Guardicore

Der Leitfaden zur korrekten Wahl eines Mikrosegmentierungslösung

WHITE PAPER

Der Leitfaden zur korrekten Wahl eines Mikrosegmentierungslösung

Da IT-Umgebungen immer komplexer und dynamischer werden, ist die Isolierung von Kommunikationsflüssen durch Mikrosegmentierung unerlässlich. Die Mikrosegmentierung bietet Ihrem Unternehmen eine granulare, auf Workloads basierende Sicherheit und eine beispiellose Transparenz auf Prozessebene über Ihre Abläufe, reduziert das Angriffsrisiko und verbessert die Governance über Ihren gesamten IT-Stapel. Darüber hinaus erzeugt Sie ein umfassendes Verständnis Ihrer Infrastruktur und bringt Sie somit in eine bessere Position, um die Einhaltung von Vorschriften zu erreichen und hat zudem einen immensen strategischen Wert. Dies ermöglicht Ihrem Unternehmen, durch Cloud-Technologien sicher zu innovieren und flexible, aber sichere regelbasierte Richtlinien in jedes Element Ihrer Architektur einzubauen.

Die Mikrosegmentierung bietet Ihrem Unternehmen eine granulare, auf Workloads basierende Sicherheit und eine beispiellose Transparenz auf Prozessebene über Ihre Abläufe

Da die Mikrosegmentierung immer beliebter wird, gibt es eine Reihe von Optionen für Ihre Sicherheitsoperationen, von den Anbietern selbst bis hin zu den Tools und Prozessen, die sie anbieten. Lassen Sie es uns etwas näher betrachten. Was sind die wesentlichen Elemente, die Sie beachten müssen, bevor Sie Ihre Wahl treffen, und was sind die Voraussetzungen für die Mikrosegmentierung, um es einfach zu machen, die Früchte wirklich zu ernten?

In diesem Leitfaden werden wir einen Blick auf Folgendes werfen:

- Transparenz durch Anwendungserkennung und Abhängigkeitsabbildung
- Sicherstellen, dass Ihre Lösung plattformunabhängig ist.
- Einrichten einfacher Richtlinienmanagement/Workflows mit einer logischen und einfachen Benutzeroberfläche.
- Wie Sie eine Untersegmentierung vermeiden können mit Layer 7 insight
- Inklusive Bedrohungserkennung und Response
- Die Wahl des richtigen Anbieters und die Vermeidung der Falle der Mikrosegmentierung “Alles oder Nichts”.

Sichtbarkeit durch Anwendungserkennung und Abhängigkeitsabbildung

Eine starke Mikrosegmentierung kann ohne eine starke Sichtbarkeit nicht existieren. Viele Mikrosegmentlösungen sind der Herausforderung nicht gewachsen, da es an Transparenz auf Prozessebene oder an der Möglichkeit mangelt, Daten kontextuell zu betrachten. Sie können sich auf traditionelle Netzwerktransparenz oder manuelles Mapping verlassen, was nicht ausreicht. Aufgrund der mangelnden Transparenz auf granularer Anwendungsebene ist es unmöglich, Segmentierungen für Anwendungen, Workloads oder Benutzer zu identifizieren und abzubilden, da Sie den Unterschied zwischen sanktioniertem und nicht sanktioniertem Verhalten nicht wirklich visualisieren oder Anwendungsabhängigkeiten bewerten können.

Datenerfassungs- und manuelle Abbildungsprozesse erfordern Zeit und Mühe und werden in den heutigen großen Rechenzentren und hybriden Cloud-Umgebungen immer schwieriger. Bei Zehntausenden von Workloads und Hunderttausenden von Assets wird das manuelle Mapping bald überflüssig sein. Es ist bereits ineffizient und unterliegt menschlichem Versagen, was es für die Unternehmen, die es weiterhin nutzen, untragbar macht. Darüber hinaus müssen Sie ohne Kontext für Ihr Mapping eine ausführliche Analyse durchführen, bevor Sie konkrete Entscheidungen über Anwendungs-Workflows treffen können. Die richtige Lösung macht dies nahtlos, so dass die Mikrosegmentierung schnell umsetzbar und effizient ist.

Darüber hinaus wird selbst die Transparenz auf Prozessebene irrelevant, wenn Sie keinen Zugriff auf eine Echtzeitansicht haben. Ein statischer Schnappschuss Ihrer Anwendung, selbst in detaillierten Details, kann die Dynamik und Schnelllebigkeit der hybriden Umgebungen, in denen wir heute arbeiten, nicht genau wiedergeben. Einfach ausgedrückt, ohne echte Echtzeit-Visualisierung auf Prozessebene sind IT- und Sicherheitsexperten mit blinden Flecken übersät.

Aus diesem Grund sollte Ihre Mikrosegmentierungslösung standardmäßig Anwendungssichtbarkeit und Abhängigkeitszuordnung bieten. Als Live-Map aller Komponenten in Ihrer Anwendung, von Services und Ports über Kommunikation bis hin zu den zugrunde liegenden Prozessen, sehen Sie eine Echtzeitansicht Ihrer Architektur. Dadurch können die relevanten Metadaten importiert werden, um Asset-Labels automatisch zu generieren und maßstabsgetreu über alle Umgebungen und Infrastrukturen hinweg arbeiten zu können. Ihre Lösung sollte dann in der Lage sein, Segmentierungsregeln vorzuschlagen, die auf der Beobachtung des Echtzeitverhaltens basieren und sich bei Bedarf anpassen. Mit dieser granularen Sicht wird Ihnen die ganze harte Arbeit komplett abgenommen.

Sicherstellen, dass die Mikrosegmentierung Ihrer Arbeitslast plattformunabhängig ist

Die Unabhängigkeit Ihrer Sicherheitsverfahren von einer bestimmten Plattform ist unerlässlich, wenn Sie eine Multi-Clash- oder Hybrid-Umgebung betreiben. Die Vorteile der Nutzung einer Kombination aus Public und Private Cloud Optionen, IaaS oder SaaS Lösungen wachsen. Unternehmen verfügen zunehmend über einen Mix aus Servern, virtuellen Maschinen und neuen Cloud-Technologien wie Containern, die die Architektur ihrer IT-Systeme bilden. Angesichts dieser zunehmenden Komplexität der Abläufe kann es schwierig sein, eine angemessene Transparenz zu finden und sogar zu verstehen, wer für die Sicherheitsmaßnahmen verantwortlich ist und wie diese in einer so komplexen IT-Umgebung eingesetzt werden können. Durch den Einsatz einer plattformunabhängigen Lösung für Sicherheit und Mikrosegmentierung, einschließlich Durchsetzung bis Layer 7, muss die Komplexität Ihrer Sicherheit nicht überwältigend werden, und Sie können neue und spannende plattformübergreifende Möglichkeiten nutzen.

Wenn es um den Public Cloud-Betrieb geht, kann jeder Anbieter seine eigenen Punktlösungen anbieten, die ausschließlich auf seine Architektur zugeschnitten sind. Dies ist nicht nur zeitaufwendig zu verwalten, sondern bietet auch einen schlechteren Standard an Support, als Sie vielleicht denken. Trotz der Tatsache, dass die Auslagerung von Sicherheit einer der Gründe ist, warum viele Unternehmen den Wechsel in die Cloud wagen, ist das angebotene Standardsicherheitsniveau in der Regel, gelinde gesagt, unzureichend. Während die Vorteile der Möglichkeit der automatischen Skalierung und des Hinzufügens von Mobilität und Flexibilität leistungsstark sind, können native Cloud-Sicherheitskontrollen auf bestimmte Bereiche beschränkt werden. Die Sicherheitskontrollen können auch mit dynamischen Richtlinieneinstellungen zu kämpfen haben, selbst wenn Sie nur eine Cloud-Plattform verwenden. Da sich die Arbeitsbelastung erhöht oder verringert, können Sicherheitskontrollen möglicherweise nicht ausreichend aktualisiert oder geändert werden. Es kann schwierig sein zu verstehen, wer die Verantwortung für wichtige Sicherheitsentscheidungen trägt oder wer über Updates oder Patches informiert bleiben sollte. Ohne die Sichtbarkeit auf der Anwendungsebene und mit einem Modell der gemeinsamen Sicherheit sind blinde Flecken unvermeidlich. Ihr Unternehmen steht im Dunkeln und kämpft darum, seine eigenen Vermögenswerte erfolgreich zu identifizieren und zu sichern.

Die Sicherstellung der Plattformunabhängigkeit Ihrer Lösung und die Bereitstellung der Mikrosegmentierung nach Workloads bedeutet, dass Sicherheitsprotokolle, wenn sich Workloads in unterschiedlichen und dynamischen Umgebungen bewegen, ausgerichtet und persistent bleiben

Die Möglichkeit, eine Lösung bereitzustellen, die über den gesamten IT-Stapel funktioniert, ermöglicht nicht nur eine effektive Implementierung der Mikrosegmentierung. Dieser Ansatz ist auch wesentlich schneller und einfacher zu verfolgen und zu verwalten als mehrere unterschiedliche Sicherheitsprotokolle. Darüber hinaus bietet es einen zielgerichteten Fokus und eine maßgeschneiderte plattformunabhängige Lösung für Ihre spezifischen Geschäftsziele und Sicherheitsanforderungen. Im Gegensatz dazu wird der Cloud-Anbieter vernünftigerweise seine eigenen Anforderungen an vorderster Front und im Zentrum haben, die möglicherweise nicht auf Ihre individuellen Herausforderungen ausgerichtet sind, und mit ziemlicher Sicherheit nicht daran arbeitet, die Bedrohungserkennung für Ihr Unternehmen in erster Linie zu unterstützen.

Die Sicherstellung der Plattformunabhängigkeit Ihrer Lösung und die Bereitstellung der Mikrosegmentierung nach Workloads bedeutet, dass Sicherheitsprotokolle, wenn sich Workloads in unterschiedlichen und dynamischen Umgebungen bewegen, ausgerichtet und persistent bleiben. Dies alles ohne die Verantwortung Ihres IT-Sicherheitsteams für die Verwaltung mehrerer Richtlinien oder SLAs.

Einrichten einer einfachen Richtlinienverwaltung von Workflows

Für viele Unternehmen wird Ihre Richtlinien-Engine der Schlüssel zum Erfolg Ihrer Mikrosegmentierungslösung sein. Es ist wichtig, dass Ihr Anbieter es so einfach hält, dass jeder in Ihrem Unternehmen Ihre Richtlinienerstellung verstehen und verwalten kann. Eine einfache und unkomplizierte Benutzeroberfläche sollte von der ersten Phase des Prozesses bis zur Ausführung Ihres vollständigen Segmentierungsplans logisch sein. Es sollte in der Lage sein, Ihnen im Detail die Auswirkungen Ihrer Regeln und Richtlinien zu zeigen, bevor sie auf den Verkehr angewendet werden. Ihr Unternehmen benötigt Transparenz über den gesamten Prozess, um Einblicke in den Weg von einer leeren Seite über die Abbildung und Anwendungsabhängigkeiten bis hin zur Festlegung der Regeln selbst und der Vorteile in Aktion zu erhalten. Diese Benutzeroberfläche sollte integrierte automatisierte Richtlinienvorschläge enthalten, die das Produkt-Know-how zeigen und dazu beitragen, den Prozess von Anfang bis Ende reibungslos zu gestalten.

Eine gut durchdachte Richtlinienerstellung lässt Sie nicht auf Flexibilität verzichten, um Sicherheit zu gewährleisten. Viele Punktlösungen beinhalten “nur zulässige” Regelsätze, die auf das Geringste beschränkt sind. Um einen effektiven Sicherheitsaufbau für Ihre Umgebung einzurichten, müssen Sie in der Lage sein, globale Ablehnungsregeln durchzusetzen, die Vorrang vor allen anderen Regelsätzen haben. Auf diese Weise können Sie unbefugte Aktionen erstellen, z.B. um einen Workload mit einem bestimmten Label überhaupt vom Zugriff auf das Internet abzuhalten. Für Bereiche wie Compliance und behördliche Beurteilungen z.B. für PCI oder HIPAA - das erleichtert die Arbeitsbelastung Ihres Sicherheitsexperten erheblich. Gleichzeitig mit der Festlegung dieser Art von “Makro-Segmentierungsregeln” sollten Sie in der Lage sein, eine explizite granulare Richtlinie durch Mikro-Segmentierung für die gleichen Anwendungssegmente zu erstellen.

Bevor Sie Ihre Lösung festlegen, nehmen Sie sich etwas Zeit, um sicherzustellen, dass Ihre Wahl flexibel genug ist. Sie möchten Ihre Umgebung genau so anzeigen und steuern können, wie Sie es wünschen. Beispiele für die Mikrosegmentierung sind nach Art der Umgebung (z.B. Entwicklung oder Produktion), regulatorische Sensitivität (PCI, HIPAA usw.), Anwendung (HR, CRM, Domain Controller, Billing) Tier oder Rolle (z.B. Datenbank, Anwendungsserver, Webserver usw.) und Prozess (Hosts, Ports).

Sobald dies festgelegt ist, muss Ihre Richtlinien-Engine eine dynamische Bereitstellung und Anpassungsfähigkeit bei Änderungen ermöglichen. Von Workflows, die sich automatisch skalieren lassen, bis hin zu Services, die sich erweitern oder zusammenziehen - IT-Umgebungen sind nie statisch und zunehmend dynamisch. Wenn sich Ihre Policy-Engine nicht anpasst, kann es nicht zu einer Mikrosegmentierung kommen.

Einige Funktionen, um die es die Lösung Ihres Anbieters zu überprüfen gilt, sind:

- Die Flexibilität, kundenspezifische, hochspezifische, compliance-basierte Regeln festzulegen.
- Dynamische Beschriftung als Skalierung von Workflows nach oben oder unten
- Mehrere Workloads können Labels und damit Richtlinien gemeinsam nutzen.
- Segmentierungsrichtlinien, die mit Leichtigkeit angepasst und in Blockierungsrichtlinien umgewandelt werden können.
- Blockieren von Richtlinien, die den legitimen Datenverkehr nicht beeinflussen oder beeinträchtigen, um sicherzustellen, dass der geschäftskritische Prozess nicht gestört wird.
- Eine Richtlinienengine, die im Falle einer Verletzung proaktiv die lateralen Bewegungen begrenzen kann.

Wie man mit Layer 7 Insight eine Untersegmentierung vermeidet

Traditionelle Netzwerksegmentierung reicht nicht aus, wenn man das vielfältige Ökosystem betrachtet, in dem die meisten Unternehmen heute ihre IT-Infrastruktur aufbauen. Während sich die Netzwerksegmentierung auf die Verwaltung einer komplexen Umgebung konzentriert, untersucht die Mikrosegmentierung die optimale Sicherheit. Anstatt zu versuchen, die dynamischen Workloads zu begrenzen, kann die richtige Lösung sie von Anfang an einfach sicherer machen. Altmodische Sicherheitsverfahren können es erfordern, dass Sie Ihre IT-Umgebung so einfach wie möglich halten und Sie ermutigen, sich vor neuen Möglichkeiten zu scheuen - da diese mit unbekannten Risiken verbunden sind. Mit Mikrosegmentierung, Transparenz und enger workloadbasierter Segmentierung ist das Risiko immer unter Kontrolle, so dass Sie Agilität und Innovation ohne Beeinträchtigung der Sicherheit nutzen können.

Damit dies funktioniert, muss Ihr Unternehmen sicherstellen, dass es nicht untersegmentiert ist und dass es die Kommunikationsflüsse bis hin zu Layer 7 verwaltet. Port-Hijacking ist zu einer häufigen Bedrohung geworden, wobei bekannt ist, dass Verstöße einen zulässigen Port für den Datenabfluss zu übernehmen. Ein reiner Layer 4 Ansatz, der sich nur auf die Transportschicht konzentriert wäre vergleichbar mit einer Bank, die keine Wachen beschäftigt, sobald man an der Haustür vorbeikommt. Obwohl dies in der Vergangenheit vielleicht ausreichend gewesen wäre, verfügen Angreifer über mehr Werkzeuge als je zuvor. Es wird für Angreifer immer einfacher, sich Zugang durch Ihren Perimeter zu verschaffen. Wenn sie diese erste Hürde durch den Perimeter überwunden haben sind sie meist unbeaufsichtigt und zudem recht frei in Ihren weiteren Bewegungen. Wenn Ihre Lösung nur auf Layer 4 Tiefe segmentiert oder schützt, begrenzen Sie die Angriffsfläche nicht und hinterlassen sie gefährlich groß. Je mehr wir uns auf eine dynamische Infrastruktur stützen und je mehr Workloads zwischen den verschiedenen Segmenten interagieren und kommunizieren, desto gefährlicher wird diese Sicherheitsschwäche sein.

Obwohl die Vorteile der Möglichkeit der automatischen Skalierung und des Hinzufügens von Mobilität und Flexibilität leistungsstark sind, können native Cloud-Sicherheitskontrollen auf bestimmte Bereiche begrenzt werden.

Ein leistungsstarker Mikrosegmentierungsansatz wird für Ihr Rechenzentrum dasselbe tun, was Sie von Ihrer Perimeter-Sicherheit erwarten würden, die Sie nie mit weniger als einer Layer 7-Firewall schützen würden. Die Segmentierung und Durchsetzung bis hin zur Anwendungsschicht für Ihr Rechenzentrum bedeutet, dass Sie eine hohe Sicherheit gegen laterale Bewegungen durch offene Ports und Protokolle bieten, Angriffe stoppen, bevor sie außer Kontrolle geraten oder mehr Schaden anrichten, als sie bereits getan haben. Sie blockieren oder erlauben auch den Datenverkehr sowohl durch Quell- als auch durch Zielprozesse auf Ihrem gesamten Betriebssystem, und nicht nur durch Server und Ports allein.

Bedrohungserkennung und Incident Response zur Stärkung des Sicherheitsstatus

Durch die Isolierung von Anwendungskomponenten hat die Mikrosegmentierung den automatischen Vorteil, dass sie Verletzungen Ihrer Umgebung isoliert und Angreifer stoppt, bevor sie die Bedrohung erhöhen oder laterale Bewegungen ausführen können. Eine leistungsstarke Mikrosegmentierungslösung sollte in der Lage sein, mehr zu tun, indem sie sich in Sicherheitstools integriert, die präventive Maßnahmen zur Verhinderung von Angriffen bieten, und durch Reputationsanalysen einen Verstoß sofort erkennt. Die Bedrohungsreaktion kann dann Probleme in Echtzeit isolieren und beheben, ohne den echten Kommunikationsfluss zu beeinträchtigen, selbst innerhalb desselben Segments.

Um starke Sicherheitstools in Ihre Mikrosegmentlösung einzubinden, müssen Sie einen Anbieter auswählen, der auf Daten aus mehreren Angriffsvektoren zugreifen und Richtlinienverletzungen und Anomalien in Echtzeit bewerten kann. Ihre Lösung sollte Sie nicht nur erkennen und auf versuchte oder erfolgreiche Verstöße aufmerksam machen, sondern auch aktiv alle Versuche blockieren, kompromittierte Assets als Ausgangspunkt für Querbewegungen zu nutzen. Unbefugte Kommunikation oder nicht konformer Datenverkehr jeglicher Art muss sofort erkannt und zur Analyse zurückgehalten werden.

Auch diese Analyse wird von Anbieter zu Anbieter variieren. Experten für Cybersicherheit sollten in der Lage sein, mit Hilfe der Tiefenforensik die Benutzerdaten, Angriffsmethoden und Verbreitungsstrategien des Eindringlings aufzudecken und zu sammeln, den Ermittlungsprozess zu beschleunigen und diese Daten zu verwenden, um einen zukünftigen Verstoß zu verhindern.

Die richtige Mikrosegmentierungslösung enthält nicht nur einen Verstoß gegen einen Bereich, sondern versetzt Sie auch in die beste Position, um ihn im Voraus zu stoppen und einen verbesserten Sicherheitsstatus hinter den Kulissen für Ihr gesamtes Unternehmen zu schaffen.

Auswahl des richtigen Anbieters und Vermeidung der Falle der “All or Nothing”-Segmentierung

Während die Vorteile der Mikrosegmentierung einfach und unkompliziert sind, kann es schwierig sein, diesen Prozess zu starten. Deshalb ist Erfahrung wichtig. Wenn Sie dies zum ersten Mal tun, ist es wichtiger denn je, dass Sie die Expertise eines Unternehmens mit einer großen Erfolgsgeschichte, die besten Tools und den besten Service auf dem Markt nutzen, um Ihre Implementierung erfolgreich zu gestalten. Der Weg zur Mikrosegmentierung muss sich nicht wie eine steile Reise anfühlen und muss auch für Ihr Unternehmen nicht störend sein. Tatsächlich funktioniert es am besten, wenn es langsam und schrittweise durchgeführt wird. Suchen Sie einen Anbieter, der Ihnen helfen möchte, dies Schritt für Schritt zu tun.

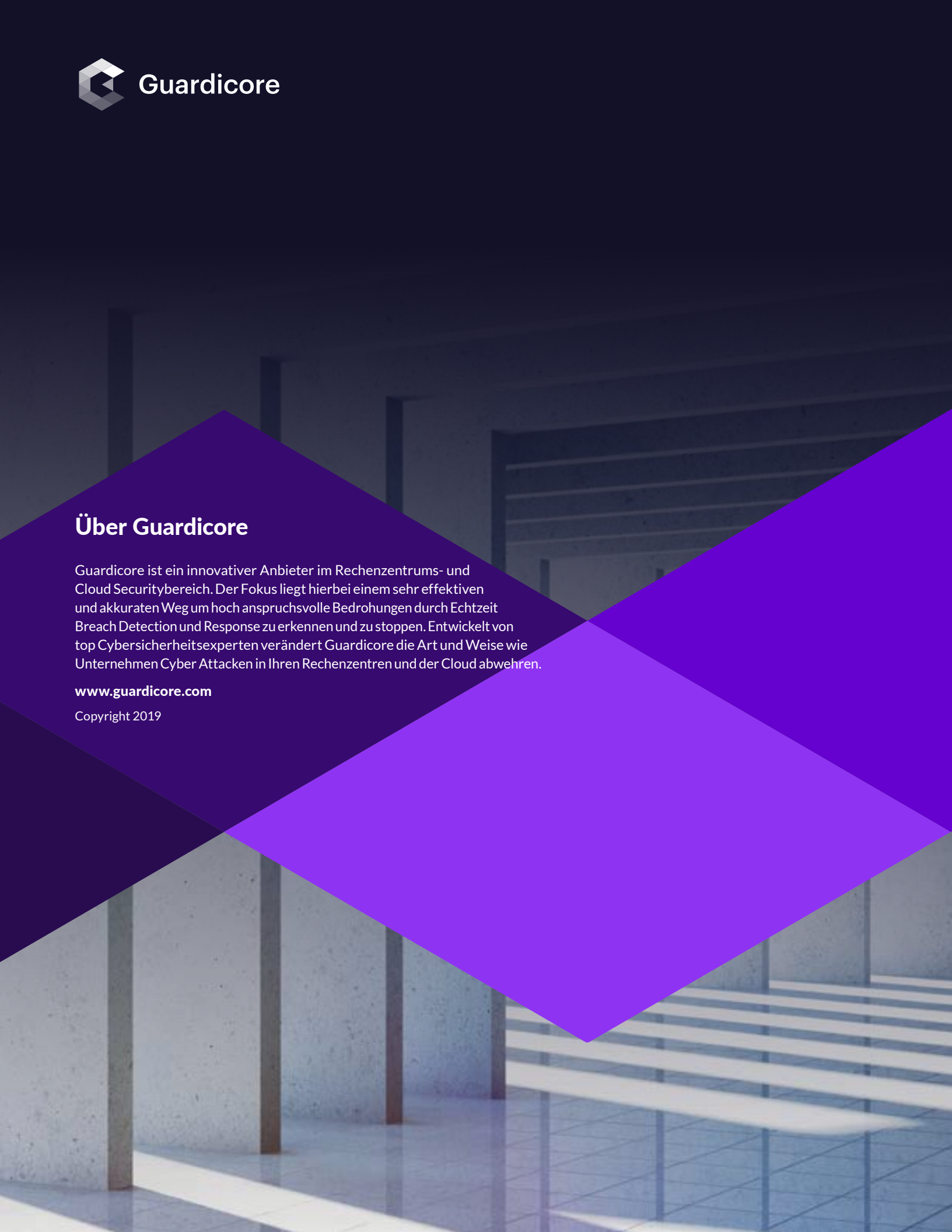
Zuerst sollte das richtige Unternehmen einen Implementierungsplan für Sie erstellen, der mit Transparenz beginnt. Dies ermöglicht es Ihnen, ein klares Verständnis Ihrer Bedürfnisse zu erhalten, bevor Sie überhaupt darüber nachdenken, welche Regeln oder Segmentierungsrichtlinien Sie erstellen möchten. Diese Phase sollte Ihnen ein detailliertes Verständnis Ihrer IT-Architektur vermitteln. Dazu gehören Netzwerkabläufe und Orchestrierungsdetails von allen Ihren Plattformen und Workloads. Es sollte Ihnen eine visuelle Karte der Beziehungen zwischen Ihren Anwendungen liefern.

Jetzt, da Sie ein besseres Verständnis Ihrer gesamten Infrastruktur haben, sind Sie bereit, kritische Vermögenswerte zu identifizieren, die in der Regel risikoreiche oder hochwertige Infrastrukturen sind. Die Mikrosegmentierung dieser einzelnen Anwendungen kann Ihnen den Nutzen dieses Ansatzes aufzeigen, indem sie den Sicherheitsbereich mit nur einer Linie von Richtlinien erheblich verkleinert. Sie können dann schrittweise zur nächsten Stufe übergehen, indem Sie die Bereiche und Anwendungen, die Sie in Mikrosegmenten einteilen, schrittweise vergrößern und die Vorteile in der gesamten Organisation verteilen.

Betrachtung der Mikro-Segmentierung als Ganzes

Die Implementierung der richtigen Mikrosegmentlösung ist ein mehrstufiger Prozess. Erstens sollte Ihr Sicherheitsanbieter Ihnen helfen können, alle Ihre Anwendungsabläufe und Abhängigkeiten genau zu visualisieren und abzubilden, beginnend mit den kritischsten und aufbauendsten. Dies sollte in hybriden Umgebungen reibungslos funktionieren und vollständig plattformunabhängig sein. Auf diese Weise können Sie die inhärente Einfachheit der Erstellung von Workflows nutzen und flexible Richtlinien erstellen, die auf Ihre individuelle Umgebung zugeschnitten sind, einschließlich der Durchsetzung bis zu Layer 7. Um die Sache noch einfacher zu machen, bietet die Erstellung Ihrer Segmentierungsrichtlinie mit Hilfe der zugrunde liegenden Erkennung und Behebung von Verstößen eine ganzheitliche All-in-One-Lösung. Dies bedeutet mehr als nur die Isolierung von Bedrohungen, es findet und löst sie in Echtzeit und stärkt so Ihre Sicherheitslage als Ganzes.

Guardicore



Über Guardicore

Guardicore ist ein innovativer Anbieter im Rechenzentrums- und Cloud Securitybereich. Der Fokus liegt hierbei einem sehr effektiven und akkuraten Weg um hoch anspruchsvolle Bedrohungen durch Echtzeit Breach Detection und Response zu erkennen und zu stoppen. Entwickelt von top Cybersicherheitsexperten verändert Guardicore die Art und Weise wie Unternehmen Cyber Attacken in Ihren Rechenzentren und der Cloud abwehren.

www.guardicore.com