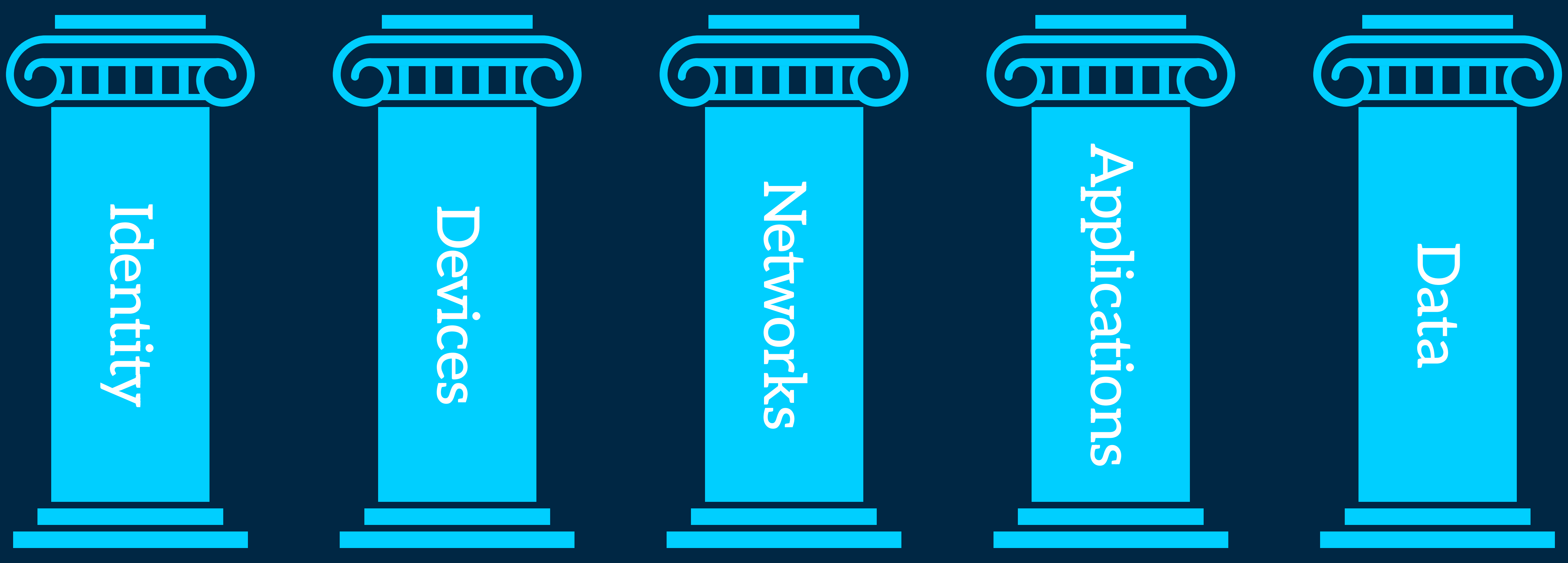
BROADCOM®

Zero Trust Architecture (ZTA) Essentials

Zero trust architecture (ZTA) transforms cybersecurity by assuming no user, device, or network is inherently trustworthy. Instead of relying on static defenses, ZTA continuously verifies identities, devices, and context to grant least-privilege access.

Zero trust (ZT) rejects implicit trust, embraces the presumption of compromise, and focuses on protecting data across five key pillars:



Identity

Devices

Networks

Applications

Data

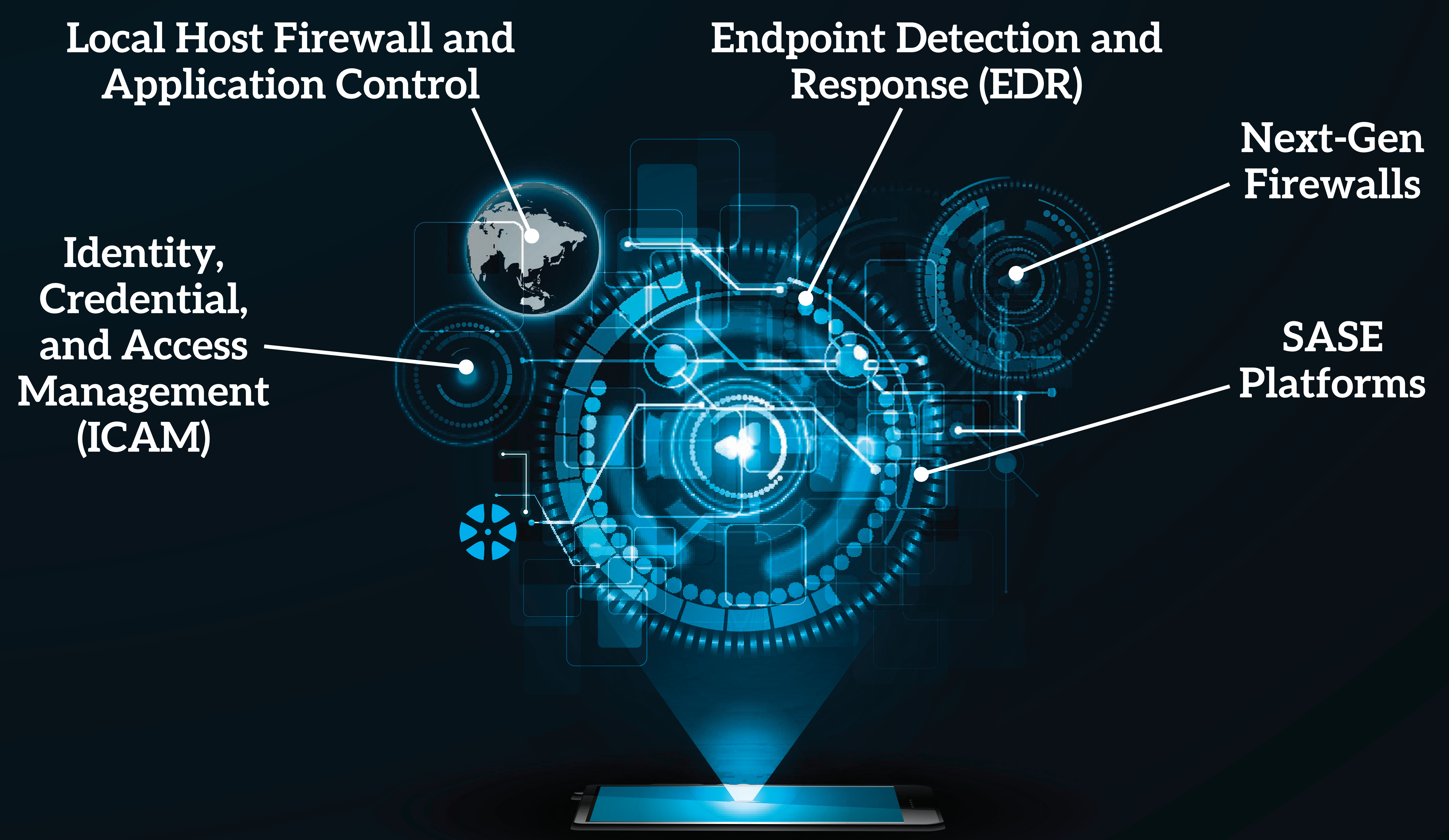
Every access request is evaluated based on a zero trust agent combining real-time attributes like:

- Device health
- User behavior
- Location

To implement ZTA, organizations must:

- Enforce dynamic, context-aware access controls
- Segment networks and workloads to limit lateral movement
- Continuously monitor and inspect traffic, users, and endpoints
- Automate security response using SOAR and SIEM
- Align ZT efforts with compliance and governance goals

Enabling technologies include:



Local Host Firewall and Application Control

Endpoint Detection and Response (EDR)

Next-Gen Firewalls

Identity, Credential, and Access Management (ICAM)

SASE Platforms

ZTA isn't a one-time deployment—it's a security mindset. Start small (e.g., secure one app with ZTNA), integrate with existing change processes, and mature capabilities over time. As threats grow more sophisticated, ZTA provides a resilient, scalable approach to securing modern, distributed environments.

BROADCOM®

SANS | Research Program