4 Gründe, warum Ihr Unternehmen Zero-Trust-Sicherheit implementieren sollte

Inhaltsverzeichnis

Einführung	3–4
01. Die Zunahme von Ransomware-Angriffen	5–7
02. Die hybride Belegschaft	8–10
03. Die Einführung von Cloud-Computing-Ressourcen	11–13
04. Strenge Compliance-Anforderungen	14–16
Globale Bank erreicht SWIFT-Compliance innerhalb von zwei Wochen	17–18

Einführung

Da die Angreifer immer raffinierter werden, Ransomware-Gruppen sich mehr und mehr ausbreiten und der technologische Fortschritt neue Schwachstellen mit sich bringt, wenden sich Unternehmen zunehmend einem Zero-Trust-Sicherheitsmodell zu. Dieser Ansatz beseitigt das implizite Vertrauen in Nutzer, Anwendungen und Geräte, das ein zentraler Grundsatz früherer Sicherheitsansätze war. In der Praxis gibt es vier Schlüsselszenarien, in denen ein Unternehmen von einem Zero-Trust-Sicherheitsmodell profitiert: ein Ransomware-Angriff auf Ihr Unternehmen, ein Wechsel zu Remotearbeit, der Schutz Ihrer Cloudumgebung oder ein bevorstehender Audit.

Diese Szenarien sind das Ergebnis aktueller Trends – die Zunahme von Ransomware-Angriffen, die Entwicklung hin zu einer hybriden Belegschaft, die Migration zu Cloud Computing und die steigenden Anforderungen bei Sicherheitsaudits – die einen neuen Sicherheitsansatz erfordern, der auf der Überprüfung der Identität unabhängig vom Standort basiert und bei Sicherheitsverletzungen proaktive Maßnahmen ergreift. Zero Trust ist der einzige Ansatz, der eine starke Nutzeridentität für den Zugriff auf Daten erfordert und proaktive Abwehr bietet, wenn ein Angriff stattgefunden hat.

Die Implementierung einer Zero-Trust-Strategie mag für bereits überlastete Sicherheitsteams überwältigend erscheinen, dies muss jedoch nicht der Fall sein. Durch einen phasenweisen Ansatz und die Konzentration auf schnelle Erfolge können Sie die Komplexität und das Risiko herkömmlicher Sicherheitslösungen verringern und Ihre Sicherheitslage verbessern.

Sie müssen Ihre vorhandene Technologie nicht auswechseln und ersetzen, um dies umzusetzen. Richten Sie in einem ersten Schritt Ihre Zero-Trust-Investitionen an Ihren dringendsten Geschäftsanforderungen aus. Entscheiden Sie sich für einen vertrauenswürdigen Zero-Trust-Anbieter und nicht für jemanden, der sich über Nacht weiterentwickelt und seine bereits überholte Lösung in Zero Trust umbenannt hat. Ziehen Sie unbedingt einen Anbieter in Betracht, der mehrere Elemente der Zero-Trust-Sicherheit (Zero Trust Network Access, DNS-Firewall, Mikrosegmentierung usw.) auf einer einzigen Plattform kombinieren kann. Was auch immer Ihr Grund für die Einführung ist, Zero Trust sorgt für geschäftliche Agilität und Kostenoptimierungen und ermöglicht die Konsolidierung Ihrer IT-Tools sowie einen reibungsloseren Gesamtbetrieb.

Die 4 wichtigsten Gründe, aus denen Unternehmen auf Zero Trust setzen

Die Zunahme von Ransomware-Angriffen

Die hybride Belegschaft

Die Einführung von Cloud-Computing-Ressourcen

Strenge Compliance-Anforderungen

01

Die Zunahme von Ransomware-Angriffen

Verbessern Sie Ihren Schutz vor Ransomware

In den letzten Jahren haben Ransomware-Angriffe Unternehmen auf der ganzen Welt auf den Kopf gestellt, von Krankenhäusern und Banken bis hin zu Pipelines und anderen wichtigen Infrastrukturen. Tatsächlich prognostiziert **Cybersecurity Ventures**, dass Ransomware seine Opfer bis 2031 jährlich rund 265 Milliarden US-Dollar kosten wird. Ferner sagt die Prognose, dass Ransomware-Täter alle zwei Sekunden einen neuen Angriff (auf Verbraucher oder Unternehmen) starten, während sie ihre Malware-Payloads und die damit verbundenen Erpressungsaktivitäten schrittweise optimieren.

Ohne eine Zero-Trust-Strategie können Ransomware-Gruppen die folgenden Schwächen ausnutzen:

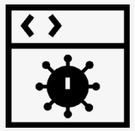
- ☑ implizites Vertrauen in Nutzer, Anwendungen und Netzwerke, wodurch Angreifer, die in das Netzwerk eindringen, sich lateral bewegen und Malware verbreiten können
- ☑ übermäßig großzügige Zugriffsrichtlinien, die ein Eindringen von Ransomware und damit die Infizierung des Systems ermöglichen
- ☑ Systeme, deren Vertrauen sich nur auf ein Passwort stützt, wodurch die Möglichkeit zum Diebstahl von Anmeldedaten besteht

So schützt Zero Trust

Unternehmen, die eine Zero-Trust-Architektur implementieren, über Zugriffskontrollrichtlinien verfügen und Mikrosegmentierung nutzen, minimieren den Schaden, den ein solcher Angriff anrichten kann. Es wird Angreifern nicht nur erschwert, in das System einzudringen, sie sind auch in ihrer Fähigkeit, sich darin auszubreiten, eingeschränkt.

So unterbricht Akamai Ransomware-Kill-Chains

Ein Ransomware-Angriff umfasst in der Regel eine anfängliche Infektion, laterale Netzwerkbewegungen sowie Datenextraktion und -verschlüsselung. Mit Zero Trust können Unternehmen jeden Schritt eines Angriffs abwehren, während er geschieht – oder sogar bevor er geschieht.



Erstinfizierung

Die Akamai Guardicore Platform verhindert, dass sich ein Angriff über den ursprünglichen Eintrittspunkt hinaus ausbreitet, während Akamai MFA Nutzer vor Diebstahl und Missbrauch ihrer Anmeldedaten schützt.

Laterale Netzwerkbewegungen

Die Akamai Guardicore Platform reduziert Ausbreitungsmöglichkeiten und verhindert laterale Netzwerkbewegungen. Akamai Guardicore Access schränkt die Möglichkeiten des Angreifers ein, die Anwendung zu infizieren, aus der er Daten stehlen möchte. Akamai Hunt erkennt selbst gut getarnte Bedrohungen in Ihrem Netzwerk und wehrt diese ab.

Datenextraktion und -verschlüsselung

Die Akamai Guardicore Platform schränkt den Zugriff auf zentrale Anwendungen ein, sodass Angreifer in einem kompromittierten Netzwerk nicht auf vertrauliche Daten zugreifen können. Akamai Secure Internet Access Enterprise blockiert Anfragen an Phishing- und Command-and-Control-Websites. Zu guter Letzt erkennt Akamai Hunt ungewöhnliches Verhalten und hindert Angreifer daran, wertvolle, Ransomware-fähige Daten zu verschlüsseln.

02

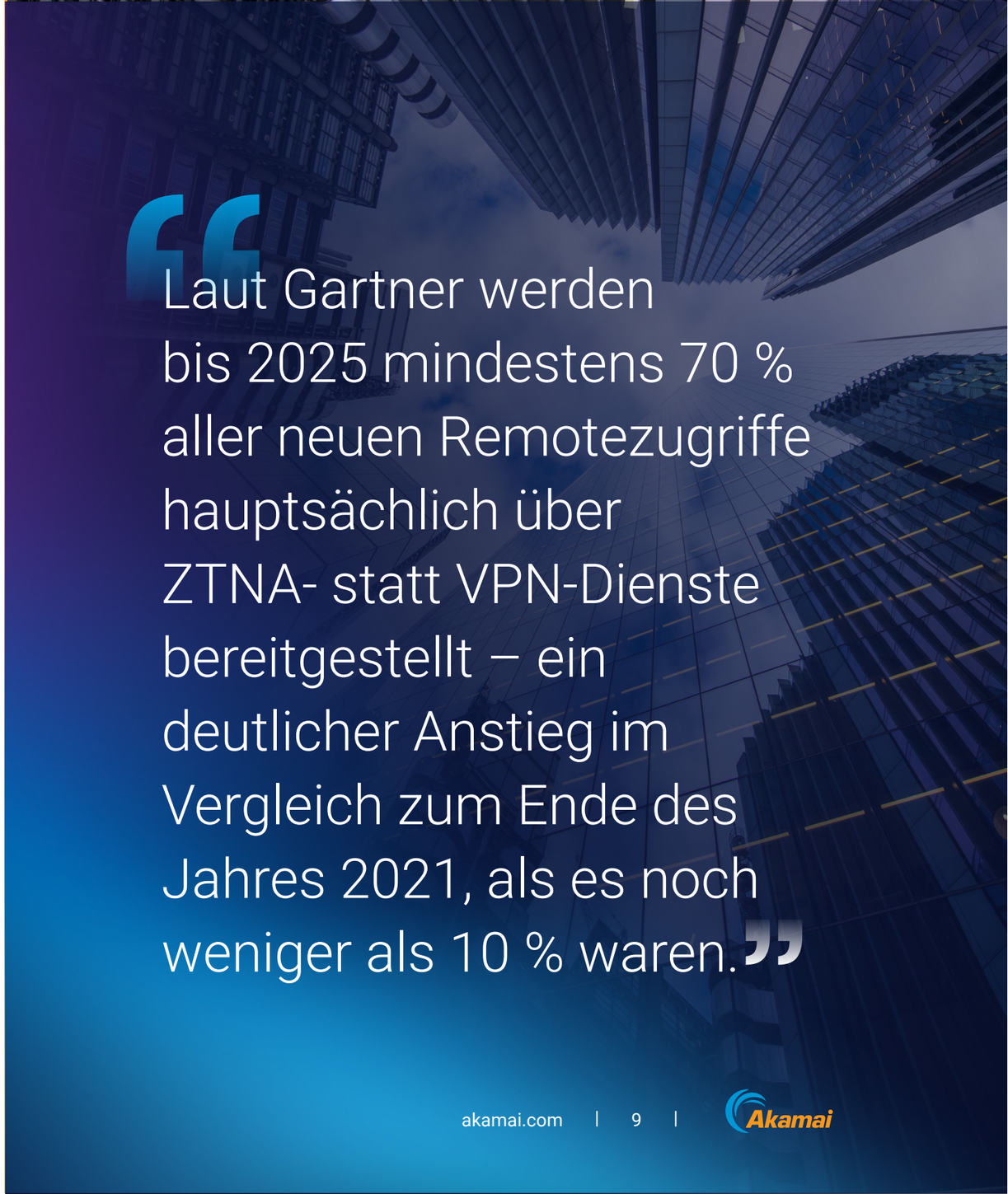
Die hybride Belegschaft

Schützen Sie Ihre neue hybride Belegschaft

Der Schutz einer modernen, hybriden Belegschaft, die aufgrund der COVID-19-Pandemie immer weiter gewachsen ist, gestaltet sich schwieriger, wenn Unternehmen auf veraltete Sicherheitstools wie Firewalls und VPNs angewiesen sind. Als VPNs für den Remotezugriff vor etwa 30 Jahren eingeführt wurden, war alles anders: Das Internet steckte noch in den Kinderschuhen, Anwendungen wurden im Rechenzentrum ausgeführt und es gab viel weniger Nutzer, die sich von anderen Standorten aus anmeldeten. Die kontinuierliche Nutzerauthentifizierung über ein VPN und der Zugriff auf das gesamte Netzwerk erhöhen die Angriffsfläche und öffnen Tür und Tor für viele der Zero-Day-Schwachstellen, die mit älteren VPNs einhergehen. Jeder Nutzer mit den erforderlichen Anmeldedaten kann sich über ein Unternehmens-VPN anmelden und sich dann lateral im Netzwerk bewegen, um auf die Ressourcen zuzugreifen, die das VPN eigentlich schützen sollte.

So schützt Zero Trust

Zero Trust basiert auf dem Prinzip des Zugriffs mit minimalen Rechten und geht davon aus, dass kein Nutzer und keine Anwendung von Natur aus als vertrauenswürdig eingestuft werden sollte. Zero Trust Network Access (ZTNA) verwendet einen völlig anderen Ansatz als VPNs, um den Zugriff für Remotemitarbeiter zu gewährleisten. Anstatt das gesamte Netzwerk zu gefährden, werden Nutzer direkt mit den Anwendungen und Daten verbunden, die sie benötigen. So werden laterale Bewegungen schädlicher Nutzer mit übermäßigem Zugriff auf sensible Daten und Ressourcen verhindert. Im Falle einer Sicherheitsverletzung kann eine effektive Zero-Trust-Mikrosegmentierungslösung das interne Netzwerk unterteilen, sodass sich der Angriff nicht ausbreitet und andere Teile des Netzwerks keinen Schaden nehmen. Laut **Gartner** werden bis 2025 mindestens 70 % aller neuen Remotezugriffe hauptsächlich über ZTNA- statt VPN-Dienste bereitgestellt – ein deutlicher Anstieg im Vergleich zum Ende des Jahres 2021, als es noch weniger als 10 % waren.



Wie Akamai hybride und Remotearbeit ermöglicht

Die umfassend Zero-Trust-Plattform von Akamai erfüllt die Anforderungen Ihrer hybriden Belegschaft. Zu den Vorteilen zählen:

Geringeres Risiko

Akamai verbindet den richtigen Nutzer direkt mit der richtigen Anwendung und reduziert so die Angriffsfläche und die Möglichkeit lateraler Netzwerkbewegungen.

Verbessertes Nutzererlebnis

Remotenutzer können unabhängig von Anwendung, Gerät oder Standort auf Ressourcen zugreifen, sodass keine Verbindung über VPN mehr hergestellt bzw. getrennt werden muss.

Mehr Agilität

Da die Lösung von Akamai als Service genutzt wird, müssen Unternehmen weder Hardware bereitstellen noch sich Gedanken über die Skalierung bei steigenden Anforderungen machen. Dadurch können Kosten und Komplexität reduziert werden.

03

Die Einführung von Cloud-Computing-Ressourcen

Vereinfachte Cloud-Migration

Unternehmen verlagern ihre Anwendungen in die Cloud, um Flexibilität und Agilität zu ermöglichen und ihre Infrastruktur zu modernisieren. Diese Cloudumgebungen erweitern jedoch die Angriffsfläche und stellen neue Sicherheitsanforderungen. Integrationen zwischen verschiedenen Clouds und lokalen Umgebungen können in Anwendungen eindringen und die Sicherheit gefährden. Wenn Unternehmen versuchen, ihre Anwendungen mithilfe herkömmlicher Netzwerkstrukturen – VPNs und Firewalls – in die Cloud zu migrieren, sind sie oft mit einem erhöhten Risiko für laterale Bedrohungen, schlechter Skalierbarkeit und hohen Kosten konfrontiert. Auch nach Abschluss der Migration müssen Assets geschützt werden und Nutzer anhand von Rollenberechtigungen authentifiziert werden. Nutzer von Cloudinfrastrukturen haben in der Regel mehr Zugriff auf Ressourcen, Services und Verwaltungsberechtigungen als in lokalen Umgebungen, was zusätzliche Risiken birgt und für mehr Störanfälligkeit sorgt.

So schützt Zero Trust

Zero-Trust-Strategien erleichtern die Migration in die Cloud. Zero Trust hebt das implizite Vertrauen auf, das vielen cloudbasierten Anwendungen innewohnt, insbesondere Anwendungen von Drittanbietern, die Schwachstellen mit sich bringen können. Zero-Trust-Lösungen stellen sicher, dass Unternehmen ihre cloudbasierten Anwendungen einfacher und geschützter bereitstellen können. Zu den Vorteilen von Zero Trust für die Cloud zählen:

- ☑ bessere Einblicke in Assets und Risiken
- ☑ weniger Angriffsfläche dank Zero-Trust-Segmentierung und Zugriff auf Cloudressourcen mit minimalen Rechten
- ☑ modernisierte Netzwerkinfrastruktur für Geschwindigkeit und Agilität
- ☑ Senkung der Betriebskosten und -komplexität

So verbessert Akamai die Cloud-Migration

Mit den Zero-Trust-Lösungen von Akamai können Sie Ihre Assets und die entsprechenden Richtlinien automatisch migrieren. Es gibt keine Ausfallzeiten und keine Betriebsunterbrechungen. Akamai hat die Lösung:

Mehr Transparenz

Mit einem besseren Verständnis für die Zusammenhänge zwischen Anwendungen können Sie effektive Richtlinien für die Cloudsegmentierung erstellen, um die Angriffsfläche zu reduzieren und Risiken zu minimieren.

Zero Trust Network Access

Die Nutzer können sich auf Basis einer starken Authentifizierung nur mit Anwendungen verbinden, für die sie auch eine Zugriffsberechtigung haben.

Threat Hunting

Die engagierten Threat Hunter von Akamai suchen kontinuierlich in Cloudumgebungen nach ungewöhnlichem Angriffsverhalten und benachrichtigen Kunden über jedes Risiko für ihr Netzwerk.

04

Strenge Compliance-Anforderungen

Einfachere Compliance und geringere Risiken

Sicherheitsexperten wissen zwar, dass Compliance-Anforderungen keinen Rundum-Schutz für Organisationen bedeuten, doch Sicherheitsaudits haben für Führungsteams nach wie vor oberste Priorität. Sie wissen, dass fehlgeschlagene Audits zu größeren Geschäftsunterbrechungen und negativen Auswirkungen auf das Geschäftsergebnis führen können. Eine Compliance-Bewertung ist für Sicherheitsteams eine der zeitaufwändigsten und ressourcenintensivsten Aktivitäten. Zusätzlich haben der Wechsel zu digitalen, perimeterlosen Umgebungen und die Verbreitung der Remotearbeit haben solche Bewertungen noch schwieriger gemacht. Unternehmen müssen in der Regel ihre Umgebungen isolieren und ihre regulierten Assets abgrenzen, um Compliance-Standards wie den Payment Card Industry Data Security Standard (PCI DSS), den Health Insurance Portability and Accountability Act (HIPAA) und die Standards der Society for Worldwide Interbank Financial Telecommunication (SWIFT) zu erfüllen.

Unternehmen müssen auch Remotenutzer, lokale Nutzer, Partner, Lieferanten und vieles mehr unterstützen. Es ist daher nahezu unmöglich, die Grenzen einer Unternehmensumgebung zu definieren. Sicherheitsteams, die sich auf Audits vorbereiten, bei denen die Zugriffskontrolle einen wichtigen Erfolgsfaktor darstellt, müssen die folgenden Fragen beantworten:

- Wie können wir den Zugriff auf vertrauliche Informationen auf autorisierte Nutzer beschränken?
- Wie können wir den Umfang des Auditumfelds bestimmen?
- Wie können wir den Auditprozess einfacher und weniger chaotisch gestalten?

So schützt Zero Trust

Glücklicherweise kann ein Zero-Trust-Ansatz dazu beitragen, all diese Fragen und noch mehr zu beantworten. Die beiden Grundpfeiler von Zero Trust – die Möglichkeit zur expliziten Überprüfung und Unterstützung des Zugriffs mit den minimalen Rechten – vereinfachen den Compliance-Prozess erheblich. Unternehmen können ihre regulierten Assets von anderem Traffic in ihrem Rechenzentrum oder in der Cloud isolieren und Zugriff auf der Grundlage der Identität unabhängig vom Standort gewähren. Verbesserte Transparenz zeigt, was in ihr reguliertes Umfeld eintritt und was aus diesem austritt, und hilft zu bestimmen, was in den Geltungsbereich fällt. Dies verringert die Komplexität und die Kosten des Audits erheblich und erleichtert dem Auditor das Leben.

So erleichtert Akamai die Compliance

Das umfassende Zero-Trust-Portfolio von Akamai trägt dazu bei, dass Sie auf jedes Audit vorbereitet sind – ob PCI DSS, HIPAA, International Standards Organization (ISO), Sarbanes–Oxley (SOX) oder ein anderes Framework. Akamai Enterprise Application Access steuert den Zugriff Dritter auf vertrauliche personenbezogene Daten und erfüllt die Anforderungen der Datenschutzgrundverordnung (DSGVO). Akamai Guardicore Segmentation verbessert das Verständnis regulierter Assets gemäß PCI DSS, isoliert Clearinghouse-Funktionen gemäß HIPAA, schränkt den Internetzugang ein und isoliert zentrale Systeme gemäß SWIFT-Verordnungen. Akamai MFA schützt Patientendaten gemäß HIPAA vor Angreifern, die Passwörter für Gesundheitssysteme erhalten haben. Dies erhöht die SWIFT-Compliance, da Anmeldedaten nicht kompromittiert werden.

Globale Bank erreicht SWIFT-Compliance innerhalb von zwei Wochen

Externe Aufsichtsbehörden verlangten von einem Kunden von Akamai, einer globalen Bank, alle wichtigen Anwendungen zu schützen, um die SWIFT-Anforderungen für einen sicheren Prozess für Geldtransfers zwischen Finanzinstituten zu erfüllen. In der Regel erfordert eine Anwendung wie diese mehr als 100 Server, die an verschiedenen Standorten bereitgestellt werden, einschließlich Bare-Metal- und virtueller Server. Im Durchschnitt könnte dieser Prozess bei einer Bank dieser Größe mit Planung und Ausführung zwischen 8 und 12 Monate dauern, da ein Virtual Local Area Network (VLAN) für das Segment über mehrere Standorte hinweg erstellt werden müsste. Die Ermittlung der Abhängigkeiten der SWIFT-Anwendung und das Sicherstellen, dass der Regelsatz korrekt ist und keine Schädigung entsteht, hätte den Zeitplan nur verlängert. Gleichzeitig hätte das Projekt auch den Kauf neuer Firewall-Anlagen erfordert. Da die SWIFT-Anwendung für das Bankgeschäft von entscheidender Bedeutung ist, konnte die Bank sich keine Ausfallzeiten leisten. Alles in allem war damit zu rechnen, dass das Segmentierungsprojekt einen enormen Aufwand seitens einer Vielzahl von Mitarbeitern erfordern würde. Doch mit Akamai brauchte ein einziger Security Engineer für den gesamten Prozess nur etwa zwei Wochen. Es waren keine Netzwerkänderungen erforderlich und die Bank konnte den Wechsel und Ausfallzeiten von Anwendungen vermeiden.

Vereinfachte, schnellere Compliance

Globale Bank

- SWIFT-Anwendung muss geschützt werden
- Komplexe Umgebung mit Bare-Metal-, VMware- und OpenStack-Servern

Herkömmliche Segmentierung

- Schwer zu definierende Segmente über eine komplexe Infrastruktur hinweg
- Keine Transparenz in Bezug auf Anwendungen und Abhängigkeiten
- Erfordert Ausfallzeiten
  Zeitaufwand: 8 bis 12 Monate
  Personaleinsatz: Mindestens 5

Akamai Guardicore Segmentation

- SWIFT-Anwendungszuordnung in Stunden abgeschlossen
- Segmentierungsrichtlinien werden automatisch vorgeschlagen und optimiert
- Sie müssen keine neue Hardware und keine Firewalls erwerben oder implementieren
- Keine Ausfallzeit
  Zeitaufwand: 2 Wochen
  Personaleinsatz: 1 Architekt

Erfahren Sie mehr darüber, wie Sie Ihre Geschäftsanforderungen mit dem Zero-Trust-Portfolio von Akamai erfüllen können

Weitere Informationen

Akamai schützt die Anwendungen, die Ihr Unternehmen vorantreiben, an jedem Interaktionspunkt – ohne die Performance oder das Kundenerlebnis zu beeinträchtigen. Unsere globale Plattform liefert Skalierbarkeit sowie transparente Einblicke in Bedrohungen. Gemeinsam mit Ihnen können wir auf diese Weise Bedrohungen erkennen und abwehren, damit Sie Markenvertrauen aufbauen und Ihre Vision umsetzen können. Möchten Sie mehr über die Cloud-Computing-, Sicherheits- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter **akamai.com** und **akamai.com/blog** oder folgen Sie Akamai Technologies auf **X** (ehemals Twitter) und **LinkedIn**. Veröffentlicht: September 2024.