Identity is the new perimeter

Top technology investments

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.

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).

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

Weaknesses and impacts concerning CISOs the most

The preferred path forward

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:

- Percentage of respondents planning to invest in each technology within the next 12 months:
  - Network/ micro-segmentation: 63%
  - Network security service edge (SSE) platform: 56%
  - Cloud-native application protection platform (CNAPP): 53%
  - Deception / active defense: 41%
  - Multi-factor authentication (MFA) and threat intelligence: 36%
  - Identity access management (IAM): 36%
  - Remote access: 34%

- Weaknesses and impacts concerning CISOs the most:
  - Third-party security weaknesses (i.e., connected partners): 67%
  - Unpatched software/systems: 57%
  - Cloud security gaps: 53%

- Consequences of a successful attack:
  - Exposure of PII/customer data: 67%
  - Downtime for critical infrastructure/services: 57%
  - Brand or reputational damage: 47%

- Today's risk level for cyber attacks: EXTREME

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.

The table shows the preferred path forward for CISOs.

- 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.

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:

- Percentage of respondents planning to invest in each technology within the next 12 months:
  - Network/ micro-segmentation: 63%
  - Network security service edge (SSE) platform: 56%
  - Cloud-native application protection platform (CNAPP): 53%
  - Deception / active defense: 41%
  - Multi-factor authentication (MFA) and threat intelligence: 36%
  - Identity access management (IAM): 36%
  - Remote access: 34%

- Weaknesses and impacts concerning CISOs the most:
  - Third-party security weaknesses (i.e., connected partners): 67%
  - Unpatched software/systems: 57%
  - Cloud security gaps: 53%

- Consequences of a successful attack:
  - Exposure of PII/customer data: 67%
  - Downtime for critical infrastructure/services: 57%
  - Brand or reputational damage: 47%

- Today's risk level for cyber attacks: EXTREME

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.

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:

- Percentage of respondents planning to invest in each technology within the next 12 months:
  - Network/ micro-segmentation: 63%
  - Network security service edge (SSE) platform: 56%
  - Cloud-native application protection platform (CNAPP): 53%
  - Deception / active defense: 41%
  - Multi-factor authentication (MFA) and threat intelligence: 36%
  - Identity access management (IAM): 36%
  - Remote access: 34%

- Weaknesses and impacts concerning CISOs the most:
  - Third-party security weaknesses (i.e., connected partners): 67%
  - Unpatched software/systems: 57%
  - Cloud security gaps: 53%

- Consequences of a successful attack:
  - Exposure of PII/customer data: 67%
  - Downtime for critical infrastructure/services: 57%
  - Brand or reputational damage: 47%

- Today's risk level for cyber attacks: EXTREME

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.

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:

- Percentage of respondents planning to invest in each technology within the next 12 months:
  - Network/ micro-segmentation: 63%
  - Network security service edge (SSE) platform: 56%
  - Cloud-native application protection platform (CNAPP): 53%
  - Deception / active defense: 41%
  - Multi-factor authentication (MFA) and threat intelligence: 36%
  - Identity access management (IAM): 36%
  - Remote access: 34%

- Weaknesses and impacts concerning CISOs the most:
  - Third-party security weaknesses (i.e., connected partners): 67%
  - Unpatched software/systems: 57%
  - Cloud security gaps: 53%

- Consequences of a successful attack:
  - Exposure of PII/customer data: 67%
  - Downtime for critical infrastructure/services: 57%
  - Brand or reputational damage: 47%

- Today's risk level for cyber attacks: EXTREME

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.

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:

- Percentage of respondents planning to invest in each technology within the next 12 months:
  - Network/ micro-segmentation: 63%
  - Network security service edge (SSE) platform: 56%
  - Cloud-native application protection platform (CNAPP): 53%
  - Deception / active defense: 41%
  - Multi-factor authentication (MFA) and threat intelligence: 36%
  - Identity access management (IAM): 36%
  - Remote access: 34%

- Weaknesses and impacts concerning CISOs the most:
  - Third-party security weaknesses (i.e., connected partners): 67%
  - Unpatched software/systems: 57%
  - Cloud security gaps: 53%