KPMG

Assume nothing, verify everything

Why zero trust is the way forward.

Organizations worldwide continue to grapple with cyber security challenges as the pace of digital transformation, fast evolving business models, remote work and increasingly complex partner ecosystems unleash new opportunities for cyber attacks.

Traditional cyber security approaches relying on security 'at the perimeter' were adequate in a world where data and its users resided within specific, well-defined locations. With physical boundaries disappearing — and with increasingly sophisticated cyber criminals using ransomware and other destructive malware to target organizations — conventional cyber security approaches are being rendered obsolete, ultimately driving the need for modern solutions to protect critical assets and information.

More and more businesses are wisely turning to a zero trust mindset to restructure their cyber defenses.

What is zero trust?

A zero trust approach puts user identity, access management and data at the heart of cyber security. It is an evolutionary cyber security approach and model that has been developing in response to the ever-expanding threat landscape. Zero trust is not a technology solution but a model and approach that requires a mindset shift based on three key principles: *Assume nothing, check everything and limit access.*

Zero trust relies on an identity-aware, context-driven and data-centric approach to cyber security strategy and operations. With user identity and data value as its key component, zero trust enables secure access to data and resources via strong identity management, modern software defined networks, continuous monitoring and advanced analytics.

No one either inside or outside the enterprise network is automatically trusted — every user must prove their identity to gain access. Within the zero trust framework, even with a valid username and password credentials, users are denied access to the system if their device has not been validated or the required trust level is not met.

Zero trust is different from previous approaches to IT security. Today's hyperconnected world has broken down traditional perimeters — enabling the fluid movement of data beyond organizational boundaries as multiple parties and devices access business data and systems from anywhere in the world. Add to this dynamic environment 5G technology, edge computing and hundreds of millions of emerging IoT devices and it becomes clear that conventional security approaches are fast becoming outdated and increasingly inadequate.

Businesses are waking up to a new reality of threats

While many businesses may not realize just how exposed they are to today's cyber threats, an increasing number are showing a new sense of urgency in adopting a zero trust model.

By 2025, damages resulting from global cybercrimes are expected to reach close to US$1 trillion annually.[1] Primary drivers prompting more businesses to wisely pursue the zero trust model for enhanced security include ongoing digital transformation that is revolutionizing business models and workforces, the proliferation of cloud-based services, and today's increasingly complex supply chain networks.

[1] "The Hidden Costs of Cybercrime," The Center for Strategic and International Studies. (December 9, 2020)

Objectives, considerations and trends

Also accelerating adoption is geopolitical instability — including the ongoing conflict between Russia and Ukraine. As the geopolitical landscape continues to evolve, and tensions increase, organizations may be required to implement stronger, yet more flexible access controls should the need arise where a quick disassociation is required. Such instability could also further exacerbate supply chain disruptions, with organizations being required to change suppliers at short notice. All of this points towards a more flexible and adaptive model such as zero trust. And also, not to be underestimated is the impact of Section 3 of the 12 May 2021 US executive order[2] requiring the federal government and associated agencies to adopt a zero trust architecture.

As the pursuit of the zero trust framework gains momentum, it is crucial that CISOs and CIOs work towards implementing organization-wide zero trust architectures that align with their operating priorities, risk management needs and technology capabilities.

In the race to better understand and manage today's ongoing cyber threats, zero trust puts businesses in a predictive and proactive mode, providing timely context-based analysis, insights and automated responses to potential attacks. With a zero trust approach, companies build an end-to-end cyber security approach that is 'perimeter-less' — providing protection for every aspect of the ecosystem, including assets, workloads and other resources.

A key requirement for zero trust is that the enterprise consistently collects, inspects and analyzes traffic across its entire ecosystem, ensuring maximum real-time visibility into both the data that users can access and the potential for malicious activity.

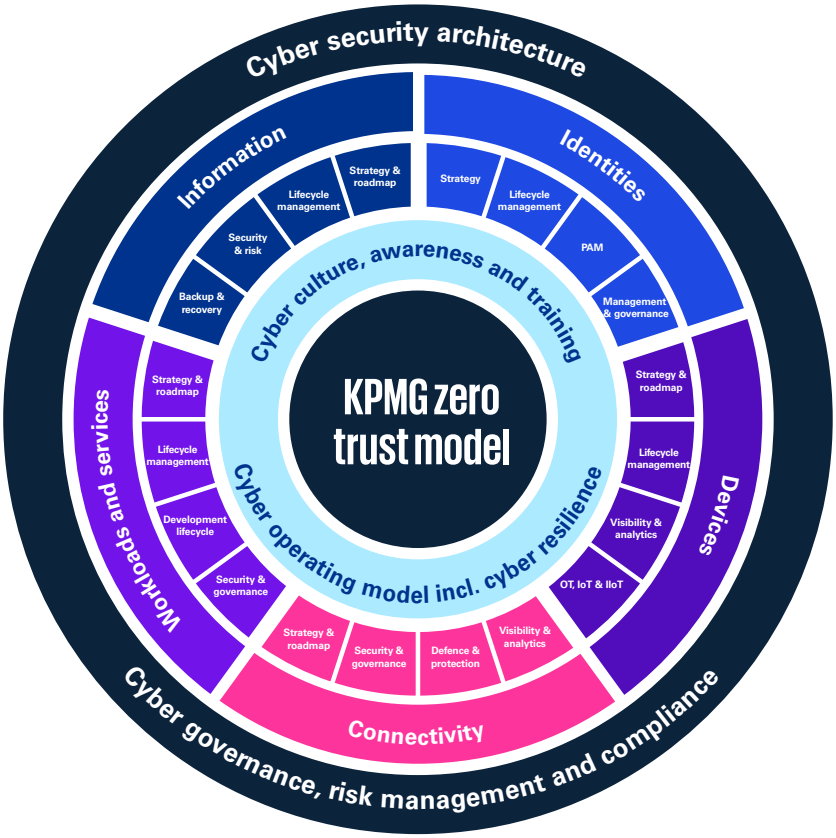
In addition to zero trust, businesses are looking to bolster security using the Secure Access Service Edge (SASE) approach, minimizing complexity among remote users by replacing data centers with internet-first network security, rather than relying on traditional technologies such as Multi-Protocol Label Switching (MPLS). Similar to zero trust, SASE aims to maximize cyber security via a layered and unified system of security measures and a software-defined network on traditional network infrastructure. Zero trust and SASE can work together to significantly enhance an organization's cyber security posture and more businesses are taking this approach.

Zero trust is a journey that continues to evolve

Make no mistake — organizations can no longer simply trust user identities, devices, workloads, networks or data. Zero trust is about knowing where your data is and controlling access to it via strong identity management, advanced analytics and a device inventory. KPMG's zero trust model anchored in NIST 800–207 (Zero Trust architecture — 5 pillars) provides an enterprise-wide focus on each client organization's unique cyber security capabilities and needs related to architecture, risk awareness and management, governance and compliance. Having it implemented helps organizations to be better positioned to detect unusual behavior and prevent communication with unauthorized apps, servers and accounts.

[2] "Executive Order 14028, Improving the Nation's Cybersecurity", NIST. (November 8, 2021)

KPMG zero trust model



As noted earlier, zero trust is an idea, not a technology, feature or standard. It's an identity-based approach to security — one requiring a mindset shift away from traditional cyber security models.

As CISOs address the evolving cyber-threat landscape, the KPMG model highlights the need to balance many responsibilities, formally and informally. This means shifting from enforcer to influencer, fostering security awareness and building vital relationships with peers. Indeed, learning how to deal in 'gray' areas rather than black and white may be one of the key learnings, shifting from a world of absolutes to one where outcomes are less certain, with risk avoidance and containment as the prime objective.

KPMG professionals take clients on a comprehensive and structured journey (illustrated below) in order to understand zero trust, align business objectives with cyber security outcomes, assess the current uplift required to deliver these outcomes, and develop strategic roadmaps with programs for successful implementation.

Zero trust journey

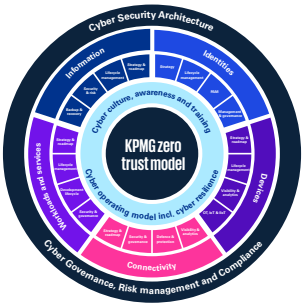
The future is identity-aware and data-centric

The zero trust approach to security is the latest crucial step in an evolutionary journey. Our goal at KPMG is to help organizations take the concept of zero trust and make it a reality by defining a strategic roadmap, an implementation plan and continually building on zero trust's capabilities, strengths and advantages — ultimately pursuing an identity-aware and data-centric approach to cyber security.

Zero trust is the right approach at this point in time — but what's next as the threat landscape continues to be uncertain?

Thinking ahead, KPMG has developed the next evolution of the cyber security model — Adaptive Security, which crystalizes the potential benefits of zero trust capabilities by grouping them using the National Institute of Standards and Technology's Cyber Security Framework Functions — delivering deeper context through end-to-end visualization of threats, leveraging key automation and orchestration capabilities to auto-remediate vulnerabilities and protect assets.

KPMG's adaptive cyber model



Adaptive security functions

Identify and assess

Once a threat has been identified, zero trust provides context for an organization to enforce the right controls.

Protect and defend

Implementing zero trust enables organizations to build an adaptive defensive capability to address threats.

Detect and contain

Using zero trust solutions allows enterprises to automate the containment of threats more effectively.

Respond and remediate

Properly configured zero trust solutions allow enterprise to automate and orchestrate remediation activities.

Recover and transform

Using zero trust principles allows organization to re-build their capabilities while accelerating the adoption of cloud services.

The combination also allows CISOs to use a threat-led and risk-based approach to identify and prioritize investments and improve their return on security investment, rather than using a siloed cyber security capability approach which is not as effective.

For more information, contact:

Manuel Kanagasuntherie
Senior Manager, Cyber Security Services
KPMG in the UK

E: manuel.kanagasuntherie@kpmg.co.uk

Deepak Mathur
Managing Director, Cyber Security Services
KPMG in the US

E: deepakmathur@kpmg.com

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

home.kpmg/socialmedia

Designed by Evalueserve.
Publication name: Assume nothing, verify everything | Publication number: 138258-G | Publication date: August 2022