AKAMAI-PRODUKTBESCHREIBUNG

Akamai Guardicore Access

Zero Trust Network Access und Mikrosegmentierung in einer Lösung

Eine einzige Konsole für mehr Transparenz und Kontrolle vereinfacht und beschleunigt Zero Trust

Unternehmen greifen schnell auf Zero-Trust-Sicherheit zurück, um Ransomware zu stoppen, Compliance-Auflagen zu erfüllen und ihre hybride Belegschaft und Cloudinfrastruktur zu schützen. Zero Trust Network Access und Mikrosegmentierung sind die zwei wichtigsten Lösungen für Unternehmen, die auf eine Zero-Trust-Architektur umstellen. Zusammen können sie die Angriffsfläche reduzieren, Sicherheitsverstöße eindämmen und eine erhöhte Zugriffskontrolle mit verbessertem Nutzererlebnis ermöglichen.

Gemeinsam stark

Akamai Guardicore Access kombiniert Segmentierung mit Zero Trust Network Access. Dabei wird beides mit einem einzigen Agent bereitgestellt und über eine einzige Konsole verwaltet. Dieser innovative Ansatz gewährleistet umfassende Transparenz vom Nutzer zum Workload (North-South) und von Endgerät zu Endgerät oder Workload (East-West). Auf diese Weise sind eine identitätsbasierte Anwendungszugriffskontrolle und die Segmentierung von Endgeräten gleichzeitig möglich. Durch die Kombination dieser Technologien profitieren Unternehmen von einem zuverlässigen Sicherheitsframework, das die Netzwerksicherheit stärkt, Risiken minimiert und eine sichere und konforme Umgebung fördert.

Die Akamai Guardicore Platform ist die erste Sicherheitsplattform, die branchenführende Mikrosegmentierung und Zero Trust Network Access kombiniert und Sicherheitsteams dabei unterstützt, die Verbreitung von Ransomware zu verhindern, Compliance-Vorschriften einzuhalten und sowohl die hybride Belegschaft als auch die Cloudinfrastruktur zu schützen.

Zum ersten Mal überhaupt können Unternehmen Segmentierungen implementieren, um ihre Angriffsfläche zu minimieren und gleichzeitig den Zugriff der hybriden Belegschaft von überall aus problemlos verwalten – und zwar mit einem einzigen Agent, der eine einzige Konsole für alle Arten von Assets und Infrastrukturen nutzt.

Wichtige Funktionen

End-to-End-Transparenz
Erlangen Sie vollständiges Verständnis Ihres Netzwerks mit End-to-End-Transparenz, die sich sowohl auf der Karte als auch in Protokollen niederschlägt und Einblicke in die Zugriffsmuster der Endnutzer bietet. Dies ist nur durch die Kombination von Segmentierung und Zero Trust Network Access in einem einzigen Produkt möglich. Darüber hinaus werden Verbindungspfade angezeigt – von Endgeräten zu Workloads bis auf die Prozessebene. Die Darstellung von Echtzeit- und Verlaufsdaten erleichtert forensische Analysen und beschleunigt die Abwehr.

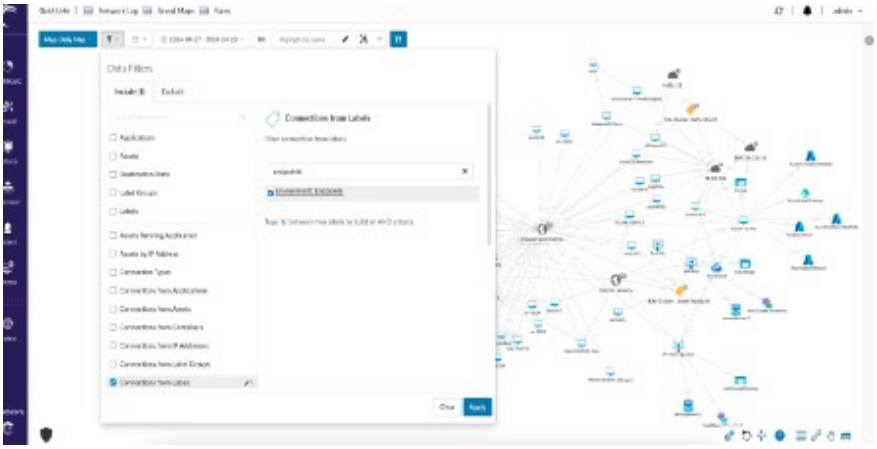
Vorteile für Ihr Unternehmen

Eine einzige Konsole und ein einziger Agent
Implementieren Sie Segmentierung, um die Angriffsfläche zu minimieren und gleichzeitig den Zugriff Ihrer hybriden Belegschaft von überall aus zu verwalten – mit einem einzigen Agent über eine einzige Konsole

Breite Abdeckung
Wenden Sie Zugriffskontrollen überall an und schützen Sie Ihre Belegschaft remote und im Büro

Einheitliche Richtlinie
Setzen Sie Richtlinien für den East-West-Traffic und North-South-Zugriff ohne Änderungen an der Syntax oder den Konsolen durch. So können Sie Zero Trust einfach und effektiv erreichen

Anwendungserkennung
Beschleunigen Sie die Umsetzung von Richtlinien, indem Sie schnell die Anwendungen identifizieren, die Zugriffsberechtigungen benötigen. Ermitteln Sie mühelos Ihre privaten Anwendungen und erhalten Sie wertvolle Einblicke in Nutzungsmuster, einschließlich Nutzerzugriff und Häufigkeit.



Ermitteln Sie ganz einfach die Anwendungen, für die ein Zugriff erforderlich ist

Synchronisierung von Zugriffs- und Segmentierungsrichtlinien
Reduzieren Sie teamübergreifende Abhängigkeiten und beseitigen Sie Spielraum für menschliches Versagen mithilfe einer automatischen Synchronisierung von Zugriffskontrollen und Segmentierungsregeln.

Hauptanwendungsfälle

Umfassender Schutz vor Ransomware: Reduzieren Sie die Wahrscheinlichkeit und die Auswirkungen von Ransomware- und anderen Malware-Angriffen mit identitätsbasierten sowie Machine-to-Machine-Richtlinien. Stellen Sie sicher, dass Endgeräte auf die Ressourcen mit den geringsten Berechtigungen zugreifen, während Sie granulare Zugriffskontrollen durchsetzen.

- Schutz wertvoller Assets: Ermöglichen Sie Nutzern den Zugriff auf kritische Assets basierend auf sicheren Zugriffskontrollen und blockieren Sie direkten VPN-Traffic
- Einschränkung berechtigter Nutzer: Blockieren Sie VPN-Traffic zu ausnutzbaren Admin-Ports, um Administratoren sicheren Zugriff zu ermöglichen

Verteilte Belegschaft: Unterstützen Sie flexibles Arbeiten von jedem Standort aus, indem Sie strenge Zugriffskontrollen durchsetzen und sicherstellen, dass jedes Gerät nur mit den benötigten Ressourcen verbunden ist. Dadurch wird die Angriffsfläche minimiert und die laterale Bewegung innerhalb des Netzwerks verringert.

Compliance: Implementieren Sie Segmentierungsrichtlinien für Endgeräte, um sicherzustellen, dass die Unternehmensendgeräte den relevanten Branchenstandards und Vorschriften entsprechen. Dadurch wird das Risiko von Sanktionen aufgrund von Verstößen verringert und die Sicherheit insgesamt erhöht.

Drittanbieterzugriff: Sorgen Sie dafür, dass Auftragnehmer und Partner eine Verbindung zu bestimmten Anwendungen herstellen können, ohne einen Agent zu installieren. Der Zugriff wird dabei über ein dediziertes Akamai-Portal geleitet und authentifiziert.

Weitere Informationen finden Sie unter Zero-Trust-Sicherheit von Akamai.