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

Es gibt vier wichtige Szenarien für die Implementierung einer Zero-Trust-Architektur als Sicherheitsmodell. Erfahren Sie mehr über die potenziellen Vorteile.

Ein Zero-Trust-Sicherheitsmodell bietet viele Vorteile. Am meisten profitieren Unternehmen jedoch von den folgenden vier Geschäftsszenarien:

Alle 2 Sekunden

Bekämpft Ransomware

Häufigkeit der erwarteten Ransomware-Angriffe pro Unternehmen, Verbraucher oder Gerät bis 2031

Ransomware-Marktbericht von Cybersecurity Ventures

70 %

Schützt hybride Belegschaften

Aus einem Gartner®-Bericht: „Gemäß einer Prognose von Gartner erfolgen bis 2025 mindestens 70 % der neuen Remotezugriff-Implementierungen überwiegend über ZTNA-Services und nicht über VPN-Services. Ende 2021 lag dieser Wert noch unter 10 %."

Gartner Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access, 8. April, 2022, Nat Smith, Mark Wah, Christian Canales

PCI DSS, HIPAA, SWIFT, DSGVO

Umsetzung von Compliance

Einige der gesetzlichen Auflagen, die Unternehmen mithilfe eines Zero-Trust-Sicherheitsmodells leichter umsetzen können

Eine Plattform für alle Ihre Zero-Trust-Anforderungen

Akamai bietet eine einheitliche Lösung für alle Ihre Zero-Trust-Anforderungen

- Segmentierung
- Secure Internet Access Enterprise
- Zero-Trust-Netzwerkzugriff
- MFA

Stoppen Sie die Ausbreitung von Angriffen im gesamten Netzwerk und wechseln Sie schneller zu Zero Trust.

E-Book herunterladen