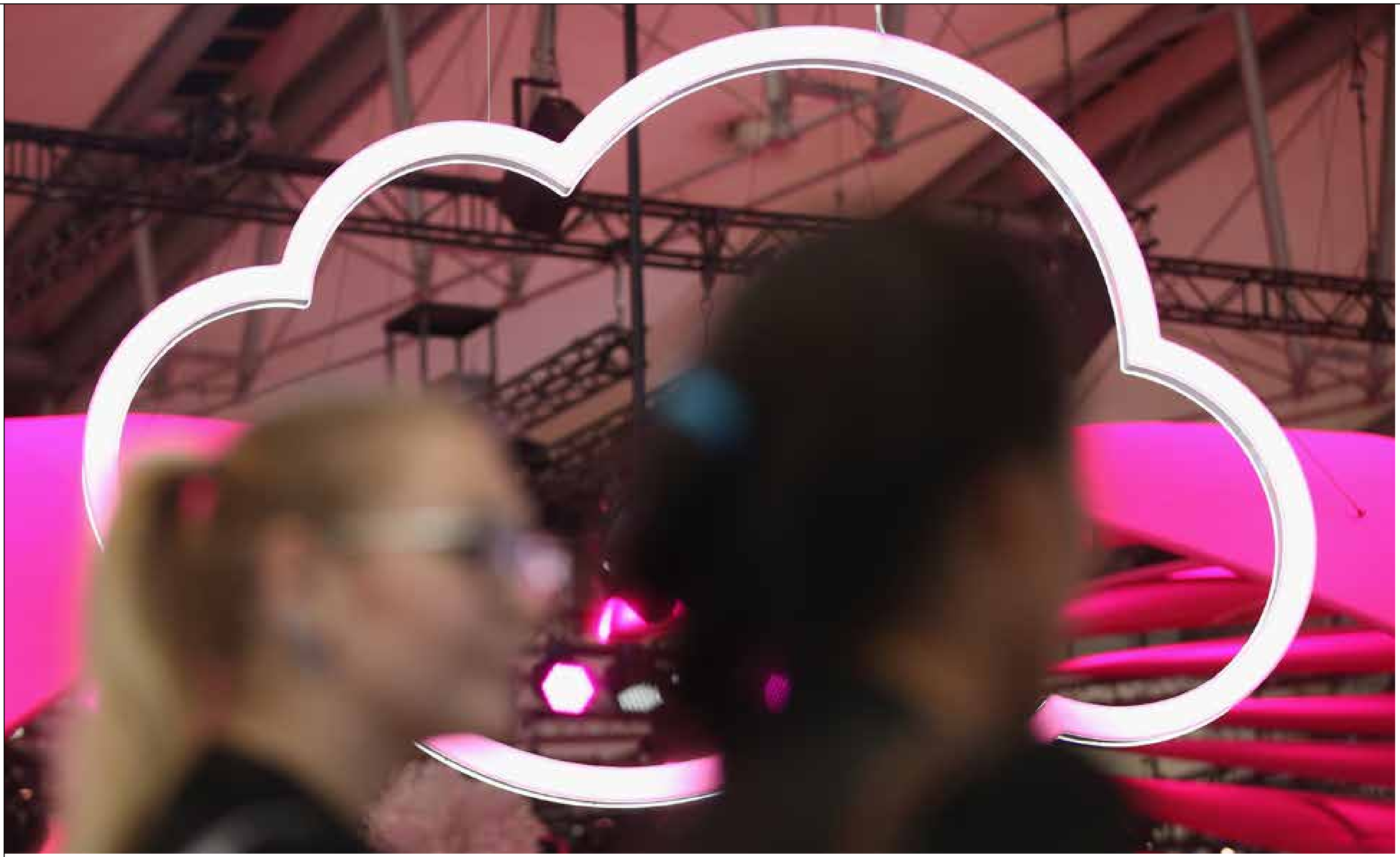

Picture credit: Getty

PRAGMATISM PAYOFF

Raghu Nandakumara *explains the essential role that Zero Trust plays when it comes to transforming cyber concerns from mountains into mole hills*

Digital transformation has been the watchword of the last decade, and in the past two years, the concept has become even more synonymous with hyperconnectivity. The Covid-19 pandemic accelerated the move to the cloud for many organisations, and today modern, digital businesses thrive on remote, hybrid connection – enabling greater productivity while also opening organisations up to a wide range of newfound threat vectors.

The latest reports from IDC estimate that cloud spending increased by 8.3 percent last year (compared to 2020), with total global cloud spending topping $71-billion. Meanwhile, reports estimate that the number of IoT devices installed worldwide hit 35 billion in 2021, with the number set to double by 2025.

As a result of trends like these, the shape of the average business IT environment has drastically changed in just a few short years. While these changes have brought benefits including lower costs and greater agility in the cloud, they have also led to more complex environments that are increasingly difficult to manage and secure. The attack surface has expanded dramatically, with each new cloud environment and fleet of IoT devices creating yet more opportunities for threat actors.

Total global spending on the cloud topped $71-billion in 2021

As a result, the security landscape has also been vastly altered. The old stalwart security model of 'trust but verify' has been rendered outdated and inadequate to account for such a dense and dynamic environment. It can neither match the complexity created by multi and hybrid-cloud environments, nor scale effectively as businesses continue their ambitious digital expansions – how can you assign 'implicit trust' to such a wide variety of resources? Instead, most organisations are now looking to the Zero Trust model to build sustainable resiliency as their IT estates expand.

Cybersecurity has long been a reactive affair, with organisations opting for strategies built around prevention-at-the-perimeter defences (VPNs, firewalls, *etc*.), largely trying to thwart attackers at the outside gate. By contrast, Zero Trust is a transformational approach to security, predicated on concepts like 'assuming breach' that bolster organisational resilience proactively and from within.

Zero Trust is a mindset rather than a specific set of tools or practices. As Forrester succinctly defines it: "Zero Trust is not one product or platform; it's a security framework built around the concept of 'never trust, always verify' and 'assuming breach.'"

The theory behind Zero Trust is nothing new – it was first coined by Forrester analyst John Kindervag over 10 years ago. However, where Zero Trust was once a cutting-edge strategy for only the organisations most concerned about defending against elite threat actors, the framework has become more widely known over the years.

The Zero Trust approach of 'never trust, always verify' means that no user or system is ever implicitly trusted to access *anything*. This is a stark contrast to the way access has been handled in previous years, where having access to the network was often enough to grant immediate access to the entirety of the infrastructure. Instead, with Zero Trust, access between individual resources is verified and then granted based on their context and whether access must exist between them – having access to one resource is no guarantee of access to anything else.

These additional verification measures are implemented with a risk-based approach that varies based on factors like the importance of the asset being accessed and the user's location and device. While capabilities such as enhanced Identity and Access Management (IAM) and Zero Trust Network Access (ZTNA) are important parts of a Zero Trust Architecture, Zero Trust Segmentation (also known as microsegmentation) is a central pillar in creating a unified and resilient Zero Trust security posture that can successfully scale across the business.

As technology and the threat landscape advance, Zero Trust has become an increasingly common element of a modern cybersecurity strategy. Research commissioned by Illumio and conducted by Forrester found that more than 75 percent of respondents not only knew what Zero Trust was but felt that it had an important role to play in their current security strategies. This awareness generally seemed to extend to deeper technical familiarity, rather than just name recognition.

Over the last year, Zero Trust awareness has been boosted further by the Biden Administration's executive order and memorandum on Zero Trust, which explicitly mandated US government agencies move to a Zero Trust architecture. Achieving visibility and segmentation across the hybrid infrastructure is central to making a Zero Trust strategy a reality. But Zero Trust is about much more than implementing the right tools and processes – it also demands the adoption of the right mindset. Taking on the 'assume breach' mentality is a big part of that.

The 'assume breach' mindset assumes at its core that a threat actor has *already* gained access to your critical business assets – whether that be your corporate networks, an employee laptop or your remote datacentre. While this might seem defeatist, this kind of pragmatism is essential in today's hostile threat landscape. Breaches are now occurring on a near constant basis, and research indicates that credentials are the primary target of most attacks. Even the most well-secured organisations must assume that their users will be the targets of phishing attacks or be otherwise compromised. And, as we have seen time and time again, it only takes one compromised user to set a potentially cataclysmic breach into motion.

Assume breach is an important part of Forrester's definition of Zero Trust, particularly when adopted alongside a 'least privilege' mindset. If you start with a mentality when designing security controls, the focus is: "how do I limit what a malicious actor can do?". This shift leads to the definition of least privilege access policies – resulting in attacks being slowed down and contained earlier on, thus having significantly limited impact.

REMOTE HYBRID CONNECTIONS OPEN ORGANISATIONS UP TO NEW THREAT VECTORS

Zero Trust Segmentation is one of the most important assets for containing an intruder post-breach. With Zero Trust Segmentation, the organisation splits its IT environment (whether that be in the cloud, the network, the datacentre, *etc*.) into multiple sealed sections. This means that the initial reach or impact of a breach is drastically limited, with the attacker only being able to access a small section of the business.

Attackers will often aim to breach external defences in order to gain initial access to the enterprise. From there, they'll move across the organisation until they reach their intended target. With Zero Trust Segmentation, firms are empowered to own their attack surface and limit the reach of a breach by ensuring their critical assets are sectioned off from the general business infrastructure, meaning that even in the event the organisation is breached, those essential business assets remain unscathed.

Given Zero Trust Segmentation enables least privilege access between resources within an organisation, it is an essential pillar of any respectable Zero Trust architecture. It ensures that a minimum level of containment is in place, regardless of what state IAM or ZTNA may be in. In short, it's the foundation on which organisational resilience is built.

While Forrester's research found that the nature and benefits of Zero Trust are generally well understood by business leaders today, there were still significant challenges when it came to turning that awareness into action. Just over a third of respondents stated they were in the implementation phase of their Zero Trust project, and only six percent said they had fully deployed their strategies.

One of the biggest barriers to Zero Trust progress appeared to be a lack of resources. For example, two

▶

thirds of respondents stated that their internal teams lacked the time, subject matter expertise and skills to successfully implement microsegmentation.

However, in many cases organisations are failing to make progress because they view Zero Trust as a single project that is too big to begin. Because a pure Zero Trust adoption will eventually encompass the entire operation, there is a misconception that it's an all-or-nothing venture.

ZERO TRUST BOLSTERS ORGANISATIONAL RESILIENCE PROACTIVELY AND FROM WITHIN

In reality however, Zero Trust is best implemented as a series of smaller, iterative projects that can be completed and add immediate value in their own right. Changes can be made on a step-by-step, application-by-application basis. And each step is a step towards a more comprehensive and resilient Zero Trust state.

One of the defining differences in organisations that have succeeded with Zero Trust is clear communication between security leaders and their stakeholders. Buy-in from the top is important since it's essential for securing the budget and resources needed to get any security project off the ground.

But communication should extend to every other relevant stakeholder – in the end, everyone will be living Zero Trust daily. It's crucial to explain what Zero Trust is, how it will benefit those stakeholders specifically and most importantly, why it is necessary for the organisation.

Firms who have enjoyed the most success out of their Zero Trust endeavours have invested time up front in helping their stakeholders understand the methodology and worked out a timeline for rolling it out across the business. Good planning, good engagement and consistent education are key elements that make for a successful and long-lasting Zero Trust programme.

Every Zero Trust journey starts with understanding your risk. Firms must gain full visibility into their IT infrastructure, determine where key assets are located, and understand how they are interconnected. This process will make it easy to mark out the highest priority areas for Zero Trust adoption. Organisations should focus their attention wherever Zero Trust will have the greatest impact on mitigating critical risk.

Finally, it's important to create a realistic roadmap for implementation. What this looks like will vary depending on each organisation's resources and priorities. Even the most supportive board will become sceptical if the project appears to be stalling or failing to deliver value. The ideal roadmap should be marked with multiple milestones that continually demonstrate progress and value. Every company has its own timeline, but it is important to establish one that fits and make continual progress against it or risk losing support.

With today's increasingly hostile threat landscape, Zero Trust has never been more important. It's also never been more achievable. While organisations are still coming to grips with what true Zero Trust is, by taking a realistic, iterative approach, backed by an assume breach mindset and capabilities like MFA and Zero Trust Segmentation, organisations can start making resilience a reality. That way, even when a threat actor does manage to break through perimeter defences, your organisation will be able to carry on with minimal business disruption ●

Raghu Nandakumara is Senior Director, Head of Industry Solutions, at Illumio

The 'assume breach' mindset is essential in today's hostile threat landscape

Picture credit: Andrea Piacquadio