Zscaler Zero Trust Exchange at a Glance

Platform Benefits:

SECURITY
Reduce cyber risk and prevent data breaches through a modern architecture built on least–privileged access.

SIMPLIFICATION
Eliminate cost and complexity by retiring legacy infrastructure and point products like firewalls and VPNs.

TRANSFORMATION
Increase organizational agility by securely enabling digital transformation and accelerating productivity.

The cloud and mobility are empowering digital transformation—making organizations more agile and competitive. SaaS apps like Microsoft 365 and cloud platforms like AWS are now the default. Today's hybrid workforce means that users accessing these services may be doing so from any location. The network perimeter has effectively inverted, with more work being done outside of it than within it. These changes pose challenges for traditional, network–centric IT architectures.

Hub–and–spoke networks and castle–and–moat security models are no longer fit for purpose. Endlessly extending the network to more and more users, devices, clouds, and locations increases complexity, cost, and risk, and so does trying to build a security perimeter around this ever–expanding network with tools like firewalls and VPNs. As such, today's cloud and mobile world requires a new architecture with a modern approach to networking and security.

Zscaler delivers zero trust architecture as a service and at the edge from the Zero Trust Exchange, the world's largest security platform. This cloud comprises more than 160 global data centers and processes more than 500 billion transactions per day. The platform acts as an intelligent switchboard that provides secure any–to–any connectivity based on context and risk. Rather than extending network access, Zscaler delivers secure, direct–to–app access to users, workloads, IoT/OT, and B2B partners—anywhere. In other words, it decouples security and connectivity from the network.
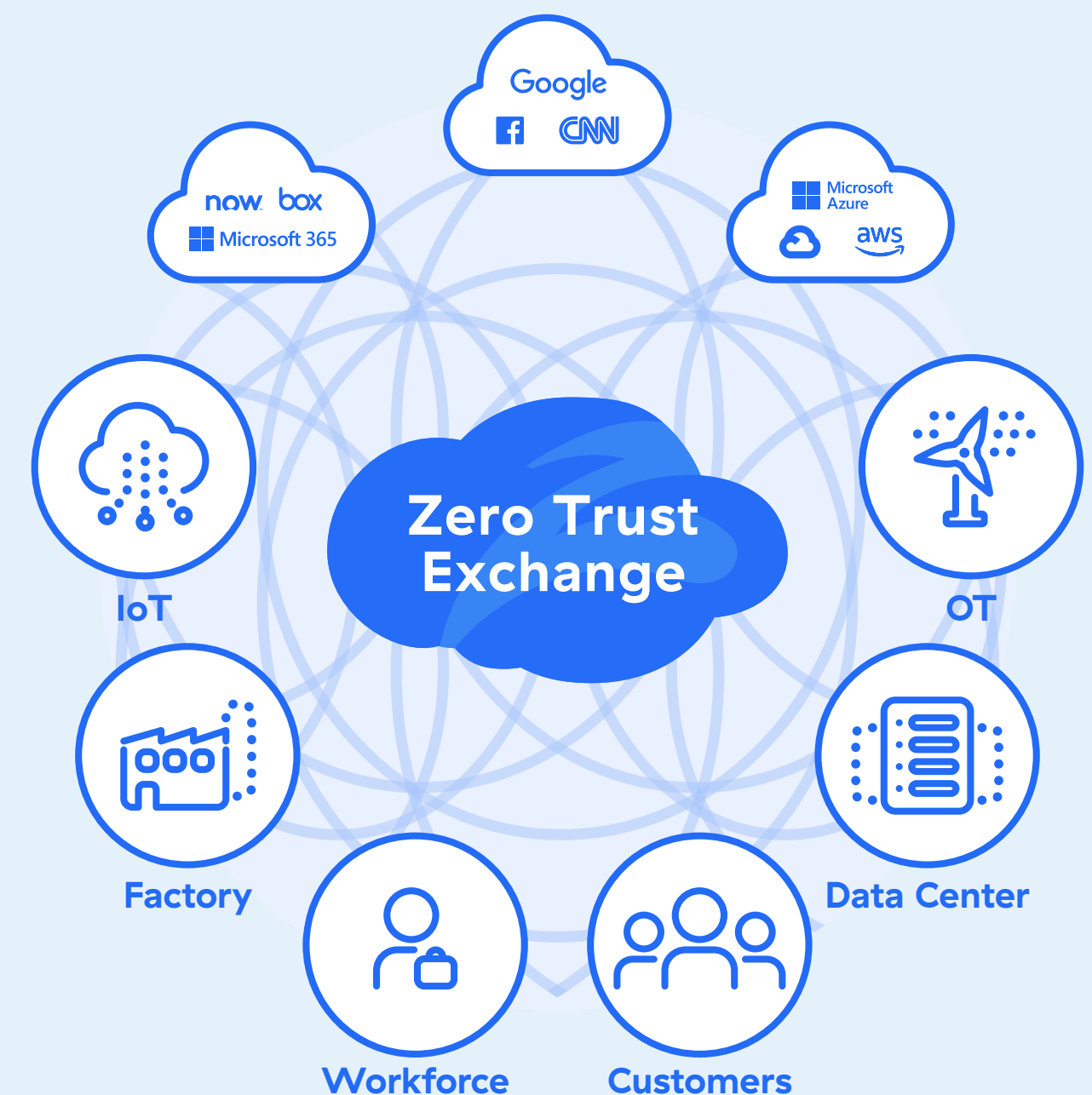
Zero Trust Exchange Key Capabilities

MINIMIZES THE ATTACK SURFACE
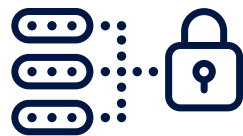Eliminates public IPs and hides apps behind the Zero Trust Exchange—adversaries can't attack what they can't see

STOPS COMPROMISE
Inspects all traffic at scale (even TLS/SSL traffic) and stops threats with real–time security policies

PREVENTS LATERAL THREAT MOVEMENT
Connects users directly to apps, not the network, so threats can't access network–connected resources

BLOCKS DATA LOSS
Finds, classifies, and protects sensitive information across all potential data leakage channels

SECURES WORK-FROM-ANYWHERE
Lets employees safely and seamlessly work from anywhere via secure, edge–delivered connectivity—without the need for VPN

ENSURES A GREAT USER EXPERIENCE
Provides built–in digital experience monitoring and optimizes direct–to–app connections that eliminate traffic backhauling

SIMPLIFIES BRANCH LOCATIONS AND SECURES IOT/OT
Forgoes the need for VPN and MPLS through secure connections that use the internet as the corporate network

SECURES CLOUD CONNECTIVITY
Grants workloads zero trust access to one another and the web, eliminating network–based connectivity and lateral movement

ENABLES THIRD-PARTY APP ACCESS
Extends least–privileged app access to B2B partners, like suppliers, to keep third parties off your network

To learn more about the Zscaler Zero Trust Exchange, visit zscaler.com/products/zero-trust-exchange.

Zero Trust Everywhere