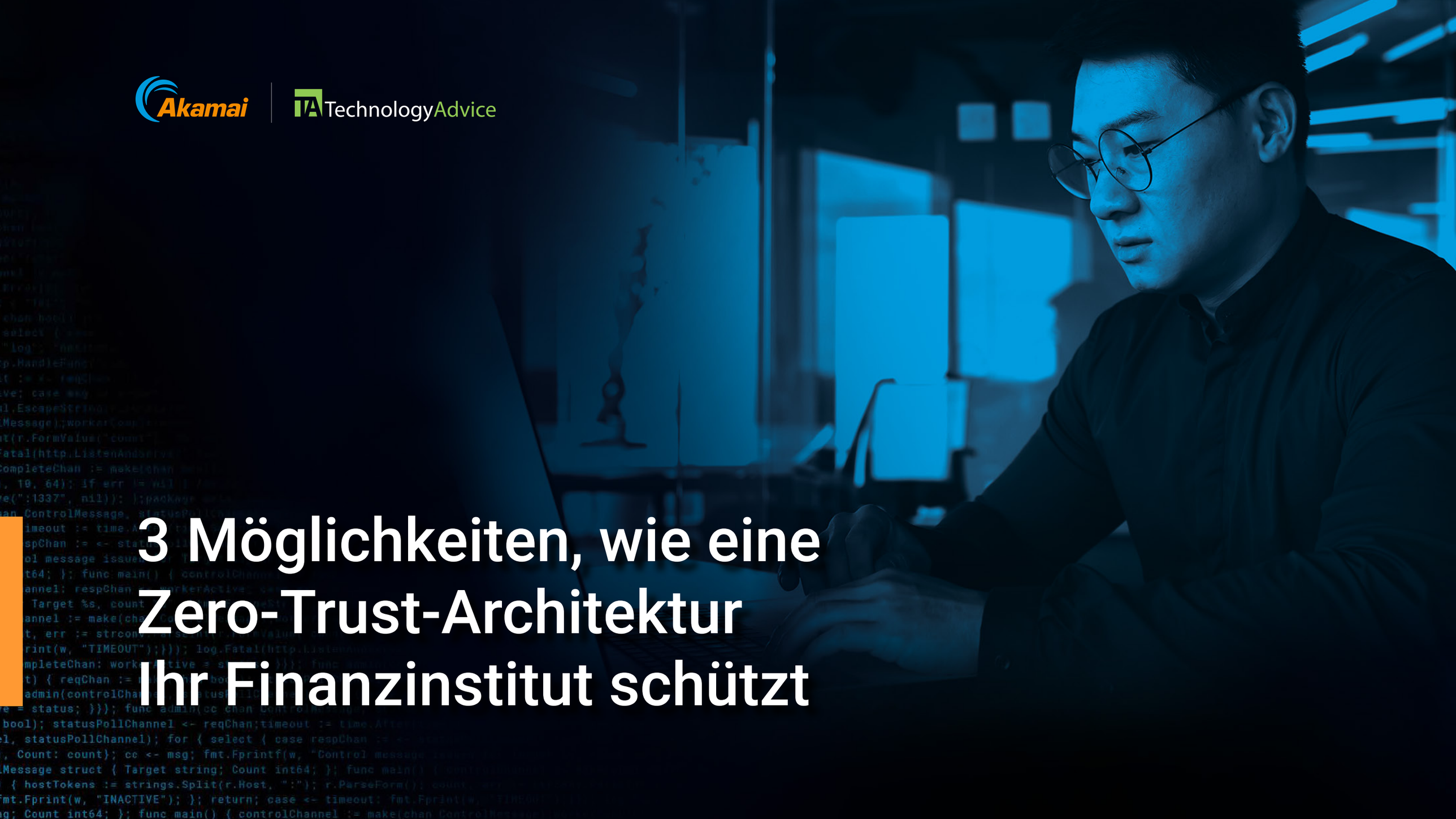
Akamai | TechnologyAdvice



3 Möglichkeiten, wie eine Zero-Trust-Architektur Ihr Finanzinstitut schützt

Finanzinstitute sind nach wie vor die Hauptziele für Bedrohungsakteure und sehen sich im Vergleich von Q2 2022 zu Q2 2023 mit einem Anstieg der Angriffe auf Webanwendungen und APIs um 65 % konfrontiert. Dieser unablässige Angriff von sich weiterentwickelnden Cyberbedrohungen bindet nicht nur Ressourcen, sondern lenkt auch die Aufmerksamkeit von wichtigen Geschäftsfunktionen ab.

Herkömmliche Firewall- und Endpoint-Lösungen vertrauen Endpoints, Geräten und Nutzern implizit. Dazu müssen diese nur die anfängliche Überprüfung einer Kombination aus Passwort und Nutzername überstehen – auch wenn sie gelegentlich durch Multi-Faktor-Authentifizierung (MFA) verstärkt wird. Anwendungen, APIs und Systemservices innerhalb des Netzwerks funktionieren oft ohne Sicherheitsüberprüfung, die über die grundlegende Überwachung von Endpoint-Malware hinausgeht. Um sich den wachsenden Bedrohungen durch Ransomware, strengen Compliance-Auflagen und den Herausforderungen der Cloudmigration zu stellen, setzen Finanzinstitute jetzt auf Zero Trust.

Zero Trust eliminiert implizites Vertrauen und überprüft kontinuierlich die Zugriffsberechtigungen für alle Anwendungen, Nutzer und Geräte basierend auf dem Kontext der Anfragen und Berechtigungen. Selbst wenn ein Angreifer ein Gerät oder Anmeldedaten für den Zugriff auf ein Netzwerk kompromittieren kann, kann der Zugriff stark eingeschränkt und der Schaden erheblich reduziert werden.

Aber wie genau schützt ein Zero-Trust-Framework Ihr Finanzinstitut?

Einhalten von sich ständig ändernden Vorschriften

Finanzinstitute müssen erhebliche Ressourcen für den Nachweis der Einhaltung verschiedener Vorschriften bereitstellen, wie etwa des weit verbreiteten Payment Card Industry Data Security Standard (PCI DSS) oder des kommende Digital Operational Resilience Act (DORA), der voraussichtlich im Januar 2025 vollständig zur Anwendung kommen wird. Audits nehmen aufgrund unklarer, widersprüchlicher und sich ändernder Anforderungen regelmäßig in Bezug auf Komplexität, Kosten und Zeit zu. Dennoch müssen Finanzinstitute diese Investition tätigen, da nicht bestandene Audits auch zu Umsatzeinbußen, behördlichen Sanktionen, Bußgeldern oder Strafen sowie zum Verlust von Reputation und potenziellen rechtlichen Konsequenzen führen können.

Compliance-Berichte erfordern klare und genaue Konten der Systeme, die mit regulierten Daten in Berührung kommen, sowie einen Nachweis, dass diese Systeme angemessen geschützt sind. In einem großen Finanzinstitut ist die IT-Umgebung jedoch zu groß, zu detailliert und zu komplex, um Assets und Zugriffe einfach nachverfolgen zu können.

Legacy-Firewalls und Endpoint-Schutzmaßnahmen verfolgen und schützen in erster Linie herkömmliche Nutzer und Assets. Sich nur auf diesen herkömmlichen Netzwerksegmentierungsansatz zu verlassen sorgt für Probleme bei der Skalierung, behindert die Erstellung und Durchsetzung von Richtlinien und schränkt die Agilität ein.

Um die Herausforderungen älterer Umgebungen mit Technologien zu meistern, die an zukünftige Strategien angepasst sind, benötigen Finanzinstitute eine detaillierte Übersicht über den East-West-Traffic sowie die Möglichkeit, Segmentierungsrichtlinien in Multicloud- und Containerumgebungen durchzusetzen. Angesichts der wachsenden Notwendigkeit, mehrere Regionen und IT-Infrastrukturtypen zu verwalten, einschließlich Containertechnologie, benötigen Finanzinstitute eine einfache und geradlinige Möglichkeit, um Mikrosegmentierung mit Richtlinienflexibilität, DevOps-Integration und Automatisierung zu erreichen.

Ohne regelmäßige Identifizierung, Nachverfolgung und Sicherung aller Assets kann ein Finanzinstitut nicht sicherstellen, dass der Zugriff auf regulierte Daten vollständig kontrolliert und geschützt ist. Das Übersehen oder unzureichende Überwachen von Daten, Nutzern, Anwendungen oder Geräten erhöht das Risiko eines Cyberangriffs und das potenzielle Scheitern eines Compliance-Audits erheblich.

Die Zero-Trust-Architektur verweigert standardmäßig den Zugriff und alle Verbindungen müssen explizit mit Kontext gewährt werden: dem autorisierten Nutzer auf einem autorisierten Gerät mit autorisiertem Zugriff auf die angeforderten Daten. Zero Trust setzt standardmäßig auf den Zugriff mit den geringsten Berechtigungen, wodurch vergessene oder unbekannte Legacy-Verbindungen unterbrochen werden. Die Lösung von Akamai identifiziert schnell nicht autorisierte Geräte, ältere Nutzer (Mensch, API oder Anwendung) und vergessene Datenquellen, die ältere Zweigstellen oder die alten technischen Umgebungen übernommener Unternehmen kompromittieren.

Die Zero-Trust-Architektur von Akamai ist unabhängig vom Standort des Nutzers. Dennoch kann der Kontext des Standorts in den Entscheidungsprozess für den Zugriff einbezogen werden. Sicherheitsteams erhalten Kontrolle und Reporting – in konsolidierter Form, um den Zugriff auf Assets in lokalen Netzwerken, Rechenzentren oder der Cloud schnell zu analysieren und vollständig zu verwalten.

Angesichts des erhöhten regulatorischen Drucks, kritische Anwendungen zu schützen und den East-West-Traffic zu sichern, konzentrieren sich Finanzinstitute darauf, die Sichtbarkeit und das Verständnis ihrer Umgebungen zu verbessern. Mithilfe von Zero-Trust-Prinzipien können sie nun nicht konforme Assets nahtlos identifizieren und segmentieren, sodass Anwendungsteams die Segmentierungsrichtlinien autonom verwalten können. Dies gewährleistet einen effizienten Workflow und vereinfacht den Reportingprozess.

Die vollständige Transparenz des East-West-Traffics mit Kontext ermöglicht müheloses Zuordnen und Eingrenzen geschäftskritischer Anwendungen ohne Änderungen an Infrastruktur oder Anwendungen. Diese Funktion ermöglicht es Institutionen, den Zugriff für Dritte einzuschränken und die allgemeine Sicherheit zu erhöhen.

Transparenz optimiert die sichere Migration in die Cloud. Die Segmentierung ist überdies in den DevOps-Zyklus integriert, um sofortige Richtlinienaktualisierungen ohne erhebliche Infrastrukturänderungen zu gewährleisten, was eine Abkehr von früheren VLAN-Praktiken darstellt. Darüber hinaus ermöglicht und vereinfacht Akamai die einheitliche Erstellung, Durchsetzung und das Reporting von Compliance-Richtlinien über mehrere Infrastrukturen hinweg. Dies wird durch erhöhte Transparenz, Zuordnung von Anwendungsabhängigkeiten, automatisierte Segmentierungsrichtlinien, Automatisierung von DevOps-Richtlinien und nahtlose Integration des Änderungsmanagements erreicht.

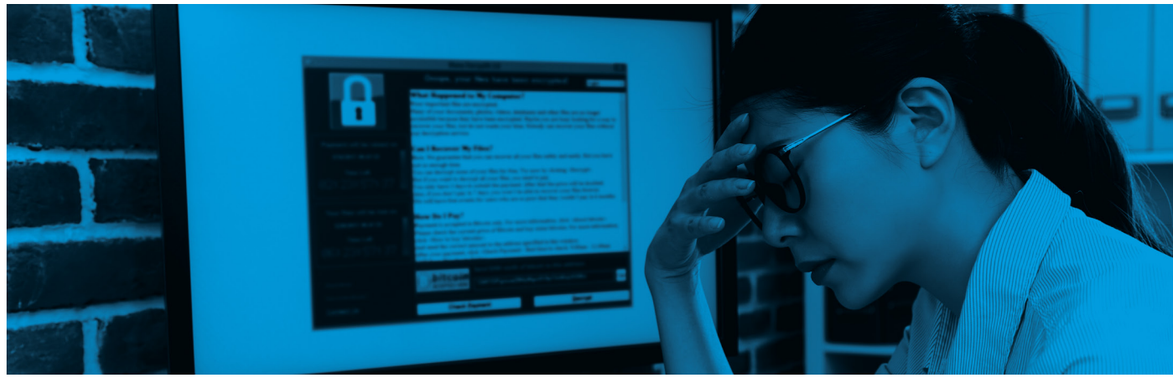
Verhindern Sie die Ausbreitung von Ransomware

Von Zweigstellen bis hin zu globalen Finanzinstituten: Ransomware-Angriffe sorgen weltweit für Schlagzeilen und Probleme. Laut dem Ransomware Market Report (Ransomware-Marktbericht) von Cybersecurity Ventures aus dem Jahr 2022 wird „Ransomware bis 2031 alle zwei Sekunden ein Unternehmen, einen Verbraucher oder ein Gerät angreifen“.

Da Finanzdienstleister so oft durch Fusionen oder Übernahmen wachsen, mangelt es ihnen meistens an Einblicken in ihr gesamtes Technologie-Ökosystem. Dadurch stehen den Angreifern Tür und Tor offen. Ransomware-Angreifer nutzen Backdoors aus oder verwenden Phishing-Angriffe, um entweder Anmeldedaten zu stehlen oder unbekannte Malware auf Endgeräten zu platzieren, die den Endpointschutz umgehen.

Übermäßig freizügige Nutzerzugriffsrichtlinien und passwortorientierte Authentifizierung ermöglichen es den Angreifern, Firewalls zu umgehen, der Erkennung von Endpunkten zu entgehen und uneingeschränkten Zugriff auf Netzwerke zu erhalten, die implizit Traffic, Nutzern und verbundenen Geräten vertrauen. Ransomware-Angreifer, die häufig in organisierten Gruppen wie CL0P operieren, nutzen kompromittierte Assets aus und bewegen sich dann lateral durch das Netzwerk, um andere gefährdete Assets zu entdecken und auszunutzen. Zero-Day-Schwachstellen wie die SQL-Injection-Sicherheitslücke MOVEit ermöglichen es Angreifern, Zugriff zu erlangen und das Netzwerk schnell zu infizieren, indem sie automatisierte Skripte verwenden, um Systeme zu verschlüsseln, Daten zu stehlen und Lösegeldforderungen zu stellen.

Mit den Zero-Trust-Lösungen von Akamai können Finanzinstitute kritische Systeme identifizieren und isolieren und den Netzwerkzugriff auf und von diesen Systemen einschränken. Dieser Ansatz minimiert die Wahrscheinlichkeit, die Auswirkungen und den Zeitaufwand für die Behebung eines Ransomware-Angriffs. Zunächst verfolgt und überwacht Akamai schädliche Domains und IP-Adressen. Dabei werden geeignete Quarantänen implementiert, um den Start vieler Angriffe zu verhindern.



Akamai überwacht und steuert den Traffic bis zu den Prozess- und Serviceebenen und ermöglicht so fast eine Echtzeiteinsicht in den Netzwerktraffic. Dank dieser umfassenden Einblicke können die Teams von Security Operations Center und Network Operations Center die jeweiligen Bedrohungen genau identifizieren und gezielt bekämpfen.

Als Nächstes wird selbst ein erfolgreicher Angriff durch die Mikrosegmentierung von Akamai Guardicore Segmentation stark eingeschränkt. Anmeldedaten und Berechtigungen werden bei jeder Zugriffsanfrage kontinuierlich überprüft. Verbindungen zu Anwendungen, die von Akamai Enterprise Application Access geschützt sind, werden abgelehnt.

Darüber hinaus werden Anwendungen, Server und andere Ressourcen, die von einem Nutzer nicht benötigt werden, automatisch vor der Erkennung verborgen. Dadurch wird den Angreifern die laterale Netzwerkbewegung oder die Erweiterung des Zugriffs verwehrt. Schließlich wird die Anomalieerkennung von Akamai Hunt ungewöhnliches Verhalten anzeigen und Sicherheitsteams benachrichtigen. So können Sie diese Angriffe erkennen, bevor Daten extrahiert oder verschlüsselt werden können.

Optimieren Sie die digitale Transformation

Um Agilität, Skalierbarkeit und Modernisierung zu ermöglichen, verschieben viele Finanzinstitute ihre Anwendungen in die Cloud. Ein derartiger Schritt bringt jedoch eine ganze Reihe neuer Herausforderungen mit sich.

Zunächst einmal können Finanzinstitute unerkannte und unbekannte Assets und Verbindungen nicht migrieren. Darüber hinaus erweitern Cloudmigrationen nicht nur die Angriffsfläche. Die Integration von Multicloud und lokalen Hybrid Clouds machen häufig Anwendungen unbrauchbar und führen zu Lücken in etablierten Sicherheitsebenen. Darüber hinaus wird eine per Software bereitstellbare Infrastruktur (Container, virtuelle Maschinen usw.) automatisch zu schnell bereitgestellt, als dass Legacy-Lösungen diese effektiv sichern oder überwachen könnten.

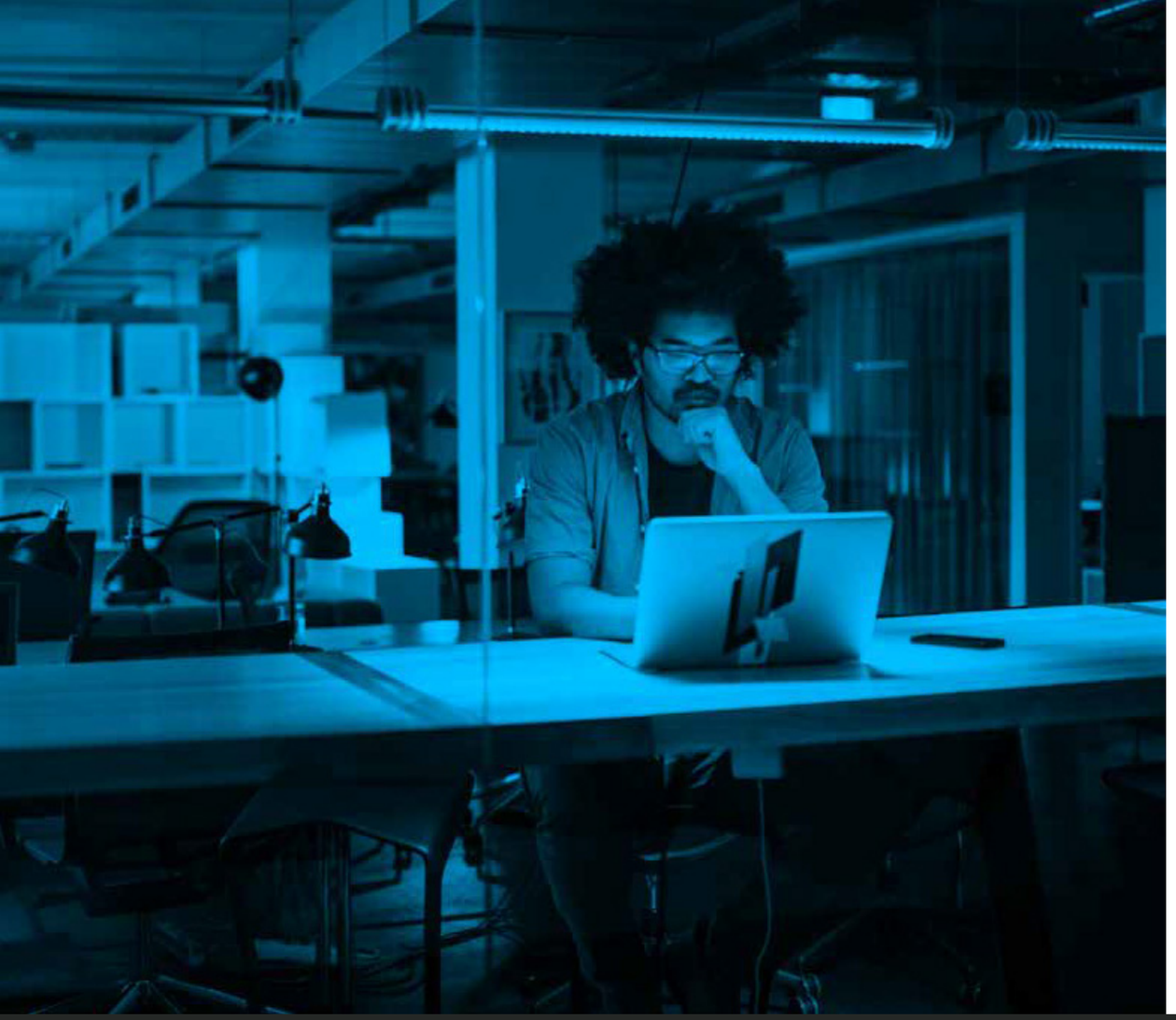
Zero-Trust-Lösungen stellen sicher, dass Finanzinstitute ihre cloudbasierten Anwendungen einfacher bereitstellen können – und das bei stärkerem Schutz und geringerem Betriebsaufwand. Die Zero-Trust-Lösungen von Akamai verfolgen alle Datenflüsse, um die potenzielle Angriffsfläche schnell zu identifizieren und Richtlinien durchzusetzen, ohne dabei das Geschäft zu stören.

Sobald diese erkannt wurden, können Sicherheits- und Betriebsteams die zentrale Steuerung von Akamai nutzen, um Anwendungen zu segmentieren, zu sichern und Datenflüsse zu überwachen. Akamai bietet eine detaillierte Kontrolle und senkt gleichzeitig die Betriebskosten und -komplexität. Für Sicherheits- und Betriebsteams in Finanzinstituten sorgt die Durchsetzung universeller Richtlinien für eine schnelle und flexible Modernisierung der Infrastruktur. Dies wird durch die zuverlässige Sicherheit der Zero-Trust-Segmentierung mit den geringstmöglichen Berechtigungen erreicht, die einen leistungsstarken Schutz vor sich entwickelnden Bedrohungen bietet.

Finanzinstitute können es sich nicht leisten, Zero Trust zu ignorieren

Angriffe auf ältere Technologien können zu gravierenden Datenschutzverstößen führen, Schäden in Millionenhöhe verursachen und das Vertrauen von Kunden und Partnern zerstören. Angriffe werden immer ausgeklügelter und schneller – ohne vollständigen Einblick in das technische Ökosystem lassen Finanzinstitute möglicherweise Hintertüren offen.

Akamai bietet mehr Transparenz in das Netzwerk, schränkt den Nutzerzugriff intelligent ein, sucht ständig nach Bedrohungen und weist auf Anomalien zur Sicherheitsüberprüfung hin. Erfahren Sie mehr darüber, wie Sie die Anforderungen Ihres Finanzinstituts mit dem Zero-Trust-Portfolio von Akamai erfüllen können.



Erfahren Sie mehr über den Schutz Ihrer digitalen Finanzabteilung mit Akamai

Weitere Informationen

TechnologyAdvice | Akamai

Akamai schützt Ihr Kundenerlebnis, Ihre Mitarbeiter, Systeme und Daten und integriert Sicherheit in alle von Ihnen erstellten Inhalte – überall dort, wo Sie sie erstellen und bereitstellen. Dank der Einblicke unserer Plattform in globale Bedrohungen können Sie Ihre Sicherheitsstrategie anpassen und weiterentwickeln, um Zero Trust zu implementieren, Ransomware zu stoppen, Anwendungen und APIs zu schützen oder DDoS-Angriffe abzuwehren. Das gibt Ihnen das nötige Vertrauen, um kontinuierlich Innovationen zu entwickeln, zu expandieren und alles zu transformieren, was möglich ist. 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.