Die wichtigsten Überlegungen bei der Implementierung von Zero Trust

Da Cyberangriffe immer häufiger geschehen und immer ausgefeilter werden, müssen Unternehmen alles tun, um ihre Verteidigung zu stärken. Die Implementierung von Zero Trust ist ein unerlässlicher Schritt, doch Unternehmen müssen auch den technologischen Wandel und die Nutzererwartungen berücksichtigen.

Alle 2 Sekunden

Die Bedrohungen häufen sich

Erwartete Häufigkeit von Ransomware-Angriffen auf Unternehmen, Verbraucher und Geräte bis 2031

Ransomware-Marktbericht von Cybersecurity Ventures

31 %

EMEA wird angegriffen

Prozentsatz der Opfer von Ransomware-Angriffen aus EMEA – der Region, die am zweithäufigsten betroffen ist – vom 1. Mai 2021 bis 30. April 2022

Bedrohungsbericht von Akamai zu Ransomware H1 2022

41 %

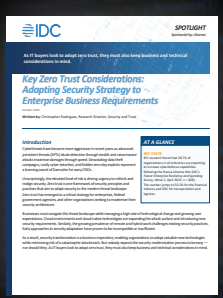
Verteidigungsmaßnahmen fokussieren

Prozentsatz der Befragten in der IDC-Umfrage von April 2022, die angeben, dass Netzwerksicherheit der Schwerpunkt in der Verbesserung ihrer Cybersicherheitsmaßnahmen ist

IDC-Bericht, gesponsert von Akamai, die wichtigsten Überlegungen zu Zero Trust: Anpassen der Sicherheitsstrategie an Unternehmensanforderungen, Dok.-Nr. US49728722, Oktober 2022

Vorteile von Zero Trust

- Bekämpft Ransomware
- Schützt hybride Belegschaften
- Unterstützt die Einhaltung von Compliance-Standards
- Sichert die Cloudmigration


IDC

SPOTLIGHT

Key Zero Trust Considerations: Adapting Security Strategy to Enterprise Business Requirements

Introduction

AT A GLANCE

Mehr Informationen finden Sie im von Akamai gesponserten IDC-Bericht: Überlegungen zu Zero Trust: Anpassen der Sicherheitsstrategie an Unternehmensanforderungen, Dok.-Nr. US49728722, Oktober 2022.

Nur auf Englisch verfügbar

Lesen Sie den IDC-Bericht

©2023 Akamai Technologies | Support | Veröffentlicht: 02/23