Key Considerations for Implementing Zero Trust

As cyberattacks have grown in both frequency and sophistication, organizations need to do all they can to strengthen their defenses. Implementing Zero Trust is a critical step, but businesses need to manage technological change and user expectations along their journey.

Every 2 seconds

Threats on the rise

Frequency that a business, consumer, or device is expected to face a ransomware attack by 2031

Cybersecurity Ventures Ransomware Market Report

31%

EMEA under attack

Percentage of ransomware victims from EMEA — the second highest region — from May 1, 2021 to April 30, 2022

Akamai Ransomware Threat Report H1 2022

41%

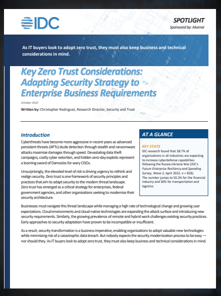
Focusing defenses

Percentage of respondents to IDC's April 2022 survey who identified network security as their main focus as they increase their cyberdefense capabilities

IDC Spotlight, sponsored by Akamai, Key Zero Trust Considerations: Adapting Security Strategy to Enterprise Business Requirements, doc #US49728722, October 2022

Zero Trust business benefits

- Combating ransomware
- Protecting a hybrid workforce
- Helping meet compliance standards
- Securing cloud migration



IDC

SPOTLIGHT

Sponsored by: Akamai

As IT buyers look to adopt zero trust, they must also keep business and technical considerations in mind.

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

October 2022

Written by: Christopher Rodriguez, Research Director, Security and Trust

Introduction

Cyberthreats have become more aggressive in recent years as advanced persistent threats (APTs) elude detection through stealth and ransomware attacks maximize damages through speed. Devastating data theft campaigns, costly cyber extortion, and hidden zero-day exploits represent a looming sword of Damocles for wary CISOs.

Unsurprisingly, the elevated level of risk is driving urgency to rethink and realign security. Zero trust is one framework of security principles and practices that aim to adapt security to the modern threat landscape. Zero trust has emerged as a critical strategy for enterprises, federal government agencies, and other organizations seeking to modernize their security architecture.

AT A GLANCE

KEY STATS

IDC research found that 38.7% of organizations in all industries are expecting to increase cyberdefense capabilities following the Russia-Ukraine War (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 3*, April 2022, n = 828). The number jumps to 50.2% for the financial industry and 50% for transportation and logistics.

Businesses must navigate this threat landscape while managing a high rate of technological change and growing user expectations. Cloud environments and cloud-native technologies are expanding the attack surface and introducing new security requirements. Similarly, the growing prevalence of remote and hybrid work challenges existing security practices. Early approaches to security adaptation have proven to be incompatible or insufficient.

As a result, security transformation is a business imperative, enabling organizations to adopt valuable new technologies while minimizing risk of a catastrophic data breach. But nobody expects the security modernization process to be easy — nor should they. As IT buyers look to adopt zero trust, they must also keep business and technical considerations in mind.

Read the IDC Spotlight, sponsored by Akamai: Key Zero Trust Considerations: Adapting Security Strategy to Enterprise Business Requirements, doc #US49728722, October 2022, for more.

Read the IDC Spotlight

©2023 Akamai Technologies | Support | Published 02/23