KPMG and Zscaler—Zero Trust architecture

Helping create a secure, scalable, and future-ready zero trust architecture that empowers digital transformation with confidence

Traditional VPN-based security models no longer provide sufficient protection against the new era of cyber threats. These legacy models rely on the outdated assumption that everything within the network is inherently safe. However, once attackers penetrate the perimeter, they can move laterally across systems and compromise critical assets. Weaknesses like these lead to costly data breaches, business disruptions, reputational damage, and regulatory penalties for noncompliance.

Today, cloud adoption, remote work, and mobile-first operations are dissolving the traditional network perimeter even further. Data and applications now reside everywhere—across software-as-a-service (SaaS) platforms, private data centers, and public clouds—creating an ever-expanding attack surface.

Zero Trust Architecture

To address these challenges, organizations must adopt a Zero Trust Architecture (ZTA) that replaces implicit trust with continuous verification. By authenticating every user, device, and application based on real-time context, Zero Trust enforces least-privilege access and drastically reduces opportunities for unauthorized activity. This eliminates the need for traditional VPNs, reduces attack surfaces, and improves user experience.

Why Zero Trust matters

Zscaler's cloud-native Zero Trust Exchange (ZTE) architecture delivers real-time monitoring, segmentation, and policy-based access controls to secure complex environments. Powered by AI, the ZTE supports scalability, agility, and low latency across all global environments.

- In environments where agents cannot be deployed (legacy operating technology [OT] systems, specialized factory equipment), organizations can utilize Zscaler to help establish secure, policy-driven communication channels among office locations, data centers, and industrial sites.

Zscaler's Zero Trust Exchange capabilities

- **Secure access to private applications:** Provides identity-based access to internal applications without exposing them to the internet. Users are connected directly to applications based on their identity and device posture, minimizing lateral movement and reducing the risk of network-based attacks.
- **Secure internet and SaaS access:** Helps protects users from threats through inline inspection, SSL decryption, and advanced threat prevention. The ZTE ensures data protection through Data Loss Prevention (DLP), Cloud Access Security Broker (CASB), and sandboxing capabilities, enabling secure use of SaaS and web applications.
- **Digital experience monitoring:** Offers broad visibility, helping IT teams identify and resolve performance issues ensuring consistent, secure, and reliable access for users.
- **Data protection and cloud security:** The ZTE leverages DLP, CASB, and Cloud Security Posture Management (CSPM) capabilities into a unified platform, a holistic approach that safeguards sensitive information across cloud environments and helps to safegurad and support compliance compliance.
- **Zero Trust connectivity for workloads and IoT:** Extends Zero Trust principles to cloud workloads and IoT/OT environments, enabling secure application-to-application communication without exposing networks or IP addresses.
- **Global cloud platform:** With over 160 data centers worldwide, Zscaler delivers low-latency, high-availability access, supporting scalability and resilience for enterprises of any varying size.

The KPMG advantage

KPMG offers strategic consulting, implementation services, and governance frameworks to help organizations integrate Zscaler into broader security programs and build operational resilience:

- **Zero Trust strategy and roadmap development:** KPMG helps organizations define their Zero Trust vision, assess current-state maturity, and design a phased roadmap aligned with strategic business outcomes, compliance mandates, and industry frameworks such as NIST 800-207.
- **Architecture design and technology enablement:** KPMG collaborates with Zscaler to design and implement scalable Zero Trust solutions that integrate identity, network, application, and data security controls across hybrid and multicloud environments.
- **Governance, risk, and compliance integration:** KPMG establishes governance frameworks to help ensure policy consistency, continuous monitoring, and adherence to regulatory standards such as HIPAA, PCI-DSS, and GDPR, while embedding Zero Trust controls into enterprise risk management processes.
- **Change management and adoption support:** KPMG drives stakeholder engagement, workforce enablement, and process redesign to help ensure that Zero Trust adoption is smooth, measurable, and sustainable across business and IT teams.
- **Ongoing assessment and optimization:** By leveraging analytics and performance metrics, KPMG continuously evaluates Zero Trust maturity, identifies gaps, and refines controls to adapt to evolving threats and business needs.

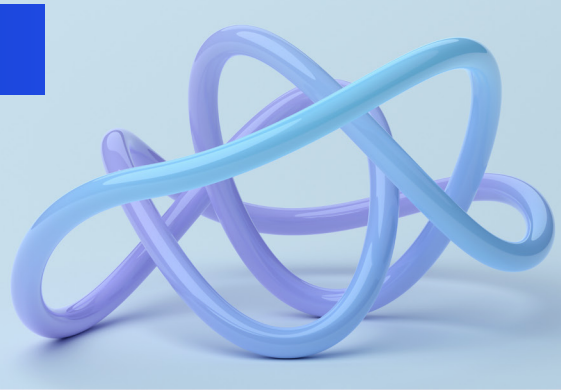
How KPMG implements Zero Trust with Zscaler

The KPMG approach builds upon a thorough Zero Trust methodology, offering a tailored, phased roadmap designed to integrate Zscaler's core capabilities into your enterprise environment:

- **Discovery and assessment:** Experienced cybersecurity consultants conduct workshops to understand your unique business objectives, existing application landscape, critical data, and user workflows.
- **Policy design and architecture development:** KPMG defines granular, context-aware access policies to align with your security posture, regulatory compliance, and business requirements.
- **Pilot deployment:** KPMG performs detailed testing of the Zscaler architecture thoroughly. A chosen group of users and applications are leveraged to evaluate performance, assess, and refine policies while collecting feedback in a low-risk setting.
- **Enterprise-wide rollout:** Upon successful deployment, KPMG guides organizations in deploying Zscaler's solution across the defined production application landscape. KPMG provides migration planning and project management, and leads adoption strategies to help ensure a seamless transition.
- **Continuous governance and monitoring:** Beyond initial deployment, KPMG continuously refines policies, monitors access logs, and adapts to the ever-evolving threat landscape.

Gain Zero Trust

By leveraging Zscaler's advanced Zero Trust capabilities, organizations can strengthen their security posture and reduce the inherent vulnerabilities. of traditional, perimeter-based models. Zscaler's cloud-native platform provides the foundation for secure, identity-driven access that protects users, applications, and data—anywhere, on any device.



Contact us

Sai Gadia
Partner, KPMG LLP
E: sgadia@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**