KPMG

From zero to hero

How to operationalize and accelerate a ‘zero trust’ model

Risk is on the rise

Transformation initiatives create exciting opportunities, not only for your business but also bad actors. Can you grow with confidence, despite expanded cyber threats that put operations, profits and reputation at risk? Can you mitigate threats in a way that enables rapid launches and protects the business at the same time?

In the dynamic digital landscape, this is the call to action for cybersecurity, but many departments are stuck in static, reactive postures that can't keep up with fast-evolving risks or business needs.

That's due to the growing proliferation of tech in on-premises, cloud and hybrid environments—not to mention cyber talent shortages, changing regulations, and remote working. Many cyber teams simply lack the centralized ability to enforce security across the vast estate of users, devices and data.

77% expect cyber risk to increase in the next 12 months.

Source: KPMG 2022 Fraud Outlook, KPMG International, 2022.

58% of cybersecurity teams are behind schedule

Source: KPMG Global Tech Report, KPMG International, 2022 (survey of more than 2,200 tech executives)

83% of executives in the Americas reported a cyber-attack in the previous 12 months.

Source: KPMG 2022 Fraud Outlook, KPMG International, 2022.

A new model for rising risk

Since companies can no longer rely on a perimeter-based security model for network access, most are pursuing a zero-trust approach, verifying users (and devices) based on who they are instead of where they are.

But like many companies, you're probably struggling to operationalize it at an enterprise level.

After all, zero trust is not a one-and-done initiative, nor is it a discrete security policy. It is a way of thinking—a journey for continually monitoring and improving your security posture. Using dynamic signals of information, it calls for you to proactively evaluate every transaction and interaction, detect threats and stay ready for whatever comes next.

Given the ongoing nature of zero trust, **forward-looking companies are making managed services part of their playbook.** They're working with providers who bring a comprehensive solution—from consulting on zero-trust strategy to implementation, ongoing enforcement, continuous monitoring and evolution.

Four layers of zero trust

The starting point for the journey is to consider the opportunity. Does your current security posture enable or inhibit your business?

The answer to that question will inform your goals, along with how to define the zero-trust model, operationalize it, enforce it across the enterprise, and continually update it to meet changing needs.

If you're like many organizations, you may struggle to achieve the proper balance of security and access. Undoubtedly, for instance, the principle of least privilege is easier said than done when business units tend to believe that all data is critical and everyone needs access.

It's even more challenging in DevOps environments, when the prevailing focus is on speed to market, not management of risk.

Cyber-attacks are a key global risk of 2023

But only about

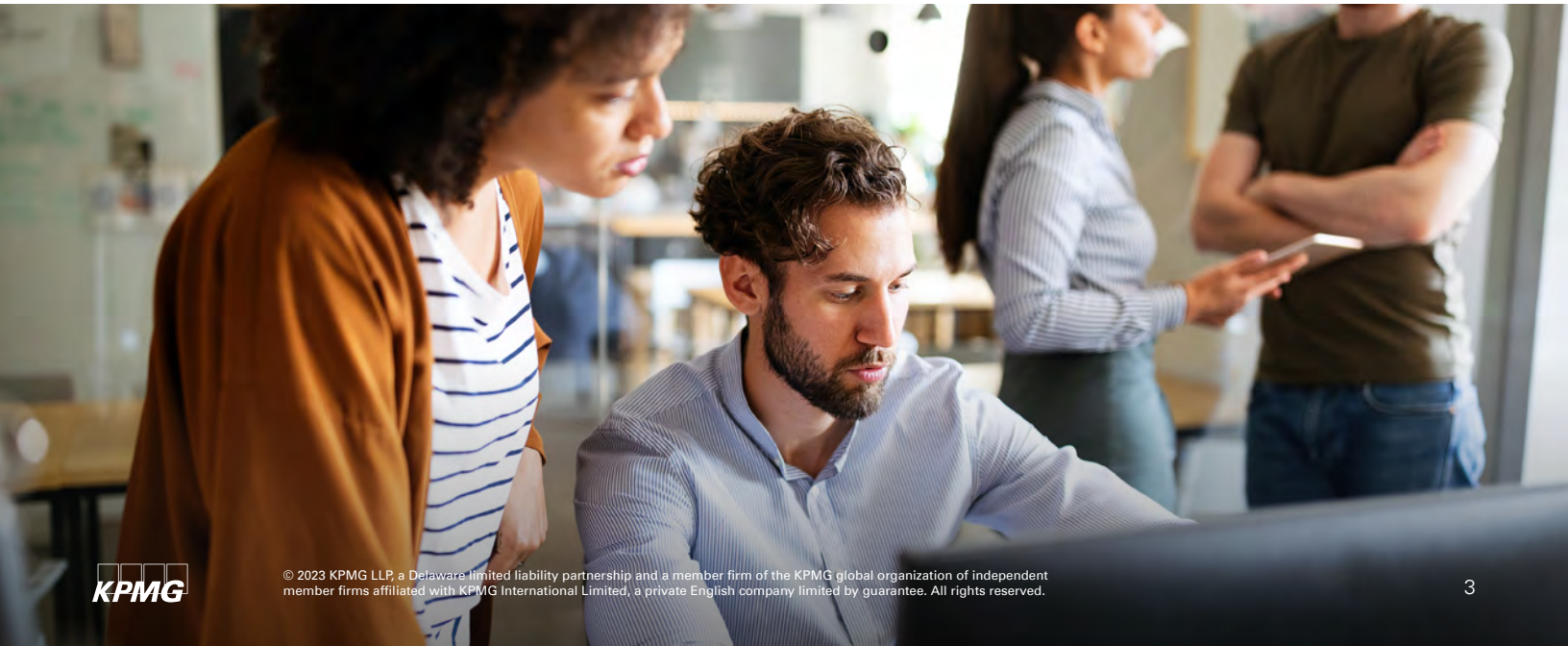
30% of risk officers say current risk management activities are effective.

Source: World Economic Forum, The Global Risks Report 2023, 18th Edition

To help,

80% of companies plan to **increase their use of managed services** for cybersecurity over the next two years.

Source: KPMG and HFS Managed Services Outlook, a global survey of 800 executives, 2022



To explore opportunities, consider what zero trust could look like in four critical layers of cybersecurity:

01 Data protection

Technology ecosystems are now centered around cloud and data, so an effective security operations center (SOC) must understand the different kinds of data in the enterprise—including which data is required for mission-critical processes, the location, and the level of sensitivity. Only then can the SOC determine who should have access and when.

Indeed, data governance and cyber risk have become so important that they are top issues on the 2023 board agenda.

Source: On the 2023 Board Agenda, KPMG Board Leadership Center, December 2022

02 Identity access management (IAM)

Any zero-trust model requires a centralized, well-managed identity ecosystem, enabling you to establish correct digital identities and revoke them as relationships change. Authentication systems should be dynamic, challenging users as appropriate in each interaction or transaction, and policies must be consistently enforced.

Consider factors such as cloud directories; the process for joining, leaving or relocating within the organization; and the management of service accounts and access privileges. Do your current policies meet the needs of the business? Can you nimbly onboard new technology to your IAM systems? Can you quickly adjust to meet changing requirements for mergers, acquisitions, or regulatory compliance?

03 Threat detection and response

To move from reactive to adaptive security, a SOC must understand normal patterns of behavior and be able to detect anomalies, while also proactively hunting for threats.

Have you prioritized the threats to your business resiliency so you can manage them accordingly? Are you aware of the enterprise security posture at all times? Do you have a unified view of the threat landscape across users, devices and applications?

Many organizations struggle to rationalize signals and controls across disparate dashboards and teams, but leading SOCs have a single-pane view. That means full threat visibility and one source of cybersecurity truth—for faster detection, containment and response that help the company manage through disruptive events.

04 Application security

Threat detection and IAM are critical, but another key consideration is where enterprise data lives: the applications. That's why it's essential not only to embed security into development—but also to continually test applications for vulnerabilities, viewing the process through a zero-trust lens. With the right approach to application security, you can help your company get products to market faster and more securely.

For example, the most effective cybersecurity organizations conduct ongoing penetration testing of web apps, mobile apps and application programming interfaces. They also perform manual or automated code review while apps are being built, as well as runtime scans afterward. In addition to connecting apps to authentication systems, they continually test the access controls, to help ensure that the right users have the right access to the right data.

A closer look

Stay tuned for additional articles about zero TRUST in each of the four layers of cybersecurity.

Ongoing execution for long-term outcomes

These four interconnected layers are the underpinnings for a zero-trust model. To put them into action, progressive organizations start with a strategy for "perimeter-less" defense—including fundamental decisions around enterprise risk, key principles and objectives—followed by a roadmap for transforming processes and deploying new technology.

However, amid constantly changing security threats and business priorities, setting up the model is not enough. Zero trust also requires ongoing execution across all four layers—including continual monitoring, detecting, testing and authenticating to stay ahead of risks.

That's why companies are increasingly seeking providers who deliver a comprehensive solution for zero trust: strategy, implementation, and ongoing managed services.

Managed services, typically delivered remotely in a multi-year subscription, combine human domain expertise and advanced technology to take responsibility for ongoing cybersecurity processes. Leading providers offer predictable costs, the option to flex up or down to meet fast-changing needs, and meaningful outcomes.

Already, nearly **40%** of companies are using managed cybersecurity services at scale across the enterprise...

...and another **29%** are using managed cybersecurity for a business function.

In the next two years, companies expect cybersecurity to deliver more value than any other managed service.

Source: KPMG and HFS Managed Services Outlook, a global survey of more than 1,000 executives, 2023-2024

For example, savvy managed services can enable the business to:

Operate at the speed of business

With the right managed cybersecurity provider, you don't have to trade-off between high security and agile development. Instead, you can achieve both by embedding 24/7 monitoring, testing and other activities into the heart of your processes, turning your SOC into an accelerator of transformation initiatives—not an inhibitor.

Look for providers who help reduce adversary dwell time through an outcome-driven model, supported by operational metrics such as time to provision a user account, quantifying impact of vulnerabilities, mean time to detection, mean time to remediation, and incident response time.

Operate even faster than the speed of business—by proactively getting ahead of issues

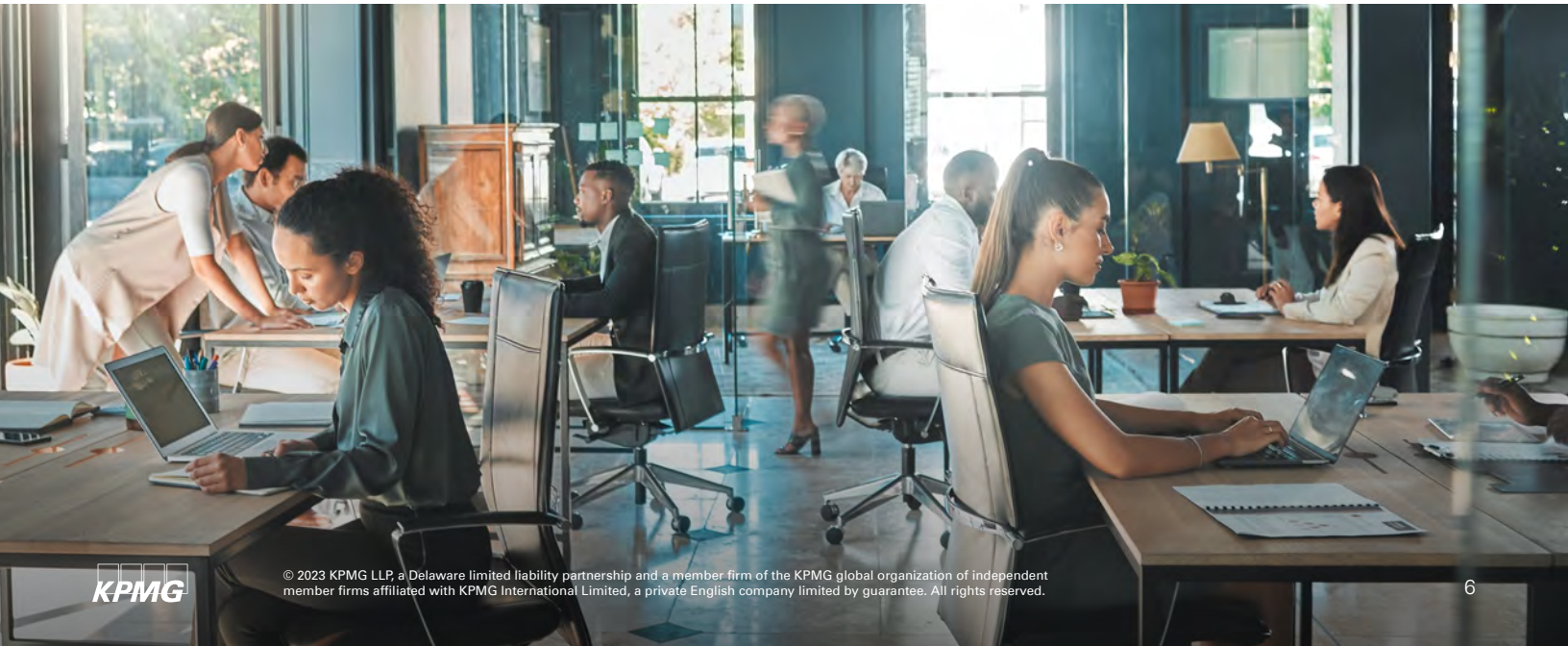
Leading providers harness artificial intelligence, machine learning and behavior analytics to bring predictive, actionable insights on emerging threats. With early warning on potential breaches, vulnerabilities in app development or other violations of your security policies, you can proactively mitigate threats before they become problems.

For even more value, consider providers who not only bring insights but can also contextualize those insights to your business priorities, industry and stakeholders—from the boardroom to the back office.

Enable your company's long-term ambitions

Leading managed security providers don't just step in for the "run phase" after a strategy project. They are also strategic partners at the outset of transformation initiatives, helping you design new operating models across all four layers of defense—and continually execute them through day-to-day tuning, retuning, and reevaluation of risks.

By taking advantage of providers' scale, talent and capabilities, you can keep up with the fast-changing technology, threats and regulations of today, while building enterprise resilience for tomorrow.



Lasting value

In the age of sustained digital transformation, almost every business decision is partly a cybersecurity decision. That, along with ever-changing threats, is making zero trust an increasingly critical consideration. The model can improve detection, protect data, reduce risk, enforce security policies, accelerate processes and ultimately enable the business to succeed.

But it's far from a set-and-forget endeavor. As the digital terrain continues to evolve, so must the zero-trust model, and leading managed security providers are in prime position to help.

About KPMG Managed Services

Business transformation is the path to sustained advantage. But transformation is not a fixed destination; it's an ongoing journey. How can you continually evolve your business functions to keep up with ever-changing targets?

KPMG Managed Services can help.

We combine advanced technology with functional and sector expertise to handle knowledge-intensive processes across your enterprise—on a subscription, as-a-service basis. In addition to reducing your costs, we drive outcomes like resilience, customer retention, stakeholder trust, and competitive advantage. We help you operationalize your growth ambition, so you can accelerate your transformation journey while minimizing disruption and risk.

Learn more about KPMG Managed Services for cybersecurity

Learn about other parts of the KPMG Managed Services portfolio

About KPMG Cyber Security Services

KPMG helps you create a resilient and trusted digital world—even in the face of evolving threats. We bring a combination of technological expertise, deep business knowledge, and creative professionals who are passionate about protecting and building your business. Together, we can create a trusted digital world so you can push the limits of what's possible.

Learn more about KPMG Cyber Security Services

Contact us

Rajesh Ahuja, CISSP
Managing Director, KPMG LLP
Cyber Managed Services
rajeshahuja@kpmg.com

Evan Rowell
Director, KPMG LLP
Cyber Managed Services
erowell@kpmg.com

Antonio Manelli
Lead Specialist, KPMG LLP
Cyber Managed Services
amanelli@kpmg.com

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

kpmg.com/socialmedia