# Illumio’s CPO calls for a shift to containment in cyber defence



In a landscape increasingly characterised by cyber threats and complex IT environments, Illumio’s Chief Product Officer, Mario Espinoza, proposes a significant shift in the approach to digital defence. Speaking to the Independent, Espinoza argues for a transition from a mindset focused on prevention to one prioritising containment of breaches, reflecting a pragmatic understanding that fully preventing cyber-attacks is becoming increasingly unfeasible.

Espinoza suggests that organisations should come to terms with the inevitability of breaches. "The breach is going to happen no matter what," he stated, emphasising that today's IT environments are too intricate, with advanced attacks and human errors compounding the challenges of prevention. He further advocates for the adoption of a Zero Trust security model, which operates on the premise of “never trust, always verify.” This approach contrasts sharply with traditional methods that aim to secure the perimeter of a network, an outdated notion in an era where connections can originate from both inside and outside any perceived boundary.

Zero Trust is centred around microsegmentation, which divides an organisation's IT environment into small zones, thereby enhancing internal security rather than relying solely on a perimeter. However, deploying Zero Trust has historically posed challenges due to cost and complexity, particularly in hybrid environments where cloud, virtual machines, and IoT devices proliferate. Espinoza notes, “For years, even those who agreed with Zero Trust in principle found it hard to use in practice.”

The adoption of Zero Trust is gaining momentum, largely influenced by two converging trends. Firstly, the frequency of cyber threats has escalated significantly over the past 15 years since the concept was first introduced by John Kindervag. The sheer volume of cyber breaches has prompted a reassessment of conventional security measures, with increasing evidence that they are insufficient. Secondly, advancements in technology, particularly involving AI and automation, have simplified the implementation of Zero Trust principles, making them more accessible to organisations.

Espinoza highlights how the technology landscape has evolved, saying, “It’s not as if people just now realised how effective containment is,” thus reinforcing that the difficulties previously associated with Zero Trust deployment are being addressed.

In 2021, the U.S. federal government issued Executive Order 14028, mandating the adoption of Zero Trust across its agencies, evidencing a systemic shift towards this security model. Many corporations, including notable institutions like JP Morgan Chase and Bank of America, have begun to document their own Zero Trust strategies, marking a significant move in a sector traditionally reticent to share details of their defence mechanisms.

Research firm MarketsandMarkets predicts that the global Zero Trust security market is set to more than double, reaching $60.7 billion by 2027, while Forrester Research reports that over 60 per cent of enterprises are either deploying or enhancing their Zero Trust initiatives.

Adding to the complexity of the threat landscape is the emergence of AI-powered attacks, particularly in the realm of social engineering. Espinoza states, "The weakest link today is the human at the keyboard," pointing to the ease with which attackers can exploit human vulnerabilities. This stark reality underscores the need for organisations to adopt a containment strategy, as the chances of breaches remain high.

Espinoza also encourages security leaders to explore innovative approaches like security graphs, which analyse traffic patterns within IT infrastructures to identify potential threats. While concepts such as these have been discussed in the past, they have only recently become feasible due to advancements in data processing and AI capabilities.

For those businesses looking to embrace Zero Trust, Espinoza advises that the initial focus should be on gaining visibility into their environments rather than rushing to implement controls immediately. Understanding vulnerability and data flow lays the groundwork for establishing robust Zero Trust policies.

As cyber threats continue to evolve in complexity and sophistication, the shift towards containment strategies is becoming increasingly crucial. While Espinoza acknowledges that these measures will not eliminate the risk of attacks, they are designed to mitigate their impact. “With proper containment, an attack won’t become a cyber-disaster,” he concludes, reinforcing the significance of adapting to the ever-changing cyber landscape.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://www.illumio.com/blog/contain-ransomware-at-its-source-with-zero-trust-segmentation> - This article supports the claim that Zero Trust Segmentation can effectively contain ransomware attacks by preventing lateral movement within a network, aligning with Mario Espinoza's emphasis on containment strategies.
* <https://www.illumio.com/solutions/ransomware-containment-cases> - This resource highlights how Illumio's solutions provide visibility into security risks, helping organizations define containment strategies and protect high-value assets, which aligns with Espinoza's advice on prioritizing visibility.
* <https://www.illumio.com/blog/manufacturing-ciso-tips-proactive-breach-containment> - This article discusses proactive breach containment strategies using Illumio's Zero Trust Segmentation, emphasizing network visibility and personalized insights, which supports Espinoza's advocacy for Zero Trust.
* <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/> - Executive Order 14028 mandated the adoption of Zero Trust across U.S. federal agencies, reflecting a systemic shift towards this security model as mentioned by Espinoza.
* <https://www.marketsandmarkets.com/Market-Reports/zero-trust-security-market-242526865.html> - This report from MarketsandMarkets predicts significant growth in the Zero Trust security market, supporting Espinoza's observation about the increasing adoption of Zero Trust strategies.
* <https://www.forrester.com/report/zero+trust+security+market+trends+and+forecast+2023+to+2028/-/E-RES173531> - Forrester Research reports on the widespread adoption of Zero Trust initiatives among enterprises, aligning with Espinoza's comments on the trend towards Zero Trust.
* <https://www.forbes.com/sites/forbestechcouncil/2022/02/22/the-importance-of-zero-trust-security-in-todays-digital-landscape/?sh=6c4f8a5d66b3> - This article discusses the importance of Zero Trust security in today's complex digital landscape, supporting Espinoza's views on the necessity of shifting from prevention to containment.
* <https://www.csoonline.com/article/3625334/zero-trust-security-what-it-is-and-how-it-works.html> - This resource explains how Zero Trust security operates, including its focus on microsegmentation, which aligns with Espinoza's description of Zero Trust principles.
* <https://www.gartner.com/en/newsroom/press-releases/2022-06-14-gartner-says-ai-powered-cybersecurity-solutions-are> - Gartner discusses AI-powered cybersecurity solutions, which relate to Espinoza's mention of AI advancements simplifying Zero Trust implementation and addressing AI-powered attacks.