KPMG

SOC leaders: Adopt a Zero Trust mindset to secure external—and internal—network threats

Transformation assumes security can adapt with demand

The dynamic nature of workloads, services, and collaboration requires connectivity, visibility, and automation to secure an ever-changing perimeter and threat landscape. There is an expectation that security technology can adapt as quickly as business needs require. However, the reality is tools and process often prohibit initiatives.

Traditional perimeter-based security approaches no longer effectively protect new, widely distributed, cloud-based environments. No one can be trusted by default, even those already inside the network perimeter. In an era where trust must be earned and not bestowed, Zero Trust is rapidly replacing the castle-and-moat model.

From data protection and identity access management to threat detection and response and application security, today's security operations center (SOC) is engaged in a constant battle to balance security and access. Zero Trust requires strict verification of every individual and device seeking access to resources on private networks, regardless of whether they are sitting inside or outside the environment. While traditional information technology (IT) network security trusts anyone and anything inside the network as long as they can produce a password, a Zero Trust architecture trusts no one and nothing.

And that's just how SOCs should want it. Battle tested in the aftermath of breaches, nearly a third of security leaders recently surveyed by KPMG LLP (KPMG) indicated their SOC has difficulty determining the severity of cyber threats and vulnerabilities.[1] The complexity of the IT environment, lack of integration across solutions, and a lack of expertise among SOC staff are factors contributing to this challenge.

Challenges: SOC's barriers to identifying and remediating threats and vulnerabilities

% selected as one of up to three biggest barriers

Source: KPMG SOC survey, 2024. The values in this graphic do not total 100% due to rounding.

Nearly half (49 percent) of survey respondents said that improving trust in their organization's SOC is a top goal over the next two years. They want to increase digital trust through better privacy, proactive identification, and remediation of threats. Importantly, nearly 4 in 10 security leaders (38 percent) want to enable the business to innovate and create new products and services faster.

[1] KPMG Security Operations Center survey, "The time to transform is now," 2024

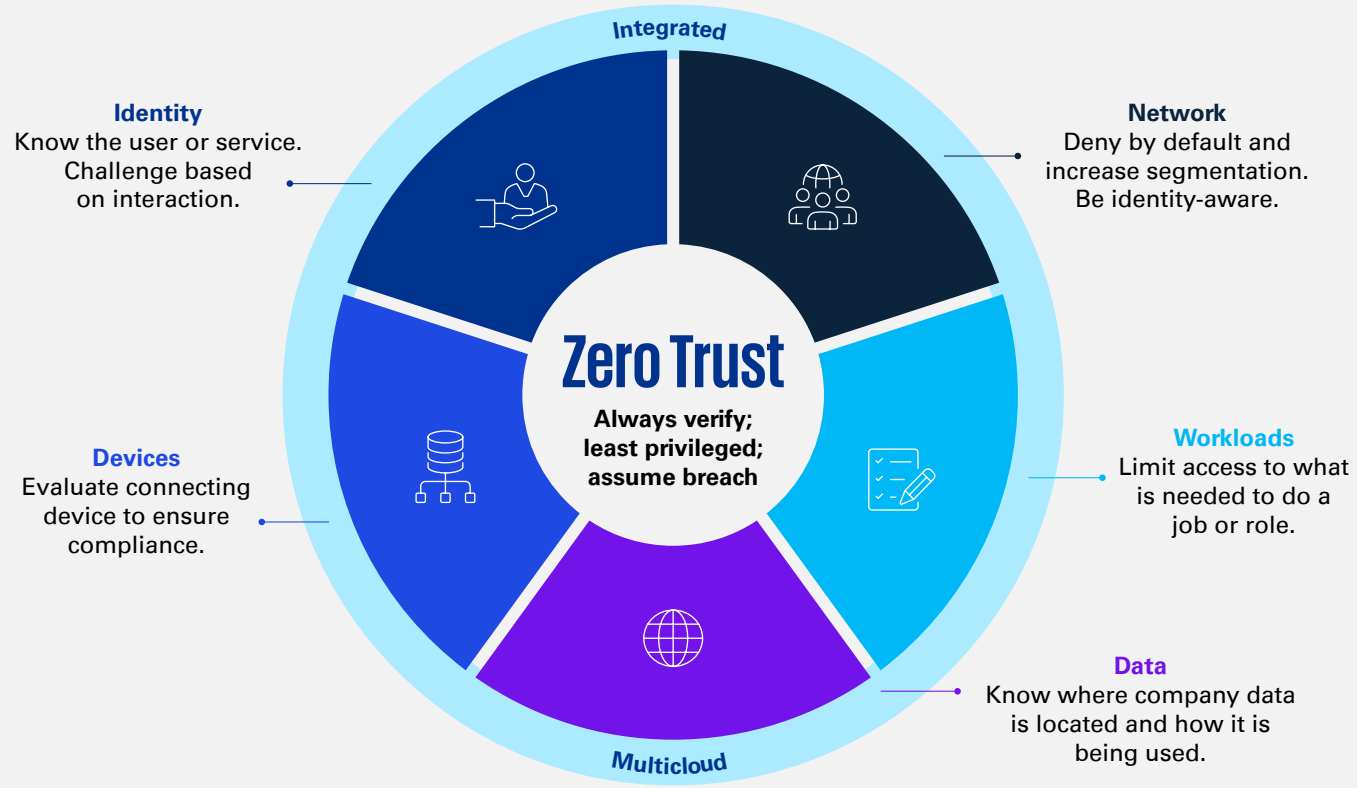
A platform-based approach

In our experience, the most effective way to achieve these goals is to assume a Zero Trust posture to mitigate risk while securing an ever-vulnerable landscape.

Many organizations today deploy 100 or more security applications when they only need 20 to 30 specific to their unique circumstances. Taking a best-of-breed approach to security products—and then trying to stitch them together—requires training across various product sets and increases costs and complexity. Worse, many of these applications cannot be integrated with each other or the system as a whole. In a business environment that thrives on maintaining connections, this lack of alignment is suboptimal, to say the least.

Relegating security architecture to fewer but more integrated platforms enables cyber teams to focus on reducing risk rather than managing technology. It can also streamlines operations, reduces ongoing expenditures, and identifies redundancies for long-term operational savings.

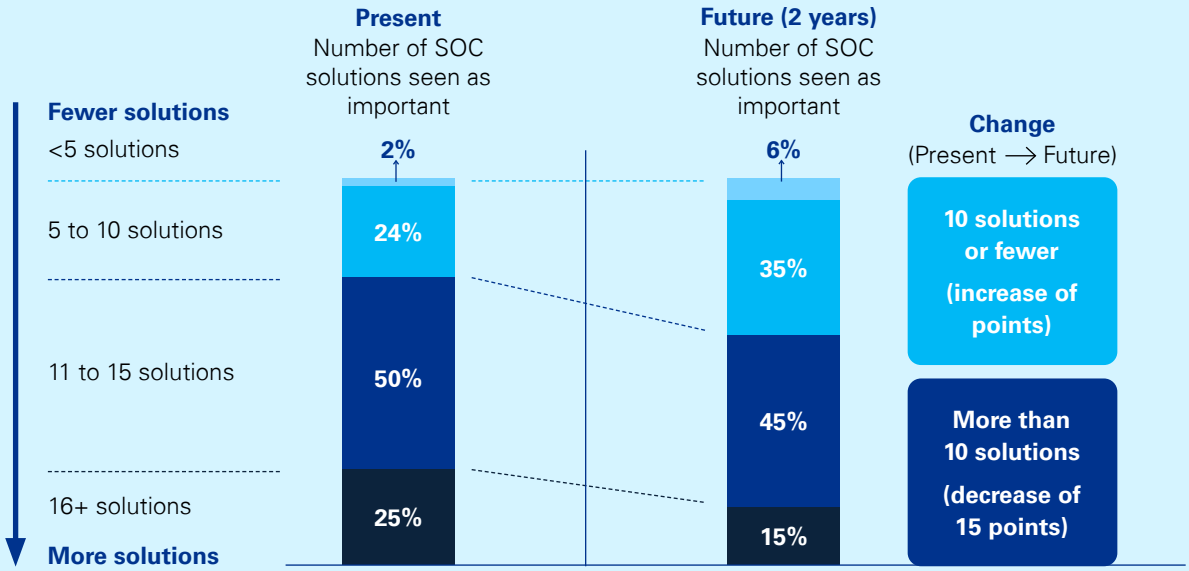
Zero Trust sits at the heart of an integrated suite of streamlined critical processes



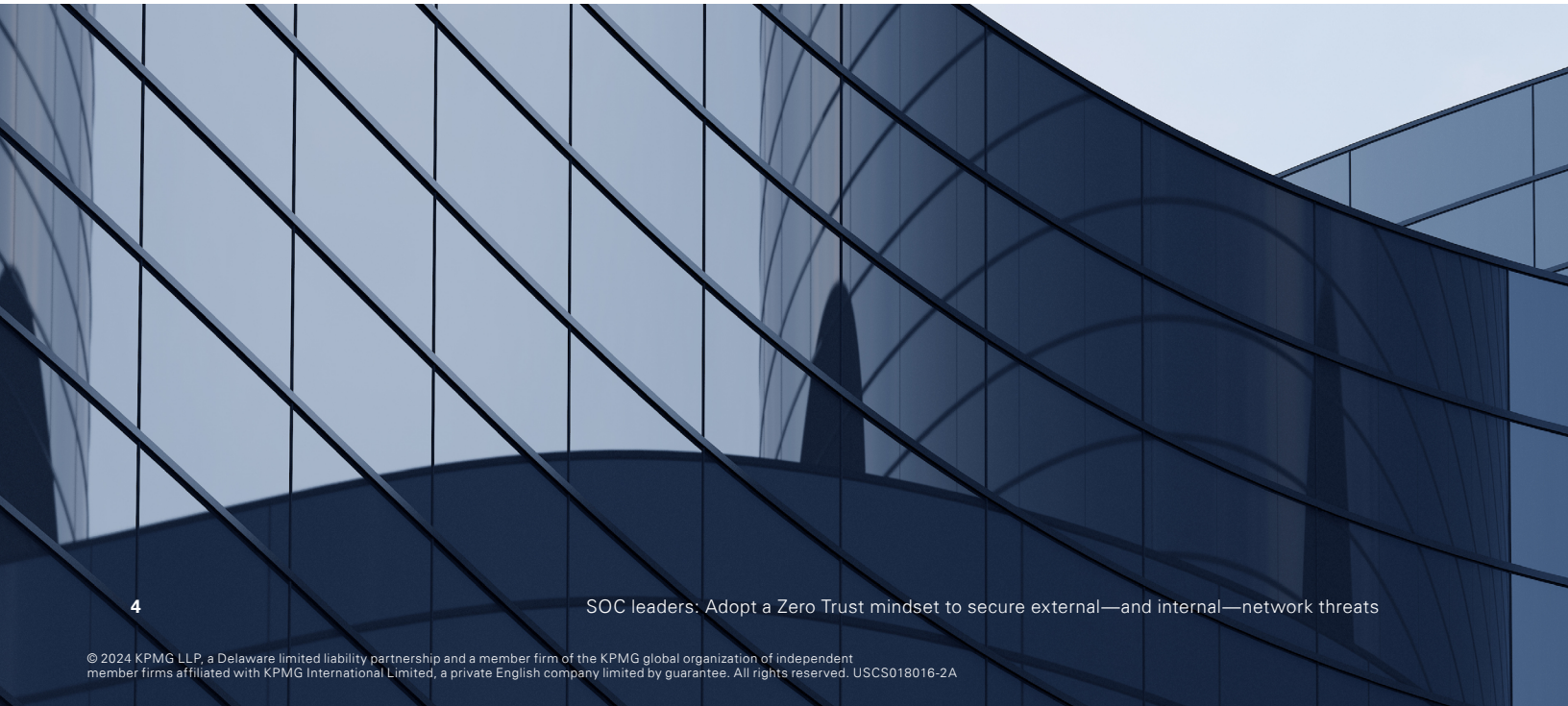
Looking ahead, security leaders say that fewer services and solutions will be important, according to the SOC survey. This finding suggests a trend toward more prioritization and consolidation of solutions in the future. It also reflects the challenges experienced with complex security environments and the lack of integration that SOC leaders cite as top challenges.

Adding to that complexity in the SOC, with numerous alerts coming from so many different tools, it becomes difficult for cyber teams to react to and handle all of these different signals across different systems instead of through a "single pane of glass."

Most important services and solutions for the organization's SOC: Present and future (next two years)



Source: KPMG SOC survey, 2024. The values in this graphic do not total 100% due to rounding.



New security operations principles

With Zero Trust accepted across the enterprise, SOCs will function according to the three key principles: assume breach, always verify, and least privilege.

In practical terms, these principles cover five Zero Trust pillars:

Identity

Know the user or service. Challenge based on interaction.

Network

Deny by default and increase segmentation. Be identity-aware.

Devices

Evaluate connecting devices to ensure compliance.

Applications

Limit access to what is needed to do a job or role.

Data

Know where company data is located and how it is being used.

Despite the rigidity of these principles, there is opportunity for balance. For example, in the short term after implementation, security teams may see an uptick in alerts. More incidents are being monitored, but they're not likely turning into successful attacks. AI-based automation embedded in the new platforms can prioritize the threats that need immediate human attention.

This balancing act helps neutralize one of the top pain points for 30 percent of security leaders, who according to our survey report fatigue from assessing a massive volume of low-fidelity alerts and/or false positives versus legitimate threats that require immediate urgent attention.

Measuring the benefits

Organizations that assume a Zero Trust posture tend to see a number of benefits, including:

- More predictable cyber spend
- Increased investment efficiency
- Improved coverage and visibility of cyber risks
- Reduction in overall cyber risk exposure
- Reduction of on-premises data centers and secure migration to the cloud.

How KPMG can help

Having implemented a Zero Trust model throughout our own SOCs in the US, we know how to use a platform strategy to diminish risk and cost. We reduced our security products from over 100 to fewer than 30 and solidified our cybersecurity in the process.

KPMG has deep experience across the Zero Trust continuum—from the boardroom to the SOC. We combine deep business knowledge with technical know-how to help clients create a resilient and trusted digital environment in the face of evolving threats. In addition to assessing your security platform and aligning it to your business priorities, we can help you develop and implement an overarching Zero Trust strategy, monitor ongoing risks, and identify and respond effectively to cyber incidents.

Contact us

Matthew P. Miller
Principal, Advisory
Cyber Security Services
KPMG LLP
T: 212-954-4648
M: 571-225-7842
E: matthewpmiller@kpmg.com

Manish Wardekar
Director, Solution Relations
Alliances
KPMG LLP
T: 312-665-1000
M: 630-605-4584
E: mwardekar@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**

New security operations principles

With Zero Trust accepted across the enterprise, SOCs will function according to the three key principles: assume breach, always verify, and least privilege.

In practical terms, these principles cover five Zero Trust pillars:

Identity

Know the user or service. Challenge based on interaction.

Network

Deny by default and increase segmentation. Be identity-aware.

Devices

Evaluate connecting devices to ensure compliance.

Applications

Limit access to what is needed to do a job or role.

Data

Know where company data is located and how it is being used.

Despite the rigidity of these principles, there is opportunity for balance. For example, in the short term after implementation, security teams may see an uptick in alerts. More incidents are being monitored, but they're not likely turning into successful attacks. AI-based automation embedded in the new platforms can prioritize the threats that need immediate human attention.

This balancing act helps neutralize one of the top pain points for 30 percent of security leaders, who according to our survey report fatigue from assessing a massive volume of low-fidelity alerts and/or false positives versus legitimate threats that require immediate urgent attention.