zscaler

The CISOs Report

What CISOs Have to Say

Prepared by CISOs Connect in conjunction with AimPoint Group and W2 Communications, The CISOs Report cuts through the headlines and hype of a hyperactive industry to reveal the greatest concerns of today's cybersecurity leaders, the biggest problems their teams face, and the priorities and plans they're putting in place to successfully defend their organizations.

A key finding: implementing a Zero Trust security model is top of mind for today's CISOs.

Today's risk level for cyber attacks: EXTREME

75%
hit by at least one cyber attack that caused material damage in the past 12 months

57%
hit by more than one cyber attack that caused material damage in the past 12 months

67%
perceive the threat landscape to be worse now, compared to one year ago

Cyber threats of greatest concern

- Ransomware
- Phishing/spear phishing
- Supply-chain attacks

Weaknesses and impacts concerning CISOs the most

Greatest vulnerabilities

#1
Third-party security weaknesses (i.e., connected partners)

#2
Unpatched software/systems

#3
Cloud security gaps

Consequences of a successful attack

#1
Exposure of PII/customer data

#2
Downtime for critical infrastructure / services

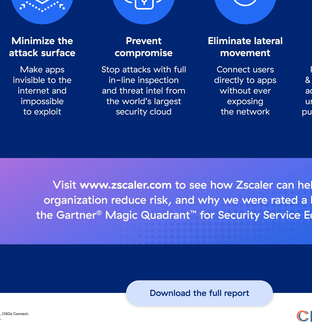
#3
Brand or reputational damage

External impacts concern today's CISOs the most, as the consequences of failures in these areas have the widest-ranging effects beyond an organization's own walls.

The preferred path forward

In response to an expanding attack surface and unrelenting threat landscape, an overwhelming majority of organizations are now pursuing a Zero Trust security model.

What's your organization's status with regard to a Zero Trust security model?



96.5%
Percentage of CISOs who are banking on a Zero Trust security model to improve their organization's security posture

Identity is the new perimeter

The redistribution of resources — apps, systems, and users — from primarily within the physical enterprise to without (think cloud and work-from-anywhere) has eroded the legacy network perimeter, rendering it ineffective as a trust boundary. One important outcome — and a key tenet of Zero Trust — is identity being anointed as the new perimeter. Changes CISOs are making to account for this new reality include:

- Investing in solutions to mitigate the risk of exposed credentials/ identity information
- Increasing inspection of user devices before granting access
- Investing in next-generation MFA that delivers a frictionless user experience
- Accelerating implementation of a Zero Trust security model

Top technology investments

Percentage of respondents planning to invest in each technology within the next 12 months:

63% network/ micro-segmentation

56% security service edge (SSE) platform

53% cloud-native application protection platform (CNAPP)

41% deception / active defense

How Zscaler can help

The Zscaler Zero Trust Exchange enables secure cloud transformation and protects your users, applications, and workloads no matter where they are. Powered by the world's largest security cloud, Zscaler stops threats using a four-tiered approach:

Minimize the attack surface
Make apps invisible to the internet and impossible to exploit

Prevent compromise
Stop attacks with full in-line inspection and threat intel from the world's largest security cloud

Eliminate lateral movement
Connect users directly to apps without ever exposing the network

Stop data loss
Prevent data theft & accidental exposure across managed and unmanaged devices, public cloud, and SaaS

Visit **www.zscaler.com** to see how Zscaler can help your organization reduce risk, and why we were rated a leader in the Gartner® Magic Quadrant™ for Security Service Edge (SSE).

Download the full report

CISOs CONNECT