durchsetzungsoptionen für Hybrid- und Multi-Cloud-Implementierungen.

Dennoch soll die Cloud Nutzung laut Prognosen in den nächsten zwei Jahren auf fast 80 % wachsen.[1] Bis 2020 werden fast 50 % der Unternehmen einen Großteil ihrer Daten in einer Public Cloud speichern.[2] Unternehmen setzen auf die Cloud, um die Geschäftsabläufe zu beschleunigen. Herkömmliche Sicherheitsmaßnahmen können diese Prozesse jedoch verlangsamen oder – schlimmer noch – sabotieren.

Worin liegt die Gefahr?

Einer der größten Problempunkte aktueller Schutzmaßnahmen sind fehlende Visibilität und Kontrolle über den Ost-West-Traffic in der eigenen Infrastruktur (auch als lateral movement bezeichnet). Da Netzwerksicherheit bislang auf ein- und ausgehenden Datenverkehr durch den Perimeter beschränkt war, unterliegen Angreifer nach dem Überwinden der Perimeter-Firewall(s) häufig keinerlei Einschränkungen. Mit anderen Worten: Die Hacker können sich frei im Netzwerk bewegen, bis sie ihre Ziele erreichen. Ein grundlegendes Problem eines „flachen Netzwerks“.

Die gleichen Netzwerksicherheitsprobleme bestehen auch bei der Cloud, da viele Unternehmen ihre Public-Cloud-Umgebungen als logische Erweiterungen ihrer vorhandenen Rechenzentren betreiben.

Illumio ASP löst das Problem unsichtbarer oder verschleierter Seitwärtsbewegung (lateral movement) in Netzwerkumgebungen. Dazu setzt die Lösung auf Sicherheit durch eine „Default-Deny“-Policy, und zieht sog. Mikro-Perimeter um die Daten und Anwendungen im Rechenzentrum und allen anderen Infrastrukturen.

Was ist Zero Trust?

Bei „Zero Trust“ – zu Deutsch „Kein Vertrauen“ – sagt der Name schon alles. Anstatt davon auszugehen, dass interner Datenverkehr im Netzwerk immer vertrauenswürdig und „sicher“ für zulässigen Zugriff ist, verhindert Zero Trust den automatischen Zugriff von allen Quellen – ob intern oder extern. Das Forrester Zero Trust eXtended (ZTX)-Framework nennt sieben Domänen, bei denen Zero-Trust-Prinzipien angewendet werden sollten, as show in figure 1. Abbildung 2 zeigt, wie sich Illumio ASP in das Framework einfügt.

> "Forrester kam kürzlich zu dem Ergebnis, dass ein Unternehmen mit Zero Trust sein Risiko um 37% oder mehr verringern kann. Es zeigte sich aber auch, dass Unternehmen mit Zero Trust die Sicherheitskosten um 31% verringern und im IT-Sicherheitsbudget Einsparungen im Millionenbereich ermöglichen können.”[3]

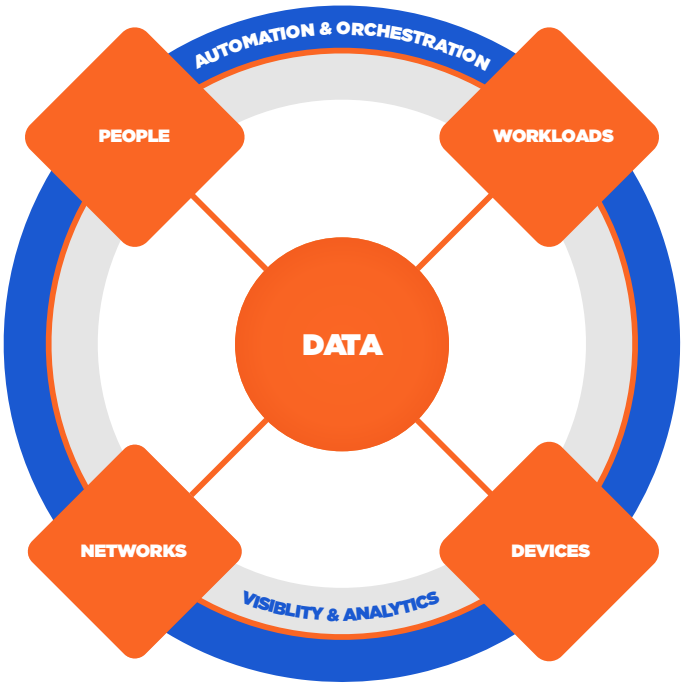

Abbildung 1: Das Zero Trust eXtended (ZTX) Framework

illumio

Framework-Komponenten	Funktionen von Illumio ASP
Netzwerk	• Mikrosegmentierung mit Default-Deny-Policy • Datenbasierte, feingranulare Policy-Modellierung und -Validierung • Enforcement in jeder Infrastruktur • Warnmeldungen bei Verstößen
Daten	• Absicherung von Daten und Anwendungen mit Mikro-Perimetern • Sicherheit folgt den Daten – an jeden Ort • Schutz von Data-in-Transit
Workloads	• Detaillierte Kontrolle von Policy in jeder Skalierung • Durchsetzung auf Prozessebene • Sicherheit folgt dem Workload – an jeden Ort • Einfache Implementierung
Personen	• Benutzer-basierte Segmentierung • Kontrolle über Remote-Zugriffe • Verhinderung lateraler Bewegungen
Geräte	• Segmentierung auf Geräteebene • Erkennung unbekannter Geräte • Gerätequarantäne
Transparenz und Analysen	• Live-Überblick über alle Umgebungen • Einfache Erkennung und Klassifizierung • Gründliche Audits
Automatisierung und Orchestrierunbg	• Integration des Orchestrierungs-Tools • REST-API • CMDB-Integration • CMDB-Hygiene • SIEM-Integration

Abbildung 2: So fügt sich Illumio ASP in das Forrester Zero Trust eXtended Framework ein.

Die Host-basierte Mikrosegmentierung von Illumio ASP schränkt laterale Bewegungen hinter der Firewall effektiv ein, indem sie für alle Zugriffe auf Netzwerkelemente Bestätigungen anfordert. Dabei kommt eine Allowlist zum Einsatz.

Der Allowlist-Ansatz ist hervorragend für das Zero-Trust-Modell geeignet, da er alles blockiert, was Sie nicht explizit zugelassen haben. In heutigen Rechenzentren sind Allowlists eine gute Wahl, da die Liste der gewünschten Verbindungsziele deutlich kleiner ist als die der unerwünschten. So werden False-Positives effektiv verhindert.

Funktionsweise?

Wie können Sie Zero Trust für all Ihre Daten und Anwendungen hinter der Firewall durchsetzen?

Für Zero Trust müssen Regeln und Richtlinien für die Peripherie und interne Schutzmaßnahmen koordiniert werden. In Bezug auf die Architektur müssen Sie Ihre Netzwerke standortübergreifend segmentieren und absichern (Public und Private Cloud), um Bedrohungen auf Mikro-Perimeter-Ebene zu isolieren und zu begrenzen.

Durch die Mikrosegmentierung wird Ihre Netzwerksicherheit von einem Perimeter-basierten „Outside-In"-Schutzmodell zu einem „Inside-Out"-Framework, in dem alles gesperrt ist, was nicht explizit zugelassen wurde. Unternehmen, die Zero Trust für ihre Daten implementieren möchten, können optional auch übertragene Daten innerhalb oder zwischen Mikro-Perimetern absichern.

Zero Trust bedeutet	Zero Trust bedeutet nicht
Standardmäßige Ablehnung von Zugriffen, auch als „Allowlist" oder „default-deny" bezeichnet	Zulassen von Zugriffen, die nicht explizit gesperrt wurden
Vollständige Übersicht über Ihre Umgebung für On-Premise, Cloud, Bare-Metal, virtuelle Maschinen und Container	Fehlende Sichtbarkeit in externe Umgebungen für Policy Entscheidungen und Enforcement
Einheitliche Sicherheit für Workloads unabhängig von ihrem Ausführungsort	Verwaltung unterschiedlicher Policy für unterschiedliche Umgebungen mit Sicherheit, die den Workloads nicht folgen kann
Detaillierte Segmentierung mit Micro-Perimeter zum Isolieren von Daten und Anwendungen nach Rolle, Anwendung, Umgebung oder Standort	Auf den Perimeter beschränkter Firewall-Schutz
Erfolgreiche und unkomplizierte Bereitstellung in großem Maßstab für effektiven Betrieb	Enorme Anstrengungen mit schwachen Ergebnissen

Welche Lösungen sind verfügbar?

Kann Zero Trust mit vorhandenen Investitionen implementiert werden?

Wenn ein Unternehmen seine Switches und Hypervisor mit Software-Defined Networks aufgerüstet hat, würde es sich doch theoretisch anbieten, diese Lösungen auch für Mikrosegmentierung zu nutzen. Allerdings können diese Ansätze weder einheitliches Zero Trust innerhalb und zwischen Umgebungen außerhalb des Netzwerks bieten, noch Transparenz oder Kontrolle gewährleisten.

Herkömmliche Perimeter-basierte Schutzmaßnahmen wurden für Ihr lokales Netzwerk konzipiert und entwickelt. Von der Public Cloud, die Sie mieten, war nie die Rede – und das zeigt sich deutlich. In der Praxis steigern solche Lösungen die Komplexität und schränken gleichzeitig die Übersicht über eine Umgebung ein, die im Gegenteil größere Geschwindigkeit und Flexibilität erfordert.

Was ist also das Geheimnis der Segmentierung Ihrer Daten auf Mikro-Perimeter-Ebene und der einheitlichen Anwendung detaillierter Policys für alle Umgebungen? Um zu verstehen, wie Mikro-Perimeter mithilfe von Sicherheitssegmentierung aufgebaut werden, muss zuerst klar sein, dass es sich nicht um Netzwerksegmentierung handelt. Das Netzwerk spielt letztendlich keine Rolle.

Zero Trust mit Illumio

Wie können Sie eine Zero-Trust-Architektur implementieren, ohne Ihr Netzwerk vollständig umzubauen?

Durch die Nutzung systemeigener Enforcement-Punkte, die bereits in Ihren Anwendungen vorhanden sind und koordiniert werden, um dem Workload überall zu folgen.

Wie funktioniert die Host-basierte Mikrosegmentierung von Illumio?

- Illumio ASP nutzt den äußerst ressourcenschonenden Agenten Virtual Enforcement Node (VEN), um die Betriebssystem-Firewall auf jedem Server in einem Netzwerk zu aktivieren. Dadurch lassen sich Identität, Rolle, Gruppenmitgliedschaft und zugehörige Anwendungen eines Workloads klar definieren.

- Der VEN programmiert die Windows Filtering Platform (WFP) für Windows- und Linux-Kernel-Firewalls, um Policy durchzusetzen. Mithilfe detaillierter Policy-Definition werden explizite Berechtigungen dafür festgelegt, wer kommunizieren darf und welche Workloads zulässig sind. Die Zugriffe nicht autorisierter Benutzer auf Workload-Anwendungen werden blockiert, die Zugriffsversuche protokolliert und Alarme erzeugt. Nicht erforderliche oder nicht autorisierte Kommunikation zwischen Workloads sowie nicht per Policy zugelassene Kommunikation wird ebenfalls blockiert. Das Ergebnis ist eine Übersicht mit intuitiven und einfach zu verwaltenden Abläufen, die Transparenz, Verständnis und Kontrolle gewährleistet.

- VEN-Regeln und -Richtlinien werden über eine zentrale Policy Compute Engine koordiniert, die als „Steuerzentrale“ agiert und umfassende sowie leicht verständliche Übersichten über den Netzwerkverkehr sowie Beziehungen gibt.

- Alle VEN-Informationen werden kombiniert, um die Workflows in Illumination, einer Echtzeit-Karte der Anwendungsabhängigkeiten, darzustellen. Diese Karte liefert einen Überblick über den Datenverkehr über mehrere Umgebungen hinweg sowie Rückmeldungen zu nicht autorisierten Datenflüssen. Die Transparenz ist jedoch auch notwendig, um die Mikrosegmentierungsrichtlinie zu konzipieren und zu testen – schließlich können Sie nur das schützen, was Sie sehen.

Die Illumio ASP-Architektur ermöglicht Zero Trust ohne eine weitere Schicht neuer, komplizierter und unerprobter Technologien zum Lösen von Cloud-Sicherheitsproblemen. Der Infrastruktur-neutrale Ansatz bietet weitere wichtige Vorteile: Transparenz für alle Umgebungen, zentrale Kontrolle, anpassbare Policy, die dem Workload automatisch folgt, sowie Möglichkeiten zum Messen Ihrer Ergebnisse. Auch die Bereitstellung neuer Anwendungen wird dadurch weniger riskant.

Wie sieht eine erfolgreiche Implementierung aus?

Zero-Trust-Prinzipien sind theoretisch absolut sicher. Sie müssen sich jedoch auch in der Praxis skalieren lassen. Wie kann ein Unternehmen seine Zero-Trust-Lösung zur Mikrosegmentierung implementieren, und ab wann gilt eine Bereitstellung als erfolgreich?

Eine erfolgreiche Bereitstellung zur Mikrosegmentierung erfordert eine Lösung mit den folgenden Elementen:

Vollständige Visibilität
Haben Sie einen Überblick über alle Umgebungen, um beim Ausarbeiten von Richtlinien fundierte Entscheidungen treffen zu können?

Modellierung von Policy
Können Sie Policy in einer Umgebung vor der Implementierung modellieren und testen, ohne Netzwerkkommunikation und Datenflüsse zu unterbrechen oder Anwendungen zu beeinträchtigen?

Granularität
Können Sie Richtlinien aus ganzen Umgebungen durchsetzen, bis hin zu Prozessen, die auf einzelnen Hosts ausgeführt werden?

Dynamische Anpassung
Passen sich die Richtlinien an Änderungen in Ihrer Umgebung an?

Messbare Verringerung des Risikos
Können Sie die Risikoreduzierung vor und nach der Implementierung messen?

Berichterstellung
Können Sie On-Demand-Dokumentation von Richtlinienbereitstellungen generieren?

Das Diagramm unten stellt den typischen Pfad vieler Unternehmen auf dem Weg zu Zero Trust mit Illumio dar.

1	2	3	4	5
Identifizieren und Zuordnen von Datenflüssen zu wichtigen Systemen, Verbindungen und Abhängigkeiten	**Konzipieren und Testen von Policy für Zero Trust**	**Umsetzung von Zero Trust mit Mikro-Segmentierung**	**Mitigieren von Schwachstellen durch Priorisierung von Patches**	**Automation und Koordinierung von IT-Abläufen und Sicherheitsprozessen**
Zeigen und dokumentieren Sie die die Kommunikationsverbindungen und Datenflüsse Ihrer Applikationen, Netzwerke und Workloads in einer Echtzeit-Karte.	Wählen und testen Sie die optimale Mikrosegmentierungsstrategie für Zero Trust-Sicherheit.	Nutzen Sie ein standardmäßiges Zero Trust Allowlist-Modell (Default-Deny), um autorisierte Verbindungen und Datenflüsse zwischen Workloads über verschiedene Computing-Umgebungen hinweg zu definieren.	Legen Sie Vulnerability Scan Ergebnisse von Drittanbietern über die illumio Karte, um die potenziellen Einfallstore der Angreifer zu identifizieren sowie zu visualisieren.	Nutzen Sie REST-APIs zum Koordinieren von IT-Abläufen, zur Reaktion auf Sicherheitsvorfälle sowie für Sicherheitsabläufe.
Entwickeln Sie gemeinsam mit Applikations- und IT-Verantwortlichen eine Vision zum Konzipieren von Zero Trust Mikro-Perimetern.	Nutzen Sie die für jeden Server systemeigene Stateful Firewall zur Durchsetzung von Zero Trust-Richtlinien für heterogene Computing-Umgebungen.	Stellen Sie sicher, dass Sicherheitsrichtlinien stets den Workloads folgen und passen Sie sie an Veränderungen der Umgebung an, beispielsweise automatische Skalierung, Anwendungsmigration oder die Erkennung neuer Schwachstellen.	Quantifizieren Sie die riskantesten Workloads und Anwendungen basierend auf Schwachstellen und Gefährdung für laterale Bewegung.	Profitieren Sie von der Integration mit Orchestrierungstools, die Sicherheitsabläufe fest mit dem Bereitstellungs- und Behebungsprozess verknüpfen.
	Programmieren Sie die optimalen Layer 3/Layer 4-Firewalls für alle Workloads, Zugriffssteuerungslisten (ACLs) für Load-Balancer und Switche sowie Sicherheitsgruppen für Public-Cloud-Instanzen.	Berechnen Sie die geeigneten Firewall-Regeln automatisch neu, wenn sich die kontextbezogene Umgebung eines Workloads ändert.	Blockieren oder unterbrechen Sie Angriffstechniken mit lateraler Bewegung durch entsprechende Priorisierung von Patches.	Identifizieren Sie schnell verwaiste und falsch gekennzeichnete Workloads, um CMDBs (Configuration Management Databases) zu bereinigen.
	Modellieren Sie Policy vor dem Enforcement, um Beeinträchtigungen von Anwendungen zu vermeiden.	Verschlüsseln Sie Data in Motion automatisch, ohne dass dazu Änderungen oder Aktualisierungen an der vorhandenen Netzwerkinfrastruktur erforderlich sind.	Wenn die Installation von Patches keine Option ist, nutzen Sie stattdessen Mikro-Segmentierung und schließen Sie ungenutzte Ports.	Nutzen Sie die Integration mit SIEM-Tools (Security Information and Event Management) zum Koordinieren von Reaktionen auf Sicherheitsvorfälle.

Fazit

Die schnelle Einführung von Cloud Computing und die umfassende Vernetzung der Unternehmens-IT haben die Unzulänglichkeiten vorhandener Netzwerksicherheitslösungen auf schmerzhafte Weise offengelegt. Zero Trust setzt strikte Beschränkungen für den Zugriff innerhalb und außerhalb der Firewall durch und ist daher aus gutem Grund zum vorherrschenden Framework geworden. Zero-Trust-Sicherheit erfordert:

1. Standardmäßige Ablehnung von Zugriffen

2. Absicherung von Daten und Anwendungen durch die Segmentierung mit Mikro-Perimetern

Mit diesen Maßnahmen kann die Ausbreitung von Sicherheitsverletzungen in Rechenzentrum- und Cloud-Umgebungen verhindert werden.

Host-basierte Ansätze bieten vollständige Transparenz sowie einen detaillierten Überblick – und damit die notwendigen Voraussetzungen, um Segmentierung für Ihre Umgebungen einzuführen und Mikro-Perimeter in großem Maßstab überall dort durchzusetzen, wo Workloads ausgeführt werden. Damit werden viele der Grundsätze des Zero-Trust-Frameworks von Forrester umgesetzt. Hinzu kommt, dass sich Host-basierte Mikrosegmentierung schneller und einfacher bereitstellen und betreiben lässt als herkömmliche Infrastruktur oder Hypervisor-gesteuerte Methoden. Auch der Umgang mit Umgebungen außerhalb des Netzwerks lässt sich damit flexibler gestalten.

Mehr erfahren

Lesen Sie das Illumio ASP Datenblatt ›
Besuchen Sie unsere Zero Trust Webseite ›

Oder besuchen Sie www.illumio.com/resources

Illumio, ein führender Anbieter für Mikrosegmentierung, verhindert die Ausbreitung von Sicherheitsverletzungen in Rechenzentrum- und Cloud-Umgebungen. Unternehmen wie Morgan Stanley, BNP Paribas, Salesforce und Oracle NetSuite nutzen Illumio zur Reduzierung des Cyberrisikos sowie zur Einhaltung von Vorschriften-Compliance. Nur die Illumio Adaptive Security Platform® schützt wichtige Informationen durch die Echtzeit-Zuordnung von Anwendungsabhängigkeiten und Schwachstellen in Kombination mit Mikrosegmentierung, die alle Rechenzentren und Public- oder Hybrid-Cloud-Bereitstellungen auf Bare-Metal-Systemen, virtuellen Maschinen und Containern angewendet werden kann. Für weitere Informationen zu Illumio besuchen Sie uns unter www.illumio.com/what-we-do oder folgen Sie @Illumio.

1 https://resources.idg.com/download/executive-summary/cloud-computing-2018

2 https://www.oracle.com/cloud/cloud-threat-report/

3 https://www.darkreading.com/cloud/debunking-5-myths-about-zero-trust-security/a/d-