The Time for Microsegmentation is Now Q&A

Valuable perspectives from Forrester Senior Analyst David Holmes after a recent webinar with Illumio

Featuring FORRESTER®

1. **How has the nature of threats such as ransomware changed recently?**
2. **Why have the typical approaches to network security failed?**
3. **How can an 'assume breach' mindset help to create a more robust security approach?**
4. **Why is microsegmentation critical for an organization's cyber resilience?**
5. **Can a company truly have a Zero Trust cybersecurity strategy without microsegmentation?**

1 How has the nature of threats such as ransomware changed recently?

Ransomware has become a scourge not just to well capitalized, high-tech and financial firms; attackers are now broadly targeting smaller, non-technical companies and extracting from them painful, but not unrealistic, extortion payments. Businesses are aware of this problem and are keen to do something about it. According to a 2021 Forrester survey of 978 services and cloud infrastructure decision-makers, 23% of respondents report that protecting against ransomware attacks is a priority in the next 12 months. Interestingly, among Millennial respondents at SMB firms, the percentage rises to 28%.

2 Why have the typical approaches to network security failed?

Two factors contribute to the failure of traditional approaches to perimeter security. The first is the original sin of IP connectivity; the networks we have used for the last 25 years allow any device on the network to talk to any other device. The information security model of Zero Trust arose specifically in protest to the state of security on IP networks. The second factor is that, with ransomware, attackers are highly motivated to distribute their malicious payloads. For most attackers, it is literally their job and how they get paid.

3 How can an 'assume breach' mindset help to create a more robust security approach?

When an organization invests the bulk of its security budget into perimeter security controls like so-called next-generation firewalls, all it takes is a single payload to make it past the perimeter for the game to be over and the data encrypted or exfiltrated. The more modern approach of inserting Zero Trust controls around critical data inside the perimeter, or wherever the data resides, allows protection even when the attacker is initially successful. This approach also gives the defender time to detect the attacker and remediate the improper access, whereas without these controls, there is no time delta to help the defender.

4 Why is microsegmentation critical for an organization's cyber resilience?

Year to year, approximately a quarter of respondents to Forrester surveys report that they are embarking on a Zero Trust journey. Part of that journey must include microsegmentation to address the problem of too-loose connectivity in the on-premises and cloud networks. Trusted partners like Illumio help these organizations implement Zero Trust in their networks, especially around critical and important applications and data.

5 Can a company truly have a Zero Trust cybersecurity strategy without microsegmentation?

While there are many cybersecurity technologies, disciplines and sub-disciplines, only a handful are considered truly Zero Trust. Microsegmentation is the initial, marquee Zero Trust technology, specifically designed to address the challenges of the insecure network, where organizations know that they need to do better. There has been a lot of activity around Zero Trust access to applications, especially when replacing VPN infrastructure, but after those projects are complete, an organization needs to invest in microsegmentation to successfully execute a Zero Trust security strategy.

To learn more, watch the recorded webinar **"The Time for Microsegmentation is NOW"** with host PJ Kirner, CTO and Co-Founder of Illumio, and guest speaker David Holmes of Forrester Research.

About Illumio

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.