CiO Espresso
Fueling your digital transformation, one sip at a time
#34
2025

TOP 5 TRENDS *for CIOs*

What should CIOs adopt to secure network infrastructure?

Zero Trust Architecture (ZTA)

Zero trust, maximum effort
Tackle the complexity to secure your network

Secure every corner
of your network with clever controls

ZTA is a security model that assumes *zero trust* in users, devices, and applications, regardless of their location within or outside the corporate network perimeter. CIOs typically implement micro-segmentation, least privilege access controls, and continuous authentication to secure network traffic and prevent lateral movement of threats.

Bottom line: Sounds easy but implementing zero trust architecture can be complex and resource-intensive, requiring significant changes to existing infrastructure and continuous monitoring, while also potentially disrupting user experience with strict authentication and authorisation processes. Forrester cites that only about 27% of businesses deploy zero-trust architecture well on their first attempt.

Secure Access Service Edge (SASE)

Get SASE with it:
integrate SASE for a unified, cost-saving solution

No pain, no gain:
the wins are there if you are willing to work for them

Converged network security and wide-area networking into a cloud-delivered service, providing comprehensive security and networking capabilities as a unified solution.

Bottom line: Implementing SASE involves integrating various technologies like secure web gateways, cloud access security brokers, and zero trust network access into a unified solution. This can be complex and resource-intensive, requiring significant changes to existing network and security infrastructures. ZK Research's study found organisations deploying SASE reported 30% (avg) reduction in operational costs related to network security and management.

Software Defined Perimeter (SDP)

Secure and invisible:
SDP can micro-segment networks, enforce granular controls and minimise attack surfaces

Identity-based protection
that keeps unauthorised users at bay

A security framework that dynamically creates secure, micro-segmented network connections based on user identity and device posture — effectively hiding network resources from unauthorised users and devices. CIOs should deploy SDP solutions to enforce granular access controls, prevent lateral movement of threats and reduce the attack surface exposed to potential attackers.

Bottom line: Approximately 35% of companies actively deploy SDP solutions. Why so low: complexity and implementation costs, lack of awareness and understanding, integration with legacy systems and resource constraints.

> *After 30+ years of experience...*
> Network security has undergone radical changes, transitioning from perimeter-focused defences to dynamic, identity-based models like zero trust and SASE. This shift addresses the complexities of modern threats and distributed workforces, emphasising the need for continuous verification and adaptive access controls. As Alvin Toffler said, "The illiterate of the 21st century will not be those who cannot read and write, but those who cannot learn, unlearn — and relearn".

Threat Intelligence and Automation

Smart Security:
Leverage AI and threat intelligence for real-time threat detection and response

Stay Ahead:
Integrate machine learning and automation into your security controls for proactive defence

Leverage threat intelligence feeds, machine learning algorithms, and automation capabilities to proactively detect, analyse, and respond to security threats in real-time..

Bottom line: By integrating threat intelligence into network security controls such as firewalls, intrusion detection systems (IDS), and security information and event management (SIEM) platforms, mitigate your threats more effectively and efficiently. According to a study by the Ponemon Institute, organisations that leverage threat intelligence and automation can save an average of $2.8 million annually on security breaches.

Cloud Native Security Controls

Cut security incidents by 60%
use cloud-native IAM and encryption, but brace for integration challenges

Fortify with cloud security:
IAM and NSGs can slash breaches, though complexity with legacy system is likely to persist

This includes using native security features offered by cloud providers, such as identity and access management (IAM), encryption, network security groups (NSGs), and security monitoring and logging services, to strengthen the security posture of cloud deployments.

Bottom line: According to Gartner, utilising native security features, (like IAM, encryption, NSGs, and security monitoring and logging services) can reduce security incidents by up to 60%. However, organisations often face significant challenges when integrating cloud-native security controls with existing on-premises security frameworks. This is due to differences in security paradigms, tools, and processes between traditional on-premises environments and cloud infrastructures.

Like to delve into, dissect or draw on my experience over a coffee — let's set up a time... E L