portnox®

THE BUILDING BLOCKS OF ZERO TRUST

WHAT IS ZERO TRUST?

Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted.

Visibility, Automation, Orchestration

Zero Trust Security → Identity → Endpoints → Data → Apps → Infrastructure → Network
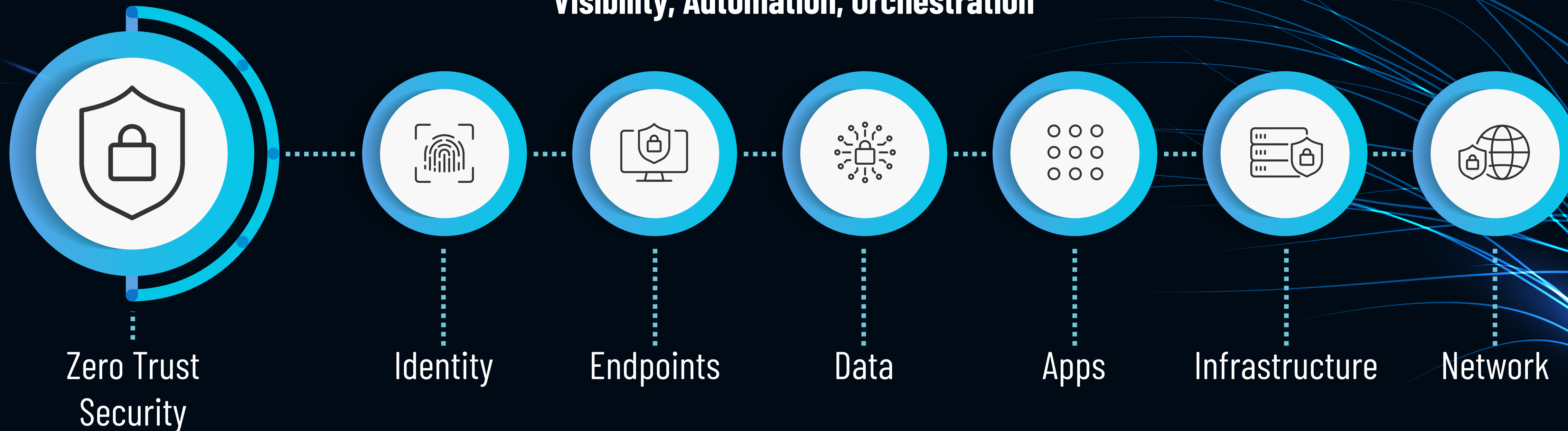
WHY ZERO TRUST? WHY NOW?

38%
A cyber-attack happens every 39 seconds.

50%
Nearly 50% of companies have experienced a data breach in the last year.

80%
Over 80% of all cyber-attacks involve credentials use or misuse in the network.

SECURITY TEAMS HAVE PRIORITIZED ZERO TRUST...

96%
96% of security decision-makers say zero trust is critical to organizational success.

$950K
Organizations with zero trust deployed reduced the average cost of a breach by $950,000.

60%
Cybersecurity & Identity are separate in nearly 60% of organizations

PRIMARY DRIVERS FOR ZERO TRUST ADOPTION

01. STOPPING NEW & MORE SOPHISTICATED ATTACKS

02. ACHIEVING HIGHER CYBERSECURITY EFFICACY

03. STRENGTHENING OVERALL PROTECTIONS

04. SAFEGUARDING DATA SOURCES

ZERO TRUST IMPLEMENTATION CHALLENGES REMAIN

ZERO TRUST COMPETES WITH OTHER SECURITY PROGRAMS

LEGACY TECHNOLOGIES CAN'T SUPPORT THE TRANSITION

VENDORS ARE MARKETING EVERYTHING AS ZERO TRUST

KEY TECHNOLOGIES FOR EFFECTIVE ZERO TRUST

ZTNA
ZERO TRUST NETWORK ACCESS

NAC
NETWORK ACCESS CONTROL

IAM
IDENTITY ACCESS MANAGEMENT

TECHNICAL CONSIDERATIONS FOR ZERO TRUST

UNIFIED
Saves time, simplifies deployment & reduces cost.
Fortify networks & infrastructure with zero trust access control and security.

FRICTION-LESS
No architectural re-engineering required.
Seamlessly deploy, scale, and manage without no on-premises hardware.

CLOUD-NATIVE
Nothing on-prem = less maintenance
Seamlessly deploy, scale, and manage without no on-premises hardware.