illumio

WHITE PAPER

Die Absicherung ihrer Wichtigsten Anwendungen

REVISED: FEBRUARY 2021

Overview

Dieser Leitfaden zeigt, warum und wie große Unternehmen ihre wichtigsten Applikationen, ihre Kronjuwelen, schützen. Unabdingbar dafür ist eine Karte ihrer Anwendungsabhängigkeiten und die Security Segmentierung selbiger, um auch in flachen Netzwerken und über RZ-Grenzen hinweg aterale Bewegung zu vermeiden.

This white paper covers:

1. Identifizieren der Kronjuwelen
2. Ermitteln der besten Schutz- oder Kontrollmaßnahmen
3. Identifizieren potenzieller Lösungen
4. Wichtige Überlegungen
5. Der Direktvergleich
6. Einholen von Angeboten
7. Bewerten der Kosten für den Schutz

illumio

21. August 1911:

Der wertvollste Kunstgegenstand der Welt – der größte Schatz unter allen Gemälden – wurde aus dem Louvre in Paris gestohlen. Am Morgen nach dem Diebstahl besuchte ein Künstler das Museum, um die Mona Lisa zu bewundern, und stand zu seinem Erstaunen vor vier Haken in der Wand. In den zwei Jahren, in denen sich das Gemälde nicht im Louvre befand, gab es lange Schlangen vor dem Gebäude – nicht, weil die Besucher das Bild sehen wollten, sondern die Stelle, an der es zuvor gehangen hatte.

Der Diebstahl hatte schmerzhafte Folgen: Wachleute wurden entlassen, der Louvre blieb eine Woche lang geschlossen und selbst der Polizeichef von Paris verlor seinen Job, da der Diebstahl in Frankreich als nationale Katastrophe wahrgenommen wurde und er in seiner Position die Verantwortung dafür übernehmen musste.

Schließlich wurde das Meisterwerk im Hotelzimmer eines ehemaligen Mitarbeiters gefunden, der den Diebstahl mithilfe einer Gruppe von Helfern durchgeführt hatte. Nach dem Diebstahl wurde die Sicherheit rund um die Mona Lisa erheblich verschärft. Statt offen in einem Raum aufgestellt zu sein, ist sie durch Sensoren und Barrieren geschützt, und der Zu- und Ausgang der Besucher in diesem Teil des Museums ist eingeschränkt. Dabei sind dies nur die Maßnahmen, mit denen ein erneuter Diebstahl verhindert werden soll.

Schutz vor versehentlicher sowie vorsätzlicher Beschädigung bietet dreischichtiges kugelsicheres Glas. Doch welcher Zusammenhang besteht zwischen diesem sensationellen Diebstahl und der aktuellen Situation in der Cybersicherheit? Die wertvollsten Anwendungen eines Unternehmens sind genau wie einst die Mona Lisa im Jahre 1911 offen in Rechenzentren und Cloud-Umgebungen zugänglich.

Jedes Unternehmen besitzt wichtige Daten und AppliKationen. Sie werden wahlweise als toxische Assets, wertvolle Assets, kritische Assets oder geschäftskritische Systeme bezeichnet. Beispiele dafür sind:

Jedes Unternehmen besitzt wichtige Daten und AppliKationen. Sie werden wahlweise als toxische Assets, wertvolle Assets, kritische Assets oder geschäftskritische Systeme bezeichnet.

Beispiele dafür sind:

- Kontoinformationen von Kunden
- Mitarbeiterinformationen
- Active Directory-Daten
- Kundendaten
- Document Management System (DMS)
- Personenbezogene Informationen
- Patientenakten
- Zahlungssysteme
- Vertrauliche Designs oder geistiges Eigentum
- Abrechnungsinformationen
- Andere Finanzinformationen

Wenn Sie für die Informationssicherheit verantwortlich sind und sich das Schicksal des damaligen Polizeichefs von Paris ersparen möchten, sollten Sie sich fragen: Mit welchen Schritten kann ich meine Kronjuwelen absichern?

Schritt 1: Identifizieren der Kronjuwelen

Zwar scheint dieser Punkt offensichtlich, doch die Klassifizierung Ihrer wertvollsten Assets kann von den jeweiligen Verantwortlichen in Ihrem Unternehmen abhängen. Wenn dieser Schritt noch nicht erfolgt ist, müssen zuerst die wichtigsten Verantwortlichen an einen Tisch gebracht werden. Das sind:

- CISO
- Verantwortliche für Risiko und Governance
- Wichtige geschäftliche Verantwortliche
- Rechtsabteilung
- Finanzabteilung

Die Aufgabe dieses Teams besteht darin, die Risiken der Assets und Anwendungen innerhalb der Unternehmensinfrastruktur zu ermitteln. Das NIST Cybersecurity Framework (CSF) bietet wichtige Anhaltspunktedafür, wie eine Risikoanalyse durchgeführt wird. So beschreibt das NIST den Ablauf:

Risikobewertung (ID.RA):

Risikobewertung (ID.RA): Das Unternehmen kennt die Cybersicherheitsrisiken für die geschäftlichen Abläufe (einschließlich Aufgabe, Funktionen, Image oder Reputation), Unternehmensressourcenund Mitarbeiter

ID.RA-4:

Potenzielle geschäftliche Auswirkungen und Gefährdungswahrscheinlichkeiten sind identifiziert.

In Unternehmen werden Metriken häufig in Geldbeträgen angegeben (entgangene Umsätze oder Kosten durch Problembehebung und Wiederherstellung nach einer Sicherheitsverletzung). Die meisten Unternehmen müssen auch Auswirkungen auf die Reputation berücksichtigen. Wenn beispielsweise eine besonders wertvolle Anwendung alle Kundendaten eines Unternehmens enthält, können die geschäftlichen Auswirkungen durch den Verlust dieses Wertes in dieser Formel ausgedrückt werden:

Wert des einzelnen Kunden (bezogen auf den Kundenakquise-Aufwand) + Kosten der Schadensbehebung laut Kundenverträgen + Kosten für Kommunikation mit Kunden über Sicherheitsverletzung × Anzahl der Kunden

In einem B2B-Szenario könnten die Kosten für die Kundenakquise bei 15.000 € liegen. Für die Behebung der Sicherheitsverletzung fallen 50.000 € an, der Aufwand für die Kundenkommunikation liegt bei 15.000 € und das Unternehmen hat 4.000 Kunden. In diesem Fall wird der Wert der Kronjuwelen wie folgt berechnet:

15.000 €	+	50.000 €	+	15.000 €	×	4.000
Kundenwert		Behebung		Kommunikation		Anzahl der Kunden

= 320.000.000 €

Diese vereinfachte Formel berücksichtigt weder entgangene Umsätze noch Kundenabwanderung infolge der Sicherheitsverletzung. Ebenfalls nicht enthalten sind die Geldbußen, die wegen des Verstoßes gegen Datenschutzrichtlinien wie die DSGVO verhängt werden können.

Schritt 2: Ermitteln der besten Schutz - oder Kontrollmaßnahmen

Wertvolle Anwendungen können auf zahlreichen Ebenen geschützt werden. Dazu gehören Identitäts- und Zugriffsverwaltung (IAM), Schwachstellenverwaltung sowie Segmentierung. Für den Anfang sollten Sie gewährleisten, dass Ihr Unternehmen ein zuverlässiges Programm für die Identitäts- und Zugriffsverwaltung mit Zwei-Faktor-Authentifizierung nutzt. Ein weiterer wichtiger Aspekt ist die priorisierte Behebung von Schwachstellen, die Unternehmensapplikationen gefährden. Das Patchen von Schwachstellen kann sich jedoch als schwierig erweisen, wenn die Systeme aus irgendeinem Grund nicht gepatcht werden können, z.B weil dies einen Produktionsstillstand verursachen würde, weil keine Patches verfügbar sind oder weil der Patch möglicherweise Anwendungen beschädigen würde. Viele Unternehmen setzen auf eine weitere Kontrollmöglichkeit – die Segmentierung. Diese wird im NIST-CSF wie folgt berücksichtigt:

Zugriffskontrolle (PR.AC):

Der Zugriff auf Assets und zugehörige Einrichtungen wird auf autorisierte Benutzer, Prozesse oder Geräte sowie auf autorisierte Aktivitäten und Transaktionen beschränkt.

Gründe für die segmentierung der Wichtigsten anwendungen

Segmentierung gewährleistet, dass die Kronjuwelen des Unternehmens nur für autorisierte Geräte zugänglich sind und diese Geräte nur auf bestimmte Geschäftsprozesse der wichtigen Anwendungen Zugriff haben. Die folgenden Abschnitte dieses Leitfadens konzentrieren sich auf Segmentierung und Mikrosegmentierung. Diese manchmal auch als „Ring-Fencing“ (engl. für Eingrenzung) bezeichnete Maßnahme erzielt beim Schutz der kritischen Applikationen hervorragende Ergebnisse.

Viele Unternehmen sichern ihre wertvollsten Anwendungen und Assets mit diesem Ansatz ab. Dafür gibt es gute Gründe. Während herkömmliche Firewall-Lösungen die Netzwerkperipherie schützen, sind die wertvollen Anwendungen, Datenbanken und Kommunikationswege zwischen den Geräten im Netzwerk völlig ungeschützt. Wir wissen, dass Perimeter-Firewalls häufig unterlaufen werden, sodass sich Angreifer relativ frei im Netzwerk bewegen und das netzwerk ausspahen können.

Segmentierung bietet beim Schutz der Kronjuwelen den Vorteil, dass Unternehmen die Geräte kontrollieren können, mit denen auf die wertvollen Anwendungen zugegriffen wird. Kriminelle Akteure kompromittieren Anwendungen häufig, indem sie von geringerwertigen Anwendungen oder Assets zu hochwertigen Assets wechseln.Segmentierung gewährleistet, dass Sie sichere Enklaven schaffen, in denen die wertvollen Anwendungen ausgeführt werden können. Dies reduziert das Risiko erheblich. Wenn die Kronjuwelen eines Unternehmens Compliance-Vorschriften wie SWIFT oder PCI unterliegen, ist Segmentierung zwingend erforderlich.

Auch wenn die Möglichkeit, Einschränkungen für bestimmte Assets in einem sonst offenen Netzwerk festzulegen, offensichtliche Vorteile bietet, ist die Frage nach der konkreten Umsetzung für viele Unternehmen eine echte Hürde. Der übrige Teil dieses Leitfadens stellt Schritte vor, mit denen sich dieser sichere und geschützte Zustand erreichen lässt.

Schritt 3: Identifizieren potenzieller Lösungen

Die Ermittlung eines Lösungsansatzes für das Segmentierungsproblem beginnt mit dem Identifizieren der wichtigsten Verantwortlichen, die in unterschiedlichen Phasen der Implementierung möglicherweise ins Boot geholt werden müssen. Im Folgenden sind einige der Rollen aufgeführt, die wahrscheinlich beteiligt sein werden, sowie die Gründe dafür.

Rolle	Aufgabe bei der Ermittlung der Lösung für Mikrosegmentierung
Security Engineering	Bieten Einblick in die Integration mit der gesamten Sicherheitsumgebung und sind wichtige Verantwortliche beim Aufbau der letztendlichen Lösung.
Network Engineering	Viele der Lösungen im Segmentierungsbereich sind mit dem Netzwerk verknüpft, sodass möglicherweise Netzwerktechniker für die letztendliche Lösung verantwortlich sein werden.
Anwendungsteams	Da diese Teams für die Anwendungen verantwortlich sind und verstehen, wie sie betrieben und ausgeführt werden, müssen sie zu normalem Basislinienverhalten und Regeln konsultiert werden. (Weitere Informationen finden Sie unten.)
Serverplattformteams	Ebenso wie die Netzwerktechniker spielen diese Mitarbeiter abhängig von der letztendlichen Lösung möglicherweise eine Rolle bei der Auswahl der Kandidaten.
Security Operations Center	Die Lösung zum Schutz der Kronjuwelen muss in das übergeordnete Sicherheitskontrollzentrum integriert werden (z. B. Bedrohungsdaten, Schwachstellenverwaltung sowie Überwachung und Untersuchung von Sicherheitsereignissen).

Das Team sollte die auf dem Markt verfügbaren Lösungen gemeinsam untersuchen. Wir empfehlen dringend, dass das Team unterschiedliche Ansätze unterschiedlicher Anbieter vergleicht. Dabei ist zu beachten, dass Segmentierung ein noch recht junger Markt ist. Bislang nutzten Unternehmen lediglich Firewalls, Subnetze und Zonen, um Anwendungen zu schützen. Doch durch die Änderungen der Bedrohungslage und die Weiterentwicklungen der Datenverarbeitung kamen neue Lösungen auf den Markt, die die Segmentierung der Unternehmensanwendungen – eben der Kronjuwelen – in vorhandenen Rechenzentren und Public Clouds umsetzen sollen.

Die unterschiedlichen Ansätze können wie folgt unterteilt werden:

- Netzwerk-basiert: Erfordert herkömmliche Firewalls und kann die Änderung von IP-Adressen, Subnetzen, Zonen und VLANs notwendig machen.
- Hypervisor-basiert: Diese Lösungen verwenden den virtuellen Switch im Hypervisor als Enforcementpoint.
- Host-basiert: Diese Lösungen nutzen die systemeigene stateful Host-Firewall zur Durchsetzung.

Wir empfehlen dringend, Lösungen von mindestens einem Anbieter in jeder Kategorie zu vergleichen.

Zu diesem Zeitpunkt verfügt das Unternehmen bereits über eine Liste der zu schützenden Assets und hat eine Vorstellung über die unterschiedlichen Ansätze.

Schritt 4: Wichtige Überlegungen

Behalten Sie stets im Auge, dass das Ziel des Projekts darin besteht, die Kronjuwelen innerhalb der Rechenzentren bzw. in der Public Cloud zu schützen. Segmentierungstechnologie identifiziert und isoliert zuerst die wertvollsten Anwendungen und ermittelt den normal dort ein - und ausgehenden Datenverkehr. Sobald diese Baseline etabliert ist, stellt die Lösung Funktionen zum Filtern des Datenverkehrs bereit, um die Gefährdung der Systeme durch böswillige Akteure zu verringern.

Entwicklung einer landkarte der Applikationskommunikation

Die Kronjuwelen sind die wichtigsten Anwendungen, die in einem Unternehmen ausgeführt werden. Sie sollten durch die Schutzmaßnahmen nicht in der Funktionsfähigkeit eingeschränkt werden. Mit der Erkennung des normalen Datenverkehrs (d. h. dem Etablieren von Baselines für akzeptablen Datenverkehr) können Sie gewährleisten, dass die Anwendung durch die aktivierte Segmentierung nicht beeinträchtigt wird. Deshalb ist es auch so wichtig, dass die Anwendungsteams den Normalzustand definieren. Im Idealfall besitzt die Lösung Funktionen, mit denen eine Vielzahl von Anwendungsexperten aus dem gesamten Unternehmen ganz einfach normale Datenverkehrmuster beobachten und festlegen können. Als zusätzlichen Bonus sollten Sie feststellen, ob die Zuordnung der Anwendungsabhängigkeiten auch die Integration in die Schwachstellenverwaltung berücksichtigt. Dadurch können Sie die Risiken und Gefahren nicht gepatchter Schwachstellen ermitteln – und auf diese Weise Segmentierung und Schwachstellenverwaltung verbinden.

Integration in workflows

Der Zielzustand beim Schutz der Kronjuwelen besteht darin, dass Richtlinienverstöße an das SIEM-System gesendet und im Sicherheitskontrollzentrum (SOC) verarbeitet werden. SOC-Teams möchten vermeiden, dass sie von einer Flut von unnötigen Warnmeldungen zu Kompromittierungsindikatoren überschüttet werden, die dadurch entstehen, dass zu restriktive Regeln bei normalem Datenverkehr False Positives generieren. Deshalb muss Ihre Lösung den Anwendungsexperten die Möglichkeit geben, gründliche Analysen durchzuführen und Baselines von Datenflüssen zu erstellen. Im Idealfall erlaubt Ihre Lösung im Produktivbetrieb die Nutzung von Regeln zum Einschränken des Datenverkehrs. Diese sollten jedoch zuvor in einem Testmodus überprüft werden, der die Anzahl der Warnungen offenbart und notwendige Anpassungen ermöglicht.

Minimierung von unterbrechungen

Auch wenn alle Lösungen die Möglichkeit bieten, die Kronjuwelen des Unternehmens zu schützen, sollten Sie darauf achten, dass Ihre Lösung Sie nicht dazu zwingt, die zugrunde liegende Infrastruktur zu ändern. Behalten Sie stets im Auge, dass Sie Ihre Systeme schützen und nicht deren Funktionen unterbrechen wollen. Daher muss das Team feststellen, mit welchen Unterbrechungen durch die jeweiligen Sicherheitslösungen zu rechnen ist. Häufig bestehen diese Lösungen darauf, etwas zwingend zu benötigen. Sie sollten solche Lösungen ausschließen. Mit der Landkarte der Applikationskommunikation können Sie die Feinjustierungen so vornehmen, dass Sie Ihre Systeme weiterhin in vollem Umfang nutzen können.

Metadata

Alle modernen Segmentierungslösungen arbeiten mit irgendeiner Form von Metadaten. Sie machen das, weil Policys mit statischen IP Adressen durch Änderungen auch nur einer IP Adresse unwirksam werden. Stabilere Policys erreicht man durch die Nutzung von Tags, Labels oder Metadaten. Die Frage ist, wie geht die Lösung mit diesen Labeln, Tags oder Metadaten um - passen sie zu den Arbeitsabläufen der Organisation? Diese Überlegungen sollten Sie beim Selektieren einer Lösung mit berücksichtigen.

Schritt 5: Der Direktvergleich

Bestimmen Sie die Anforderungen an die Lösung, legen Sie für diese Anforderungen einen Testplan fest und bringen Sie mindestens eine Lösung aus jeder Kategorie in die Testgruppe ein. Warum? Weil es bei jeder Lösung ein Für und Wider gibt. Und nur durch einen umfassenden Vergleich lassen sich die Kosten, Auswirkungen und Möglichkeiten jeder Lösung ermitteln.

Nach dem Direktvergleich sollten Sie die umfassenderen Auswirkungen auf das Unternehmen genauer unter die Lupe nehmen. Wie viele Mitarbeiter sind für die Bereitstellung und den Betrieb notwendig?

Bestehen Sie darauf, sich mit anderen Unternehmen auszutauschen, deren Umgebungen die gleiche Größe und die eine vollständige Implementierung durchgeführt haben. So erfahren Sie beispielsweise, wie lange es dauerte, bis die vollständig implementierte Schutzlösung in Betrieb war. Wenn Sie direkt fragen, erfahren Sie von Ihren Kollegen in anderen Unternehmen meist, auf welche Probleme sie gestoßen sind. Anbieter werden Sie meist an Kunden verweisen, von denen sie sicher sein können, hervorragende Referenzen zu erhalten. Daher sollten Sie nach Möglichkeit mit Branchenanalysten sprechen oder Unternehmen suchen, die diese Lösung implementiert haben, aber nicht vom untersuchten Anbieter vorgeschlagen wurden.

Schritt 6: Einholen von Angeboten

Bestehen Sie darauf, Angebote von jedem finanziell in Frage kommenden Anbieter einzuholen, der das Problem lösen kann. Hier erweisen sich klare und objektive Metriken basierend auf einem Framework wie NIST-CSF als wichtig.

Stellen Sie sicher, dass das Team den Umfang der Bereitstellung kennt und fordern Sie von jedem Anbieter ein Angebot für die vollständige Lösung des Problems an.

Lassen Sie sich von jedem Anbieter eine Schätzung zur Implementierungsdauer geben und stellen Sie sicher, dass sich alle Verantwortlichen zum Zeit- und Kostenaufwand für die Implementierung sowie den anschließenden Betrieb äußern können.

Schritt 7: Bewerten der Kosten für den Schutz

Der Schutz eines wertvollen Assets ist nicht kostenlos. Er erfordert meist eine Investition in Technologie, ist jedoch auch mit Kosten für Mitarbeiter und Prozesse verbunden. Manchmal sind die Gesamtkosten für den Schutz der Kronjuwelen höher als die zu erwartenden Folgen eines erfolgreichen Angriffs.

Zusätzlich zu den Kosten für die eigentliche Technologie sollten Unternehmen auch die Kosten berücksichtigen, die dadurch entstehen, dass Mitarbeiter geschult oder neu eingestellt und Prozesse angepasst werden müssen. Wenn die Gesamtkosten der Implementierung einer Mikrosegmentierungslösung höher liegen als die zu erwartenden Verluste durch einen erfolgreichen Angriff, wird es schwer sein, die Zustimmung der Unternehmensführung zu erhalten. Deshalb sollten Sie sich für eine Lösung entscheiden, die nicht nur effektive Schutzmaßnahmen bietet, sondern zudem durch besondere Anwenderfreundlichkeit die Kosten senkt.

Ein klassisches Beispiel dafür ist der Schutz vor Datenverlusten (Data Loss Prevention, DLP). Bei sehr komplex aufgebauten Unternehmen ist eine vollständige DLP-Implementierung mit großem Aufwand bei Mitarbeitern und Prozessen verbunden. Ein Risikoteam könnte feststellen, dass die Kosten für die DLP-Kontrolle höher liegen als die der Kompromittierung der eigentlichen Daten.

Sobald die Kronjuwelen identifiziert und Größe sowie Umfang ermittelt wurden, sollten Sie die Kosten für die Implementierung einer Segmentierungslösung genauer untersuchen. Eine einfache Herangehensweise bei der Bewertung ist diese Formel, mit der sichergestellt werden kann, dass die Kosten für den Schutz deutlich geringer sind als die potenziellen Geschäftsverluste oder Risiken:

Erwartetes Risiko – **Kosten für Kontrollmaßnahmen** (einschließlich Mitarbeiter, Prozessänderungen und Technologiekosten) > **0**

Überlegungen zu host-basierten lösungen

Klassische Infrastrukturanbieter haben erkannt, dass ihre Kunden sich von der Infrastruktur (d. h. Netzwerk und Hypervisoren) lösen. Durch den Wechsel zu Public und Private Cloud wird dies in Zukunft unvermeidlich sein. Die meisten Unternehmen haben eine Public-Cloud- Initiative – und diese Initiativen zwingen die Unternehmen, sich vom Gedanken an Segmentierung zu verabschieden, die auf Hypervisoren oder Switch-Ports basiert. Wenn sich zum Beispiel die gesamte Segmentierungsstrategie eines Unternehmens auf netzwerkbasierte Durchsetzung konzentriert, muss diese Strategie bei einem zukünftigen Wechsel in die Public Cloud wahrscheinlich überdacht werden.

Deshalb ist es so wichtig, dass jeder Infrastrukturanbieter jetzt eine Host-basierte Lösung für Mikrosegmentierung bereitstellen kann.

Fazit

Der Schutz der wertvollsten Assets oder Kronjuwelen eines Unternehmens ist unverzichtbar, um finanziellen Schaden sowie negative Folgen für die Reputation und den Geschäftsbetrieb zu verhindern. Eine der besten Möglichkeiten für den Schutz dieser Systeme ist die Einhaltung des NIST Cybersecurity Frameworks, das einen klaren, präskriptiven und risikobasierten Ansatz bietet.

Bei der Auswahl potenzieller Lösungen zum Schutz der wertvollsten Assets ist es auch wichtig, einen methodischen, offenen und kooperativen Ansatz zu wählen. Am Anfang der Analyse sollte die Abschätzung der Kosten eines erfolgreichen Angriffs auf Ihr Unternehmen stehen.

Dieser Wert dient als Referenzpunkt, mit dem die Gesamtkosten jeder Mikrosegmentierungslösung verglichen werden müssen. Nur mit einem gut durchdachten und risikobasierten Prozess kann ein Unternehmen erfolgreich sein.

Gründe für Illumio

Illumio hat eine Echtzeit-Lösung zur Erstellung einer Landkarte der Applikationskommunikation und Mikrosegmentierung entwickelt, die die Ausbreitung von Sicherheitsverletzungen in Rechenzentren und der Cloud verhindert.

Vorteile von Illumio

Netzwerktransparenz neu gedacht: Ein echtzeitüberblick über ihre Wertvollsten anwendungen

Viele Anbieter in der Sicherheitsbranche versprechen noch mehr „Transparenz“ Ihres Netzwerks. Nur von Illumio erhalten Sie eine Echtzeit - Lösung zur Erstellung einer Landkarte der Applikationskommunikation und Schwachstellen für all Ihre Rechenzentrum- und Cloud-Umgebungen. Wir legen die Datenflüsse offen und zeigen, welche Anwendungen mit welchen angreifbaren Ports verbunden sind. Diese Echtzeit-Transparenz bildet die Grundlage für die Entwicklung der idealen Mikrosegmentierungsstrategie für Ihr Unternehmen.

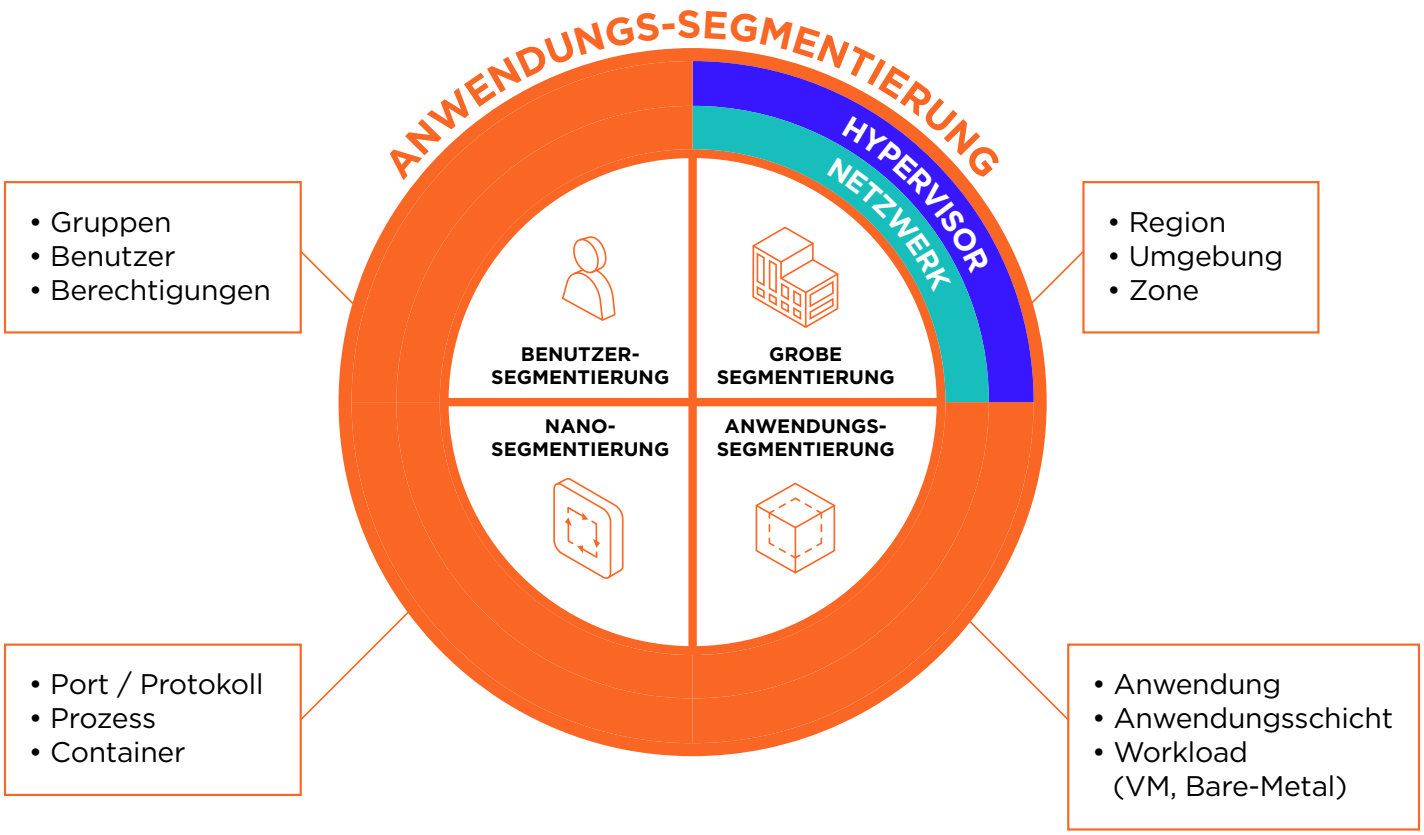
- KEine Echtzeit-Karte zeigt, wie Anwendungen in all Ihren Rechenzentrum- und Cloud-Umgebungen kommunizieren, und stellt die Anwendungen dar, die mit angreifbaren Ports verbunden sind.
- Bei der Berechnung der netzwerkinternen Gefährdung wird berücksichtigt, wie viele Workloads mit Upstream-Verbindungen die Schwachstellen eines bestimmten Workloads ausnutzen können.
- Das Anwendungsverhalten und typische Service-Abhängigkeiten (z. B. Active Directory, Exchange, DNS) werden übersichtlich aufgezeigt.
- Sie können Security Policies erstellen und erhalten visuelle Echtzeit-Rückmeldungen, um die Beeinträchtigung von Anwendungen durch neue Segmentierungsregeln zu verhindern.

Mikrosegmentierung ohne neue Hardware und unabhängig vom netzwerk

Stellen Sie sich vor, dass in Ihrem Rechenzentrum vor jedem Server, jeder virtuellen Maschine, jedem Container oder Netzwerkport bereits eine Firewall implementiert ist und Sie all diese Assets ganz einfach und automatisch in großem Umfang verwalten können. Mit Illumio werden all diese Elemente zu Sensoren (die zeigen, wer kommuniziert) und Enforcementpoints (die kontrollieren, was kommuniziert).

Mit der Mikrosegmentierungstechnologie von Illumio können Sie selbst wählen, welche Segmentierung für Ihre Umgebung notwendig ist, um Ihre wertvollsten Anwendungen zu schützen. Wir bieten die größte Bandbreite an Segmentierungsoptionen auf dem Markt – jedoch ohne den manuellen Aufwand, der mit herkömmlicher Segmentierung verbunden ist.

- Wenn jeder Host zu einem Sensor wird, der nicht autorisierte Datenflüsse erkennt und als Durchsetzungspunkt agiert, der die Ausbreitung von Kompromittierungen verhindert, erhalten Sie die Kontrolle über den netzwerkinternen Datenverkehr zurück.
- Illumio’s Policy Generator ermöglicht die Erstellung optimaler Enforcement Policies, da die Empfehlungen für die Mikrosegmentierungsrichtlinien auf der Kombination aus Schwachstellendaten und Anwendungsdatenverkehr basieren.
- Die einzigartige Policy-basierte IPsec-Verschlüsselung ermöglicht die sichere Verbindung zwischen und innerhalb von Cloud - Umgebungen und privaten Rechenzentren.



Lernen sie illumio kennen

1. Einführung in die Illumio Adaptive Security Platform®
2. Test der Illumio-Plattform mit einer kostenlosen 30-Tage- Testversion
3. Individuelle technische Demonstration durch einen Experten für Mikrosegmentierung

illumio

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.

Gartner peerinsights™

Lesen Sie, was Kunden über illumio zu sagen haben.