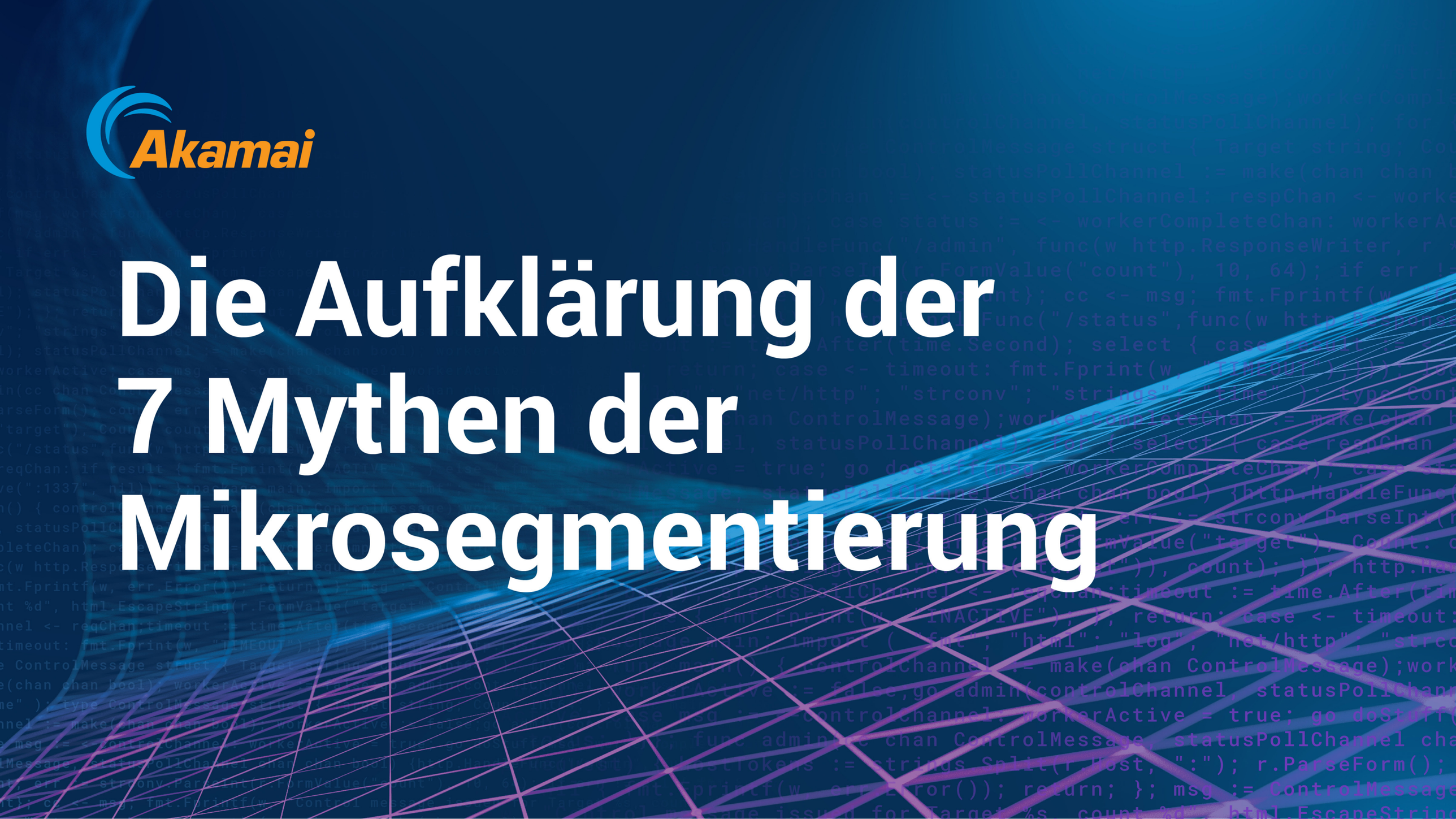
Akamai
Die Aufklärung der
7 Mythen der
Mikrosegmentierung

Es mag kontraintuitiv erscheinen, bei umfassender Skalierung klein zu denken, doch es gibt viele falsche Annahmen hinsichtlich moderner Mikrosegmentierungslösungen.

Glauben Sie, dass die Segmentierung zu Netzwerkausfällen führen könnte oder dass Ihnen die Operationalisierung einer softwaredefinierten Implementierung Schwierigkeiten bereiten könnte? Da liegen Sie möglicherweise falsch. Im Folgenden erfahren Sie, was fein abgestufte Segmentierung wirklich bedeutet.

Mythos 1

Meine EDR-Lösung reicht aus, um Ransomware-Angriffe abzuwehren

Endpoint Detection and Response (EDR) und Segmentierung richten sich beide gegen Ransomware-Angriffe, jedoch in unterschiedlichen Phasen der Kill Chain – und auf unterschiedliche Weise. EDR-Lösungen zielen darauf ab, Ransomware zu erkennen, die auf überwachten Geräten oder Endpoints ausgeführt wird. Wenn die EDR Ransomware erkennt, kann sie den Prozess beenden, das Gerät in Quarantäne verschieben und manchmal eine Verschlüsselung rückgängig machen. EDR und Segmentierung ergänzen sich: Sollte EDR Ransomware nicht erkennen, unterteilen Segmentierungslösungen das Netzwerk in isolierte Buckets, um die laterale Bewegung (Ost-West) eines Angriffs zu begrenzen. Bei Ransomware müssen laterale Bewegungen stattfinden, damit Angreifer erfolgreich sind. Durch die Segmentierung wird sichergestellt, dass Angriffe, die sich über den Endpoint hinaus ausbreiten konnten, letztendlich auf eine Blockade treffen, und so der Auswirkungsradius einer Erstinfektion begrenzt. Erfahren Sie mehr über die Unterschiede zwischen EDR und Segmentierung.

1 Std. 42 Min.

ist die mittlere Zeit, die ein Bedrohungsakteur benötigt, um sich lateral im Netzwerk zu bewegen, nachdem er einmal Fuß gefasst hat

(Microsoft Digital Defense Report 2022)

Mythos 2

Wir nutzen bereits Segmentierung

Die Segmentierung ist kein neues Konzept, sie wurde einfach nur weiterentwickelt. Seit Jahrzehnten verwenden Unternehmen einen Flickenteppich aus VLANs, internen Firewalls, ACLs und Sicherheitsgruppen, um ihre Umgebungen zu segmentieren. Diese alten Methoden haben sich jedoch nicht weiterentwickelt, um den komplexen Anforderungen moderner Hybrid- und Multi-Cloud-Infrastrukturen gerecht zu werden. Und diese unzureichende Segmentierung sorgt für Verteidigungslücken und Schwachstellen.

Beispiel: Ältere Firewalls zeichnen keine Abhängigkeiten zwischen Workflows auf und bewerten diese nicht, was die Identifizierung von Segmentierungen für Anwendungen, Workloads oder Nutzer erschwert. Daher sind Unternehmen gezwungen, umfassende Segmentierungsrichtlinien zu implementieren, die oftmals zu offen sind, was leicht – *und schnell* – zu gefährlichen Fehlkonfigurationen führen kann, die sich nur schwierig und umständlich beheben lassen.

Mit Mikrosegmentierung können Unternehmen bis hinunter auf Layer 7 segmentieren und Richtlinien durchsetzen – weit über das hinaus, was mit herkömmlichen Segmentierungstools möglich ist.

2 Mio. USD

Kostenvermeidung bei Firewall-Upgrades innerhalb von drei Jahren

(Forrester TEI)

Mythos 3

Mikrosegmentierung lässt sich nur schwer operationalisieren

Moderne Mikrosegmentierung bietet Unternehmen viele Vorteile – heute mehr denn je.

Mit Akamai Guardicore Segmentation erreichen Sie maximale betriebliche Effizienz durch den Einsatz einer einzigen softwarebasierten Lösung für Segmentierung, Transparenz, Richtlinienerstellung und Durchsetzung in allen Umgebungen: vom Rechenzentrum über die Cloud bis hin zu containerbasierten Assets. Bei der Bereitstellung erstellt Akamai Guardicore Segmentation eine dynamische visuelle Karte der gesamten IT-Infrastruktur, mit der Sicherheitsteams Aktivitäten bis hinunter zu einzelnen Prozessen überblicken können – sowohl in Echtzeit als auch auf Verlaufsbasis.

Dann können sie diese detaillierten Einblicke in das Anwendungsverhalten nutzen, um über eine intuitive visuelle Oberfläche blitzschnell fein abgestufte Richtlinien für die Mikrosegmentierung zu erstellen. Globale Deny-Regeln, Ringfencing kritischer Anwendungen und die Möglichkeit, große Umgebungen sofort zu segmentieren, sorgen für eine schnelle Amortisierung – und verringern das Risiko.

Bei älteren Segmentierungsmethoden fehlt Ihnen die Transparenz, um überhaupt zu wissen, wo Sie anfangen sollen.

↑95 %

Steigerung der SecOps-Produktivität

(Forrester TEI)

Mythos 4

Mikrosegmentierung bringt Anwendungs- und Netzwerkausfälle mit sich

Bei herkömmlichen Segmentierungsansätzen werden Anwendungen häufig zwischen Subnetzen oder VLANs verschoben, was zu Ausfallzeiten und Unterbrechungen der Geschäftskontinuität führt. Netzwerktechniker und Firewall-Administratoren müssen geplante Ausfallzeiten, Änderungskontrollen oder Wartungsfenster planen, was die Bereitstellung neuer Services oder Anwendungsupdates verlangsamt. Noch schlimmer ist, dass diese Verzögerungen die Anfälligkeit von Assets steigern und so zu einem erhöhten Risiko führen können.

Bei der softwaredefinierten Segmentierung hingegen wird die Sicherheit von der zugrunde liegenden Infrastruktur und den Betriebssystemen abgekoppelt. So kann die Segmentierung unabhängig durchgeführt werden, ohne das Netzwerk oder die Anwendung zu berühren. Im Falle eines Ereignisses wird statt der vollständigen Isolierung der betroffenen Computer nur der Angriffsvektor blockiert, wodurch die negativen Auswirkungen auf das Unternehmen begrenzt werden.

Die Mikrosegmentierung kann auch im Warnmodus bereitgestellt werden, um Richtlinien in Live-Produktionsumgebungen ganz ohne Ausfallrisiko zu testen. Zusammenfassung: Mit modernen Segmentierungslösungen sollten Kunden nicht zwischen gesteigerter Sicherheit und Unternehmensagilität wählen müssen.

Mythos 5

Mikrosegmentierung deckt meine IoT- oder OT-Umgebung nicht ab

Wussten Sie, dass Sie auf IoT- und OT-Geräten, auf denen keine hostbasierte Sicherheitssoftware ausgeführt werden kann, Zero-Trust-Richtlinien ausführen können?

Unsere agentenlosen Segmentierungsfunktionen schließen die Verteidigungslücke auf Geräten, die keine Agents ausführen können, um blinde Flecken zu beseitigen, wie z. B. bei Air-Gap-Endpoints. Diese erweiterte Abdeckung ist besonders wichtig für Umgebungen im Gesundheitswesen, im Einzelhandel und in der Fertigung, wo es viele netzwerkgebundene (und anfällige) IoT-Geräte und ältere OT-Systeme gibt. Die Integration agentenloser Segmentierung in Ihre Netzwerkinfrastruktur ermöglicht die automatische Erkennung neuer Geräte, Fingerprinting und die Durchsetzung von Richtlinien, um Risiken zu minimieren und den unternehmensweiten Weg zu Zero Trust zu beschleunigen.

Mythos 6

Mikrosegmentierungs-Agents erhöhen die Latenz zu stark

Einer der größten Irrtümer bei der Mikrosegmentierung ist die zusätzliche Latenz.

Tatsächlich kommen verteilte, softwarebasierte Segmentierungsrichtlinien zum Einsatz, anstatt den gesamten Traffic durch spezifische Firewallfilter zu leiten. Dadurch werden Engpässe im Netzwerk vermieden. Der Akamai Guardicore Agent ist für Linux, Unix, Windows und MacOS optimiert und verbraucht keine erheblichen Ressourcen.

Und da der Agent nicht inline ist, führt er keine Deep-Packet Inspection durch, die die Latenz erhöhen könnte.

Stattdessen verwendet der Akamai Guardicore Agent nur minimale Informationen aus dem Paketheader, um einen umfassenden Überblick über die Kundenumgebung zu erhalten. Sie wollen Geschwindigkeit *und* Performance? Hiermit erhalten Sie *beides*.

Mythos 7

Für Mikrosegmentierung braucht es neue VZÄs, die schwer zu finden sind

Da CISOs den Druck spüren, „mit weniger mehr zu erreichen“, müssen Sicherheitslösungen Verteidiger entlasten und nicht noch mehr knappe interne Ressourcen verbrauchen.

Herkömmliche Segmentierungsmethoden, wie die Verwaltung von Firewalls und VLANs, führen zu aufwendigen, mehrstufigen Prozessen, an denen viele Teams beteiligt sind – für Switching, Routing, Firewall-Implementierung und die Erstellung von Sicherheitsrichtlinien. Die Implementierung einer älteren Firewall kann im Durchschnitt 14 bis 22 Wochen in Anspruch nehmen. All das verzögert Projekte, wodurch das Unternehmen erheblichen Arbeits- und Betriebskosten ausgesetzt ist.

Im Gegensatz dazu dauert die Bereitstellung der softwaredefinierten Lösung von Akamai im Durchschnitt zwei Wochen – und erfordert nur einen einzigen Vollzeitmitarbeiter. Und durch die Integration von Akamai Hunt, unserem Managed Threat Hunting Service, sparen wir Ihnen Zeit und Ressourcen, indem wir Ihre Umgebung auf neue Attacken, laterale Bewegungen und ungewöhnliches Angriffsverhalten überwachen.

Heutzutage ist es schwierig, Cybertalente einzustellen, und noch schwieriger, sie zu halten. Es ist an der Zeit, dass die Verteidigung für Ihr Unternehmen arbeitet – *und nicht dagegen*.

Wichtige Statistiken

106 %

Nachweislicher ROI von bis zu ~106 % innerhalb von 12 Monaten

(Forrester TEI)

Wie Akamai Sie unterstützen kann

Akamai Guardicore Segmentation ist die softwarebasierte Mikrosegmentierungslösung, welche die einfachste, schnellste und intuitivste Methode zur Durchsetzung von Zero-Trust-Prinzipien bietet. Sie ermöglicht es Ihnen, schädliche laterale Netzwerkbewegungen durch präzise Segmentierungsrichtlinien, visuelle Darstellung der Aktivitäten in Ihrer IT-Umgebung und Netzwerksicherheitswarnungen zu verhindern. Akamai Guardicore Segmentation funktioniert in Ihren Rechenzentren, Multi-Cloud-Umgebungen sowie auf allen Endpoints. Sie lässt sich schneller umsetzen als Ansätze zur Infrastruktursegmentierung. Akamai Guardicore Segmentation bietet Ihnen unvergleichliche Transparenz und Kontrolle über Ihr Netzwerk.

Erfahren Sie, wie Akamai Guardicore Segmentation fein abgestuften Schutz, umfassende Transparenz und die beständige, flächendeckende Durchsetzung von Sicherheitsrichtlinien ermöglicht, um Ihre sensibelsten Daten zu schützen.