WHITEPAPER

Der Weg zu erstklassiger Sicherheit

Erstellen Sie einen individuellen Transformationsplan mit Zero Trust im Kern.

Um sicherzustellen, dass Akamai in der modernen dynamischen Sicherheitsumgebung geschützt bleibt – und um Selbstgefälligkeit zu verhindern –, haben wir kürzlich unsere Sicherheitsperformance mithilfe des Zero Trust Maturity Model (ZTMM, Zero-Trust-Reifegradmodell) visualisiert. Hier erfahren Sie, wie auch Sie mit dieser Vorgehensweise wichtige Verbesserungsbereiche in Ihrem Unternehmen ermitteln und eine klare Roadmap für erstklassige Sicherheit erstellen können.

Einfacher zu Zero-Trust-Sicherheit

Unternehmenszugriff und -sicherheit sind komplizierte Bereiche, die sich stetig weiterentwickeln. Vor diesem Hintergrund wissen Verantwortliche oft nicht, worauf sie sich auf dem Weg zu Zero-Trust-Sicherheit konzentrieren müssen.

Aus diesem Grund empfehlen wir, das ZTMM zu verwenden, um Ihre aktuelle Sicherheitslage zu bewerten und zu visualisieren. Auch wir haben es genutzt, um unsere eigene Sicherheit bei Akamai sowie die Sicherheit mehrerer Kunden zu beurteilen. Am Ende des Prozesses erhalten Sie einen Leitfaden mit praktischen Maßnahmen, um einer Zero-Trust-Architektur zu näherzukommen. (Weitere Informationen zum Zero-Trust-Konzept finden Sie in Anhang A.)

Vorteile des Zero Trust Maturity Model

Auf dem Weg zu stärkerer Sicherheit ist unserer Meinung nach der erste Schritt der wichtigste: der Einstieg. Wenn es jedoch um das komplexe, schnelllebige Thema der Cybersicherheit geht, ist dieser erste Schritt einfacher gesagt als getan. Viele Unternehmen tun sich schwer mit den nötigen Entscheidungen: Was muss getan werden, um Zero Trust zu erreichen? In welchem Umfang? Und in welcher Reihenfolge sollten Änderungen vorgenommen werden?

Genau hier kommt das ZTMM ins Spiel. Es schafft ein Framework für Zero Trust, das ein Gefühl der Linearität vermittelt und die Implementierung erleichtert. Es hilft Unternehmen dabei, einen Änderungsplan zu erstellen und ein Budget für Updates festzulegen. Außerdem erklärt es Zero-Trust-Konzepte für Entscheidungsträger, die keine IT-Spezialisten sind, damit IT-Teams die erforderliche Unterstützung erhalten.

Das ZTMM hat sich bewährt. Es wurde von der US-amerikanischen Cybersecurity and Infrastructure Security Agency (CISA) entwickelt und weitgehend in US-amerikanischen Bundesbehörden übernommen.

Die fünf Säulen und drei Fähigkeiten des ZTMM

Das ZTMM stellt die Implementierung schrittweise in fünf verschiedenen Säulen dar, mit denen im Laufe der Zeit kleinere Fortschritte erzielt werden können. Diese Säulen betreffen Identität, Geräte, Netzwerke, Anwendungen und Workloads sowie Daten (Abbildung 1). Beim ZTMM müssen Sie außerdem über drei Fähigkeiten nachdenken, die alle fünf Säulen durchlaufen:

- Transparenz und Analyse
- Automatisierung und Orchestrierung
- Governance

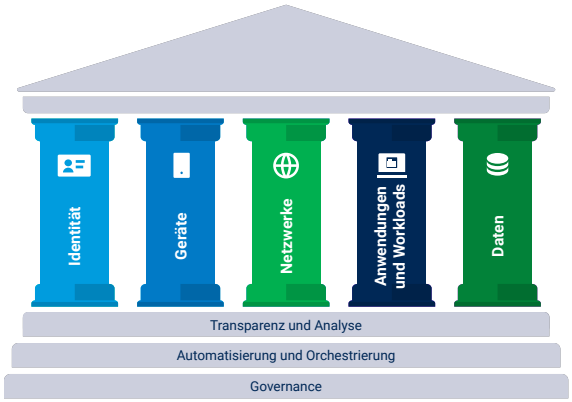


Abb. 1: Das ZTMM der CISA ist eines von vielen Instrumenten zur Unterstützung der Zero-Trust-Umstellung (Quelle: CISA)

Jedem dieser Bereiche wird ein Reifegrad zugewiesen, der beschreibt, wie weit das Unternehmen auf dem Weg zu einem Zero-Trust-Ansatz fortgeschritten ist. Die vier Reifegrade (klassisch, anfänglich, fortgeschritten und optimal) beschreiben den Weg von manueller Konfiguration und VPNs zur idealen „perimeterlosen Sicherheit“ (Abbildung 2). Beim Reifegrad „Optimal“ gewähren Unternehmen Anwendungen nur minimale Berechtigungen, verweigern anfälligen Geräten die Authentifizierung und den Zugriff, verhindern die Ausbreitung interner Bedrohungen und erkennen und reagieren sofort auf Sicherheitsvorfälle. (Eine ausführlichere Beschreibung des ZTMM-Frameworks finden Sie in Anhang B.)

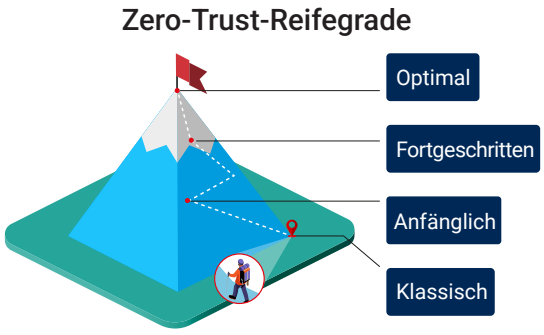


Abb. 2: Zero-Trust-Reifegrade (Quelle: CISA)

Indem Bereiche hervorgehoben werden, in denen der Reifegrad am geringsten ist, unterstützt das ZTMM Unternehmen bei der Entwicklung einer ausgewogeneren Sicherheitsumgebung. Und mit der branchenführenden Sicherheitssuite von Akamai in Kombination mit unserem Fachwissen erreichen sie einfacher denn je eine ausgereifte Sicherheit.

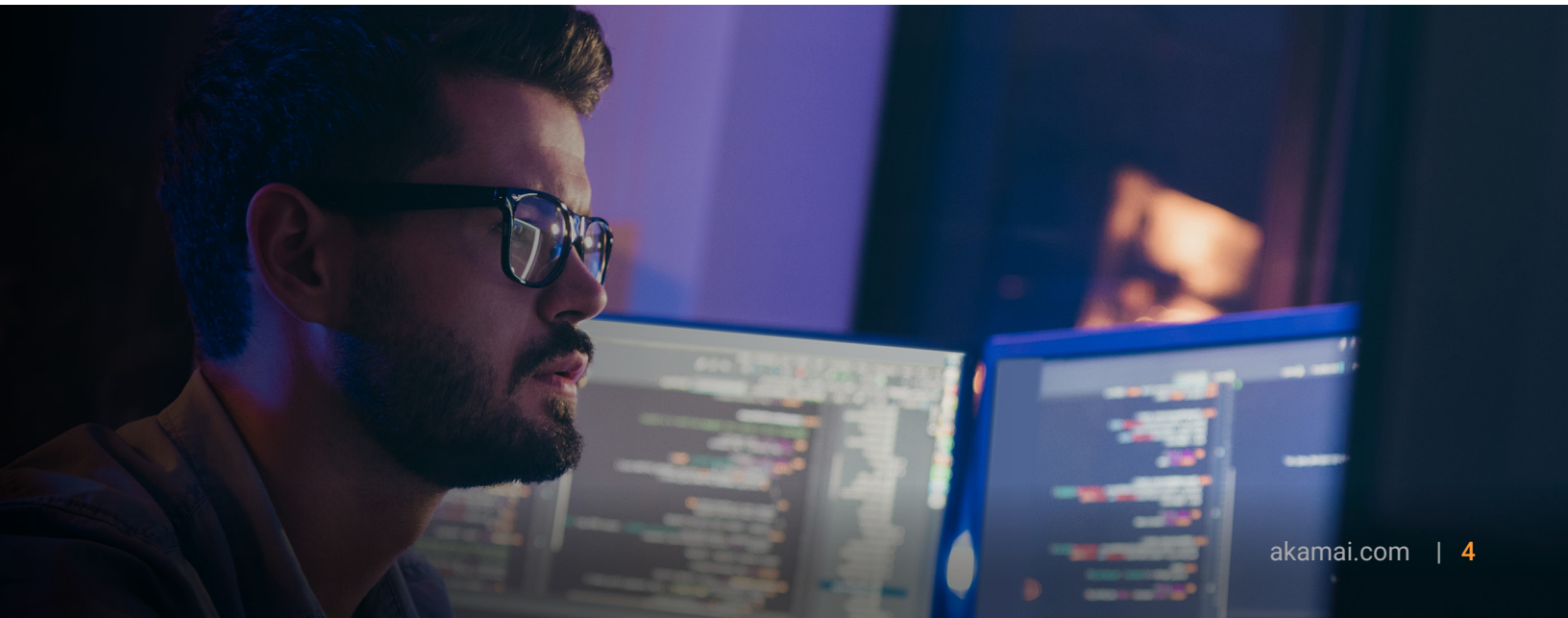
Fällt es Ihren Teams schwer, Zero Trust zu implementieren? Damit sind Sie nicht allein.

Die Verantwortung für den Aufbau einer Zero-Trust-Architektur liegt nicht bei einer einzigen Abteilung. Sie erfordert Unterstützung, Flexibilität und Zustimmung von verschiedenen Stakeholdern auf allen Ebenen des Unternehmens.

Akamai ist das Unternehmen für Cybersicherheit und Cloud Computing, das das digitale Leben unterstützt und schützt. Unsere marktführenden Sicherheitslösungen, überlegene Threat Intelligence und unser globales Betriebsteam schützen kritische Daten und Anwendungen an jedem Touchpoint weltweit. Dank dieser umfassenden Perspektive kennen wir die häufigsten Herausforderungen beim Umstieg auf Zero-Trust-Sicherheit – und wir unterstützen Sie gern dabei, die richtigen Lösungen zu finden.

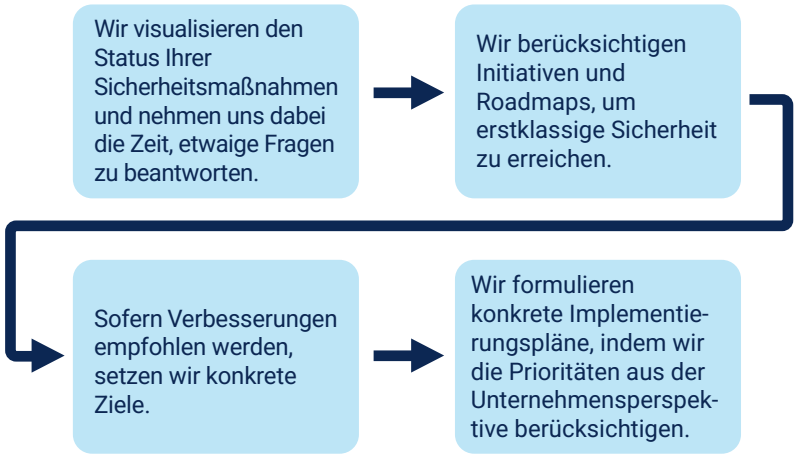
Drei häufige Zero-Trust-Herausforderungen

1. **Der richtige Einstieg:** Wir empfehlen in der Regel, mit der Workload-Transparenz zu beginnen und die Angriffsfläche zu reduzieren, um die Cyberresilienz zu verbessern. Doch das hängt natürlich von der aktuellen Sicherheitslage des Unternehmens ab.
2. **Schnelle Erfolge:** Zero Trust wirkt oft wie ein riesiges Unterfangen, weshalb es für Teams schwierig sein kann, sich auf eine Sache zu konzentrieren oder kleine Fortschritte zu feiern.
3. **ROI-Nachweis:** Zero-Trust-Projekte sind nicht billig und erfordern in der Regel kulturelle und technologische Veränderungen innerhalb eines Unternehmens. Die Fähigkeit, den ROI nachzuweisen – egal, ob es sich hierbei um eine reduzierte Angriffsfläche, eine abgewendete Sicherheitsverletzung, eine geschlossene Schwachstelle oder einen finanziellen Gewinn handelt –, ist von entscheidender Bedeutung. Das gilt insbesondere für Entscheidungsträger und Sicherheitsexperten.



Sind Sie bereit, Ihre Zero-Trust-Reise zu beginnen und Ihre aktuelle Sicherheit zu visualisieren?

Wie wir bei Akamai können auch Sie mithilfe des ZTMM den Reifegrad Ihrer aktuellen Sicherheitsmaßnahmen visualisieren. So können Sie ermitteln, wie Sie Ihren Prozess ausgewogener gestalten können und was Sie ändern müssen, um eine Zero-Trust-Architektur zu erreichen.



So kann Akamai Ihre Zero-Trust-Sicherheitsstrategie unterstützen

Eine erfolgreiche Zero-Trust-Architektur nutzt eine Vielzahl von Kontrollmechanismen und Prinzipien, um Sicherheitsschwachstellen zu begegnen.

Wir arbeiten mit Initiativen und Roadmaps, um Ihnen bei der Erstellung eines Implementierungsplans zu helfen, der Ihr gesamtes Unternehmen und seine Ziele berücksichtigt, damit Sie am Ende erstklassige Sicherheit erreichen. Mit diesem Ansatz können wir gemeinsam mit Ihnen Sicherheitssysteme und -prozesse entwickeln, die auf lange Sicht effektiv funktionieren.

Neben der Akamai Cloud sorgt unsere Suite von Sicherheitsprodukten – darunter auch eine fortschrittliche verteilte ZTNA-Lösung (Zero Trust Network Access, ZTNA), branchenführende Mikrosegmentierung, Phishing-sichere Multi-Faktor-Authentifizierung (MFA) sowie eine proaktive DNS-Firewall – dafür, dass Ihre Sicherheit den Zero-Trust-Reifegrad „Optimal“ erreicht. Darüber hinaus kann das gesamte System mit nur einem Agent und über eine einzige Konsole ausgeführt werden (Abbildung 3).

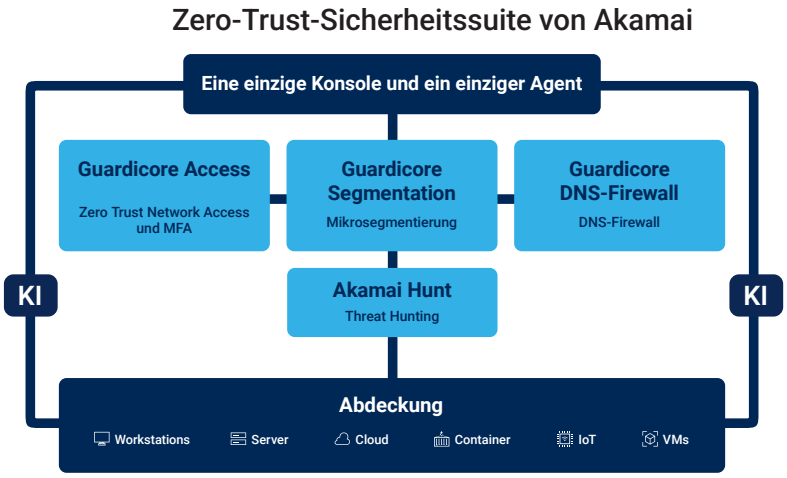


Abb. 3: Die Suite von Akamai-Sicherheitsprodukten kann mit nur einem Agent und über eine einzige Konsole ausgeführt werden.

Fallstudie

Visualisierung der Sicherheit eines multinationalen E-Commerce-Einzelhändlers mithilfe des Zero Trust Maturity Model

Vor Kurzem haben wir die Sicherheit eines multinationalen Einzelhändlers im E-Commerce-Bereich analysiert. Dabei haben wir seinen Sicherheitsstatus visualisiert und eine entsprechende Roadmap bereitgestellt, um ihn auf dem Weg zu erstklassiger Sicherheit voranzubringen. Unser Expertenteam hat im gesamten ZTMM Verbesserungsbereiche ermittelt, die wir nach Priorität von „hoch“ bis „niedrig“ bewertet haben. Im Folgenden stellen wir die Ergebnisse vor.

Ein unausgewogenes System mit unterschiedlichen Reifegraden

In jeder Säule haben wir einige Funktionen gefunden, die den höchsten (optimalen) Reifegrad erreichten, darunter Mobile Device Management und die Automatisierung der Anwendungsbereitstellung. Doch es fanden sich auch in jeder Säule einige Funktionen mit dem Reifegrad „Klassisch“, was ein erhebliches Risiko darstellte.

Insbesondere waren wichtige Funktionen in den Säulen „Identität“ und „Netzwerk“ nicht verstärkt worden – und diese Säulen sind die Grundlage einer Zero-Trust-Architektur. Zu diesen Funktionen gehörten MFA, integriertes Management der Identitätsinfrastruktur, kontextbasierte Zugriffskontrolle und Mikrosegmentierung.

Riskante ID-Infrastruktur

Unsere Analysten haben ergeben, dass die Authentifizierung bei dem Einzelhändler standardmäßig über IDs und Passwörter erfolgte. Der Einsatz der MFA war auf wenige Systeme beschränkt. Hierdurch bestand ein hohes Risiko für den Missbrauch von Authentifizierungsinformationen. Darüber hinaus waren mehrere ID-Infrastrukturen vorhanden, wie z. B. Microsoft Entra ID, lokales Active Directory (AD) sowie das Lightweight Directory Access Protocol (LDAP). Da das Management des Einzelhändlers nicht integriert war, bestand das Risiko, dass sich Sicherheitsverletzungen von einer anfälligeren ID-Infrastruktur (z. B. LDAP) auf interne Systeme ausbreitete.

Nicht integrierte Autorisierungskontrollen

Autorisierungskontrollen waren nicht integriert, sodass jede Anwendung separat gehandhabt wurde. Es war nicht möglich, den Zugriff durch anfällige Geräte oder verdächtige Zugriffsversuche zu blockieren: Wenn der PC eines Mitarbeiters oder Partners, der Zugang zum Unternehmensnetzwerk hatte, mit Malware infiziert wurde, bestand ein hohes Risiko eines unbefugten Zugriffs auf Systeme und Ressourcen über laterale Netzwerkbewegung.

Unzureichende Segmentierung

Wir stellten fest, dass sich die Sicherheitsmaßnahmen des Einzelhändlers stark auf externe Bedrohungen konzentrierten. Die Risiken, die von Angreifern ausgingen, die bereits in das Netzwerk eingedrungen waren, wurden jedoch übersehen. Ohne eine leistungsstarke interne Segmentierung könnte sich ein Angreifer, der über das WLAN in einem Warenlager oder über Schwachstellen im VPN eindringt, unkontrolliert lateral im Netzwerk bewegen. Das Fehlen interner Barrieren erhöhte das Risiko weitreichender Systeminfektionen, Datenverluste und Betriebsausfälle erheblich, da sich Angriffe ungehindert im Netzwerk ausbreiten konnten, ohne dass Maßnahmen zur Eindämmung existierten.

Unzureichendes Sicherheitsmanagement und -reaktion

Der Einzelhändler verfügte nicht über ein Managementsystem, das eine Software-Stückliste mit Schwachstelleninformationen verknüpfen konnte. Es war also nicht in der Lage, Anwendungsschwachstellen schnell zu erkennen und darauf zu reagieren. Dies stellte ein hohes Risiko dar.

Unsere Empfehlungen

Wir haben dem Einzelhändler empfohlen, die folgenden fünf Schritte zu unternehmen, um seine Sicherheit zu erhöhen:

1. Proaktive Maßnahmen ergreifen, um das Risiko eines unbefugten Eindringens und lateraler Netzwerkbewegungen zu verringern, das beim aktuellen Setup bestand
2. Die Identitätsinfrastruktur weiter in den vorhandenen Technologie-Stack integrieren
3. Einen Plan zur Erweiterung der Authentifizierungs- und Autorisierungsfunktionen in Verbindung mit Zero-Trust-Netzwerkzugriff entwickeln
4. Die effektivste Methode zur Implementierung präziser Schutzmaßnahmen für Workloads und Anwendungen auswählen
5. Ein Reaktionssystem und einen Prozess für unbekannte künftige Bedrohungen aufbauen; ein System und einen Prozess entwickeln, um Sicherheitsmanagement und -reaktionen zu verbessern; und einen Plan formulieren

Wenn Sie sich für Zero Trust interessieren, wenden Sie sich an uns, um eine kostenlose Sicherheitsbewertung zu erhalten.

Anhang A: Ein Überblick über das Zero-Trust-Konzept

Zero Trust ist eine Sicherheitsphilosophie, die darauf basiert, dass keinem Nutzer, keinem Gerät und keinem System – egal, ob innerhalb oder außerhalb des Unternehmensnetzwerks – vertraut werden sollte.

Stattdessen werden Verifizierungsprozesse und Überwachung eingesetzt, um Risiken zu minimieren. Dazu gehören Ansätze wie die Durchsetzung strenger Richtlinien für Identitäts- und Zugriffsmanagement (Identity and Access Management, IAM), die Verwendung von Multi-Faktor-Authentifizierung (MFA) und die Priorisierung rollenbasierter Zugriffskontrollen (Role-Based Access Control, RBAC).

Das Zero-Trust-Konzept gibt es seit 15 Jahren, hat jedoch während der Coronapandemie immer mehr an Bedeutung gewonnen, als Unternehmen zunehmend mit Remotezugriff arbeiten mussten. Viele Unternehmen stellten fest, dass ihre bestehenden Sicherheitsmaßnahmen nicht mehr mithalten konnten, als Nutzer und Geräte plötzlich an verschiedenen Orten und nicht mehr zentralisiert waren.

Heute gibt es viele Möglichkeiten der Implementierung für Zero-Trust-Prinzipien, darunter Zero-Trust-Architekturen, Zero-Trust-Netzwerkzugriff (Zero Trust Network Access, ZTNA), Zero Trust Secure Web Gateways (SWGs) und Mikrosegmentierung.

Erfahren Sie mehr über Zero Trust

Anhang B: Das ZTMM-2.0-Framework

Die fünf Säulen

Die Säulen können sich in unterschiedlichem Tempo weiterentwickeln – so lange, bis eine säulenübergreifende Koordination erforderlich ist.

Säule	Beschreibung
Identität	Ein Attribut oder eine Reihe von Attributen, die einen Nutzer oder ein anderes Element im Netzwerk eindeutig beschreiben
Geräte	Jedes Asset, das mit einem Netzwerk verbunden werden kann, darunter Server, Desktop-PCs, Laptops, Drucker, Mobiltelefone, IoT-Geräte (Internet of Things), Netzwerkgeräte etc.
Netzwerke	Ein offenes Kommunikationsmedium, etwa typische Kanäle wie interne Netzwerke von Behörden, WLANs oder das Internet sowie andere potenzieller Kanäle für die Übermittlung von Nachrichten
Anwendungen und Workloads	Behördensysteme, Computerprogramme und Services, die lokal, auf mobilen Geräten und in Cloud-Umgebungen ausgeführt werden
Daten	Strukturierte und unstrukturierte Dateien und Dateifragmente, die sich aktuell oder zuvor in Systemen, Geräten, Netzwerken, Anwendungen, Datenbanken, Infrastrukturen und Backups befinden bzw. befanden, sowie die zugehörigen Metadaten

Säulenübergreifende Fähigkeiten

Diese drei Funktionen unterstützen das gesamte Zero-Trust-Framework und sorgen so für integrierte, reaktionsschnelle und einheitliche Sicherheitsmaßnahmen.

Fähigkeiten	Beschreibung
Transparenz und Analyse	Unternehmen brauchen eine klare Echtzeitübersicht aller Nutzeraktivitäten, Gerätestatus und Netzwerkinteraktionen. So werden Bedrohungen schnell erkannt und angegangen, wodurch Risiken reduziert werden, und Unternehmen können fundierte, proaktive Sicherheitsentscheidungen treffen.
Automatisierung und Orchestrierung	Menschliche Fehler sind eine häufige Ursache für Sicherheitsprobleme. Wenn Automatisierung und Orchestrierung optimiert werden, wird die Wahrscheinlichkeit solcher Fehler minimiert. Automatisierung vereinfacht Routineaufgaben, während Orchestrierung Sicherheitsaktionen systemübergreifend koordiniert. So entstehen die richtigen Bedingungen für eine schnellere, koordiniertere Reaktion auf Bedrohungen.
Governance	Gute Sicherheits-Governance schafft Verantwortlichkeit und stellt sicher, dass alle dieselben Sicherheitspraktiken und -vorschriften befolgen. Das schafft eine solide Grundlage für einen sicheren Betrieb. Sie legt außerdem klare Zero-Trust-Richtlinien fest und hilft Unternehmen bei der Einhaltung von Compliance-Standards.

Der Reifeaspekt des Zero Trust Maturity Model

ZTMM 2.0 definiert vier Reifegrade für jede Funktion. Das Ziel besteht darin, den aktuellen Reifegrad der fünf Säulen und der drei Fähigkeiten zu bestimmen und anschließend einen Plan zu erstellen, um jede Säule und Fähigkeit auf dem Weg zum höchsten Reifegrad weiterzuentwickeln.

Reifegrad	Beschreibung
Klassisch	Manuelle Konfiguration, Reaktion und Risikominderung; statische und isolierte Richtlinien und Lösungen
Anfänglich	Beginnende Automatisierung; anfängliche säulenübergreifende Lösungen; einige reaktive Änderungen im Bereich der geringstmöglichen Berechtigungen; aggregierte Transparenz für interne Systeme
Fortgeschritten	Automatisierte Kontrollen, wo möglich; säulenübergreifende Richtliniendurchsetzung; Änderungen im Bereich der geringstmöglichen Berechtigungen basierend auf Risiko/Sicherheitsstatus; Reaktion durch vordefinierte Maßnahmen
Optimal	Automatisierte Kontrollen, wo möglich; säulenübergreifende Richtliniendurchsetzung; Änderungen im Bereich der geringstmöglichen Berechtigungen basierend auf Risiko/Sicherheitsstatus; Reaktion durch vordefinierte Maßnahmen

Kontaktieren Sie uns, um zu besprechen, wie die Akamai-Sicherheitssuite langfristig die Sicherheit Ihres Unternehmens unterstützen kann.