TRUEFORT™

# Restricting lateral movement with Microsegmentation

Creating more secure environments and efficiently reducing your attack surface by segmenting your application workloads.

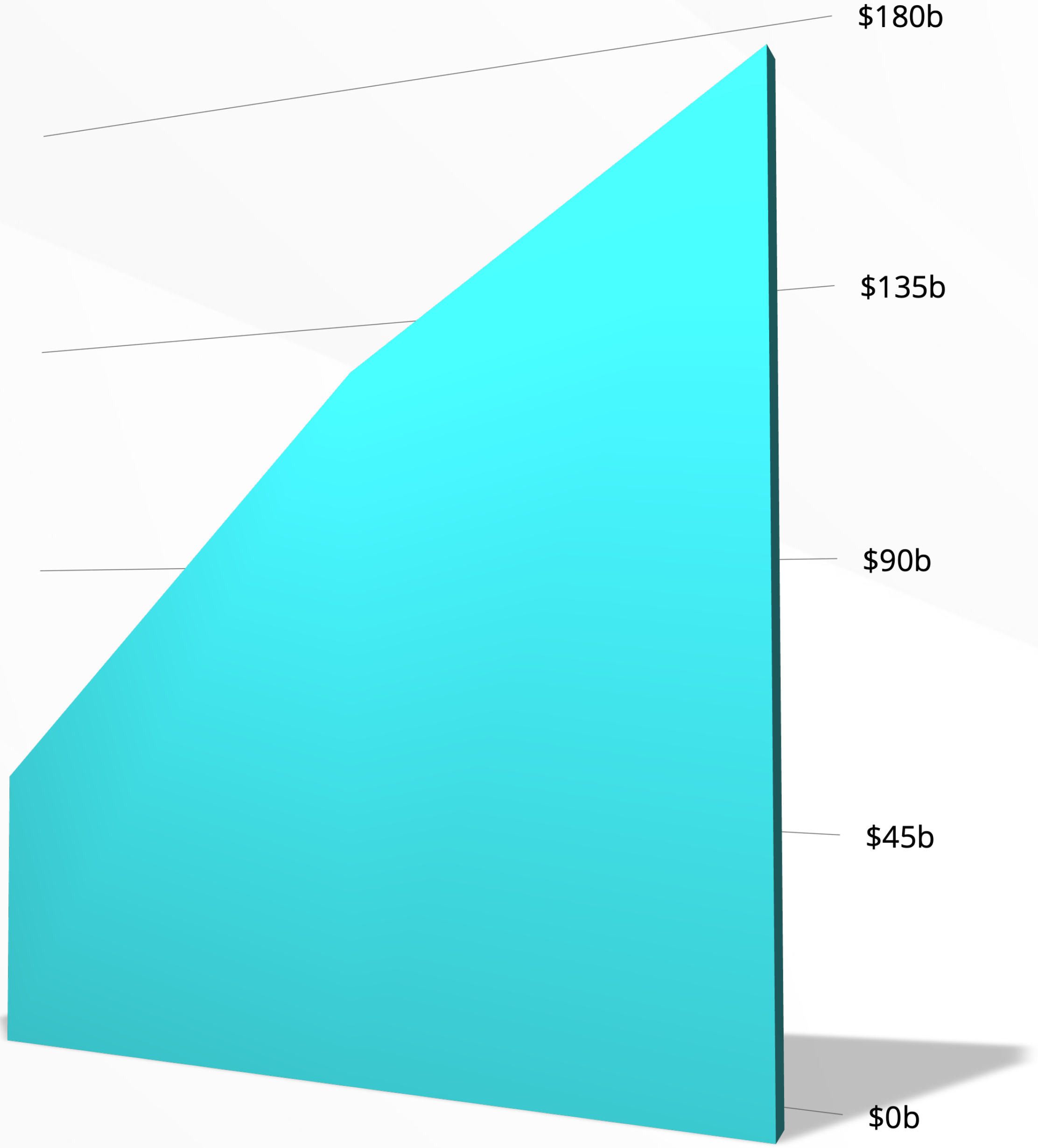
truefort.com

Every single company has a need to ensure vital workloads are protected, yet the question of how each organization opts to provide this fortification varies.

While there's no one-size-fits-all approach to safeguard your business, companies are clearly investing in vigorous security solutions.

**Gartner's research indicates that businesses will increase their security spending by nearly $50 billion between 2020 ($123 billion) and 2022 ($170 billion).**

As the ongoing evolution to distributed networks and applications grows in popularity, many organizations are unaware of the expanding threat landscape associated with these changes. Along with the increase of application environments and containerized infrastructure comes the additional increase in the complexity of protecting these diverse and dynamic applications and workloads.



# What’s the risk?

As your environment grows, so does your vulnerability to potential attacks, and just one single attack can prove costly. According to research by IBM, **it can take up to 280 days to find and contain the average cyberattack, with the expense of resolving the average attack costing $3.86 million.**

Just as networks are evolving so too are the complexities of the attacks, as each new day brings a fresh array of threats designed to impact not only your business and brand image, but also your customers.

The better part of a year to contain the average cyberattack.

The expense of resolving the average attack.

**Cyber-crime costs organizations $2.9 million every minute, and major businesses lose $25 per minute as a result of data breaches.**

- RiskIQ research.

# Why is this important?

Some of the benefits fueling the expansion of distributed applications and workloads include increased scalability, additional flexibility to share resources, and the potential of improved resiliency.

**However, to fully realize these benefits, organizations must also recognize the inherent risk of expanding their attack surface.**

One of the primary solutions to these challenges has been the adoption of the microsegmenting of environments to better isolate critical assets. Yet many are still unclear on exactly what microsegmentation is and how it can provide benefits.

# Cyber Fatigue

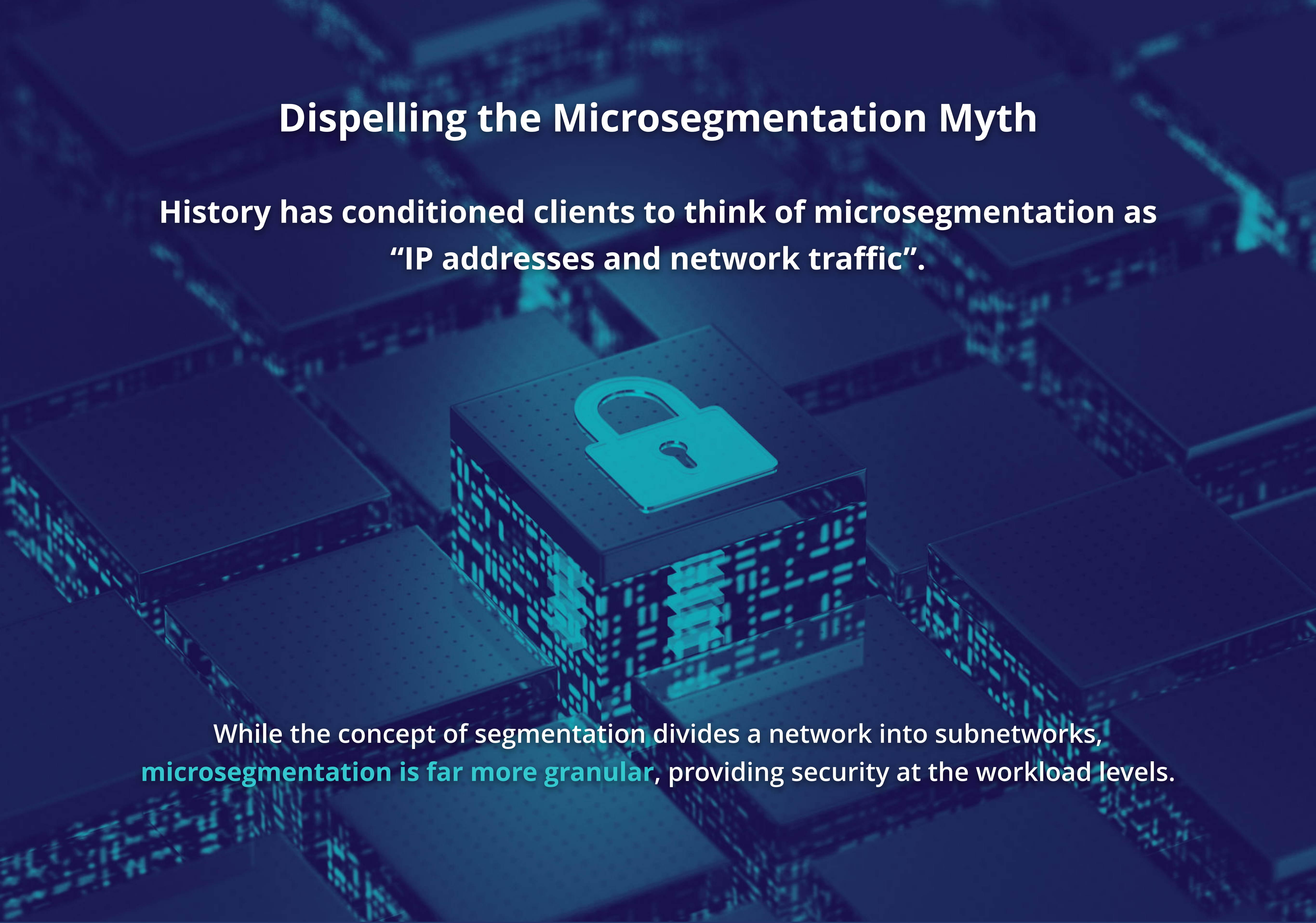
Cyber fatigue, or apathy to proactively defending against cyberattacks, affects as much as 42 percent of companies.

# Cost of Inaction

Worldwide cybercrime costs will hit $10.5 trillion annually by 2025.

# Dispelling the Microsegmentation Myth

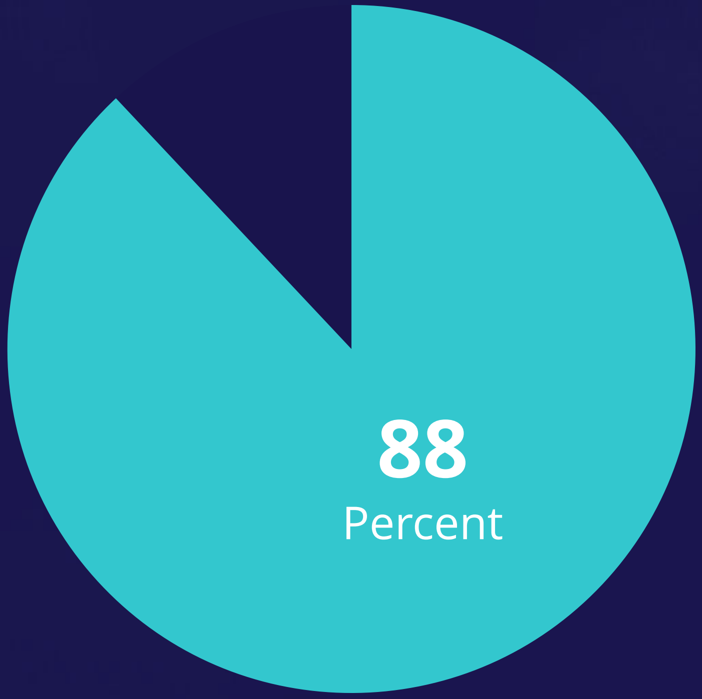
**History has conditioned clients to think of microsegmentation as "IP addresses and network traffic".**



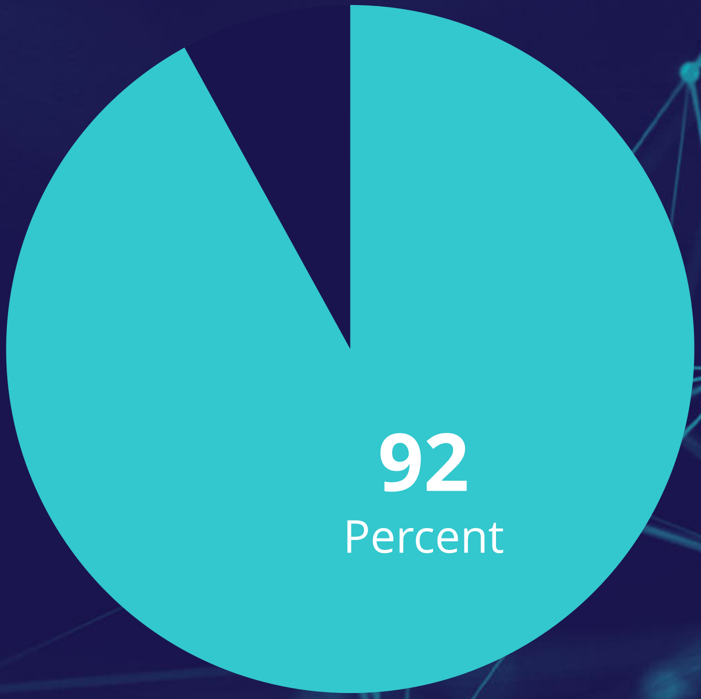
While the concept of segmentation divides a network into subnetworks, **microsegmentation is far more granular**, providing security at the workload levels.

Cyber-attacks require a preventative approach via Zero Trust, with microsegmentation uniquely positioned to ensure that the impacts of an incident are much more limited in scope.

This process is gaining acceptance across a variety of industries, with **88% of cybersecurity leaders believing microsegmentation is essential to achieving a Zero Trust architecture**, while **92% of cybersecurity leaders believe microsegmentation is more practical and efficient than its alternatives**.



Cybersecurity leaders believing microsegmentation is essential



Cybersecurity leaders believe microsegmentation is more efficient than alternatives

# Benefits of Microsegmentation

What can microsegmentation deliver for you and what is the benefit of implementing a microsegmentation solution?

By isolating critical assets and closing the pathways between systems, you can not only limit the extent of a potential attack, but also stop attacks earlier to reduce the damage they might cause to your organization.

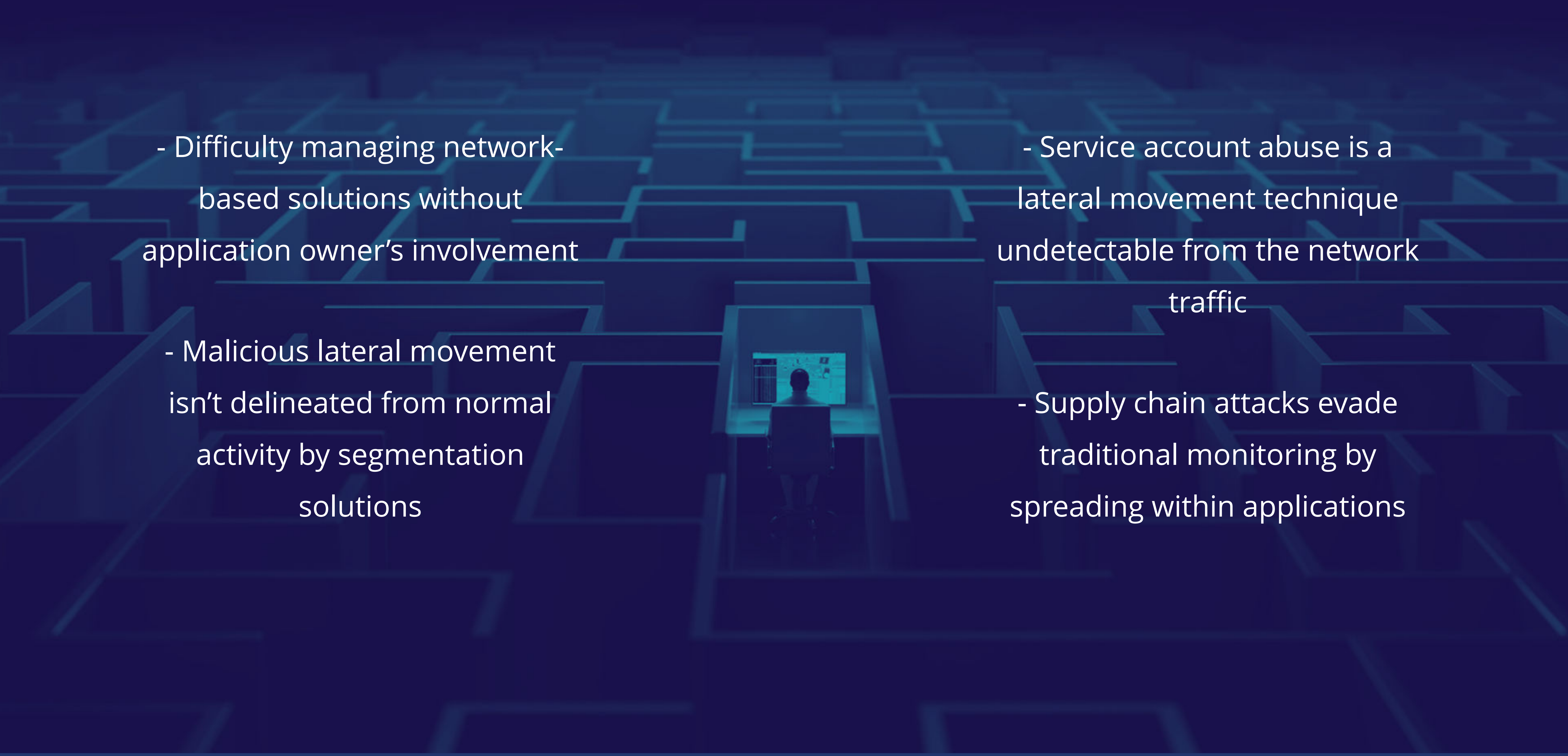
Microsegmentation also provides additional benefits such as ensuring compliance with evolving data and privacy standards, preventing unauthorized lateral movement, and establishing a foundation to implement Zero Trust security models.

- ✓ Limit the extent of attacks
- ✓ Stop attacks earlier
- ✓ Isolate critical assets
- ✓ Reduce damage of attacks
- ✓ Ensure compliance
- ✓ Prevent lateral movement
- ✓ Foundation for Zero Trust

Organizations with a Zero-Trust approach saw average breach costs $1.76 million less than organizations without.

# Barriers to success

**Despite these immense advantages, microsegmentation can also pose some unique challenges:**



- Difficulty managing network-based solutions without application owner’s involvement

- Malicious lateral movement isn’t delineated from normal activity by segmentation solutions

- Service account abuse is a lateral movement technique undetectable from the network traffic

- Supply chain attacks evade traditional monitoring by spreading within applications

**Selecting the right partner to assist you in implementing a robust microsegmentation solution can make a huge difference in setting your organization up for future success.**

In order to maximize the benefits of microsegmentation, any solution must be simple to deploy, easy to use, maintain accuracy, and produce intelligence-driven and actionable insights.

# TrueFort's Proactive Environment Attack Prevention

TrueFort provides comprehensive microsegmentation that reduces the attack surface from ransomware and other techniques targeting misconfigurations, unsecured APIs, outdated or unpatched software, unauthorized access, and zero-day vulnerabilities.

This results in more hardened systems capable of detecting and blocking unauthorized activity, allowing you to meet compliance, audit, and cyber insurance requirements.

## Using the TrueFort Platform, you'll gain real-time understanding of workload behavior and full visibility into critical applications.

Our streamlined approach is easy to deploy through agents you already have to quickly analyze the behavioral characteristics of your workloads' actions and achieve ROI at an incredible pace.

- ✓ **Discover and map all intra-application dependencies, workloads, and data flows to understand the attack surface.**
- ✓ **Define a trusted baseline of acceptable behavior across workloads and accounts to reduce unauthorized activity.**
- ✓ **Ease segmentation policy automation by application and workload profile to minimize blast radius.**
- ✓ **Enforce role-based, process-based, and user-based Zero Trust segmentation to expand the scope of containment capabilities.**

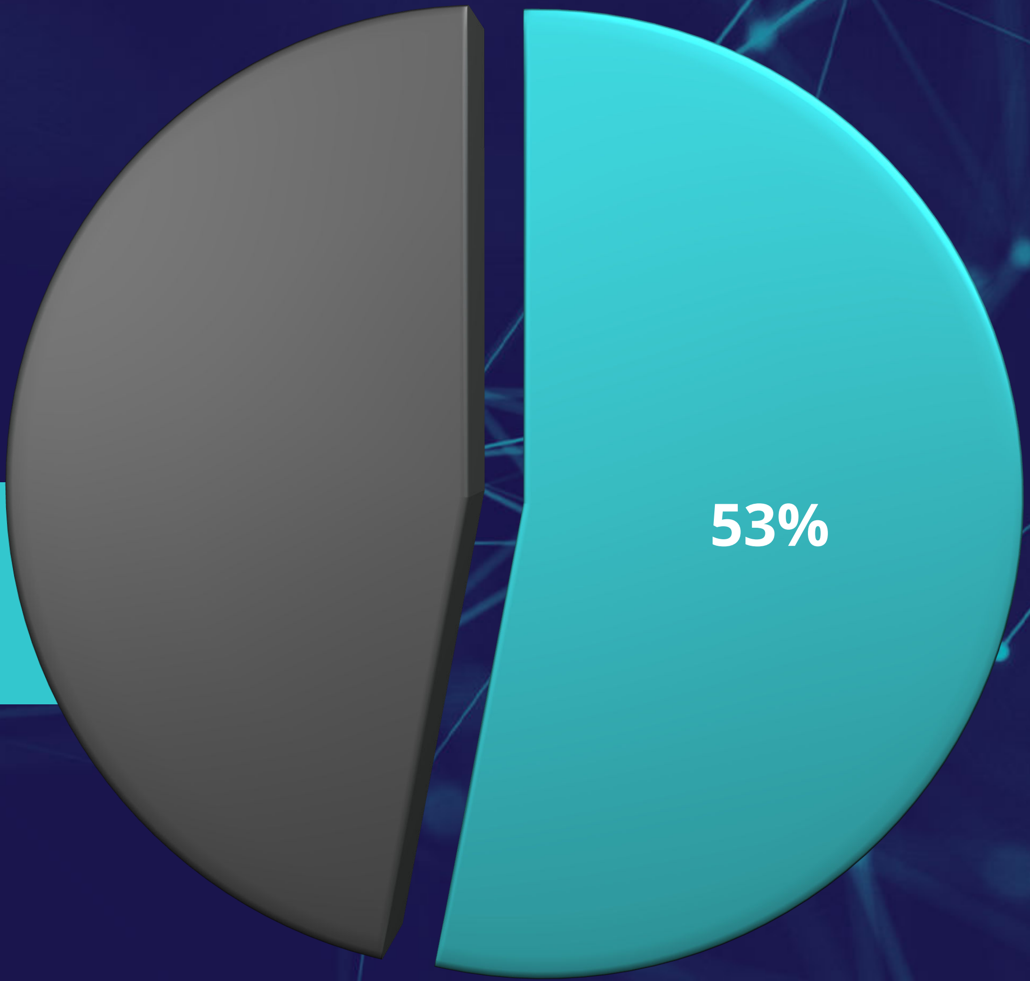
## Cybersecurity has become more difficult as applications become increasingly distributed, and the threat landscape continues to evolve.

Microsegmentation provides a superior level of security far beyond the limitations of basic network segmentation.

With the rise in both attack volume and complexity, organizations simply can't risk the conceivable damage and liability they'd be left open to without the level of protection TrueFort offers.

TrueFort protects your workloads by intelligently baselining normal, high-volume activities within and between applications, limiting future behavior to only what should be trusted.

**When asked, 53% of respondents cited the rise in cyberattacks as their main motivation towards implementing a microsegmentation solution.**



TRUEFORT™

TrueFort's innovative platform offers an intelligent approach that continuously insulates your environment against suspicious activities, detects malicious behavior, and prevents lateral movement.

**Gain comprehensive protection by securing your workloads at the application level with TrueFort.**