



# Reduce the Blast Radius with Micro segmentation

---

**Jonathan Borgesen**

# Introduction



## **Jonathan Borgesen** **Technical Director of Security**

15 years of experience in the cybersecurity industry. Throughout his career, he has built and led security practices for multiple organizations.

He emphasizes business impact, cross-architecture solutions, and strategic alignment over simply focusing on technology. This mindset has earned him a reputation as a trusted advisor and thought leader among his clients and peers.

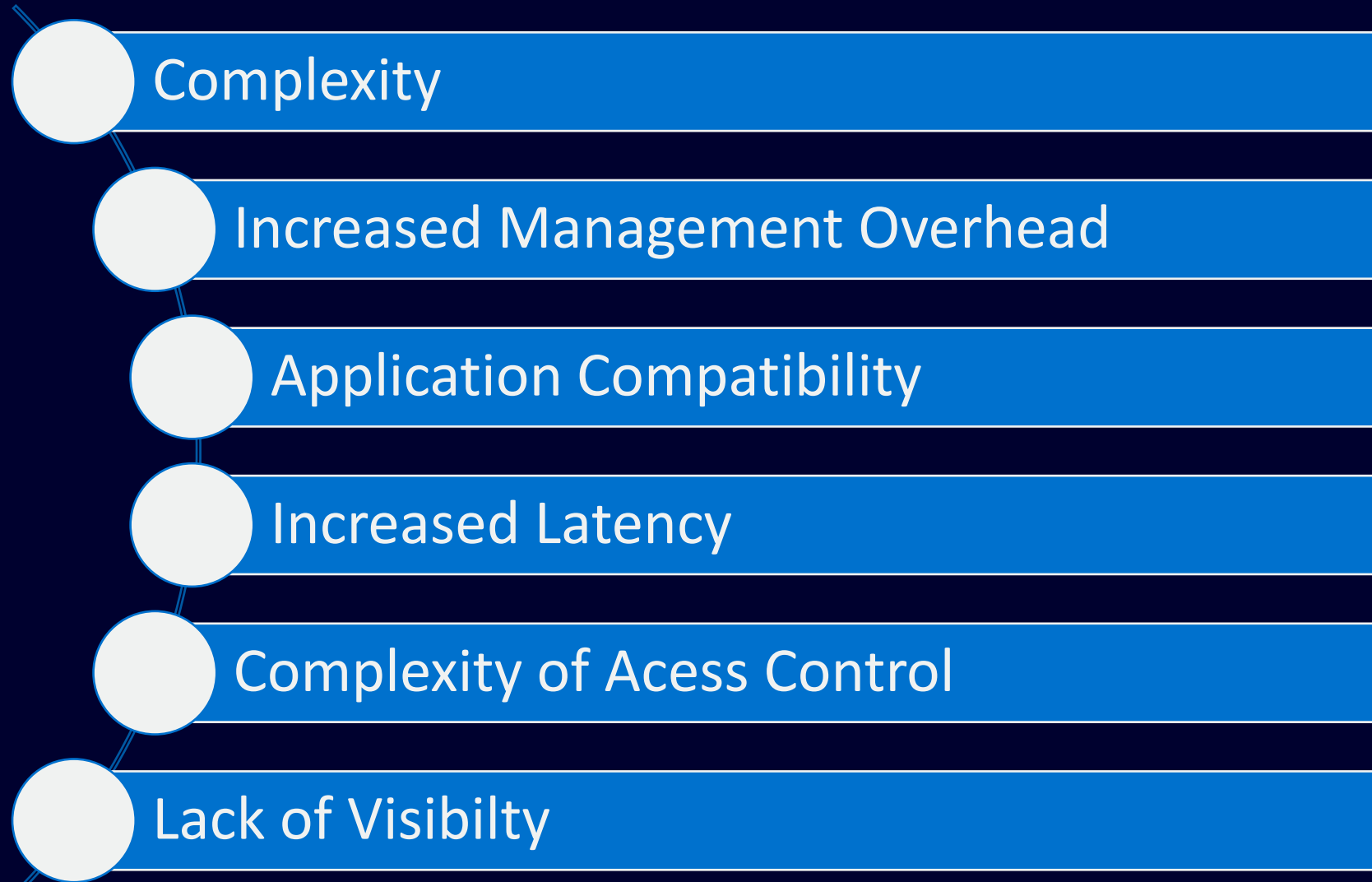


An aerial photograph of a city, likely New Orleans, showing a dense urban grid and a prominent river (the Mississippi River) winding through the landscape. The image is framed by a blue border. A dark blue rectangular box with a white border is centered over the image, containing the text "Historical Challenges" in white serif font.

# Historical Challenges



# Challenges Around Traditional Network Segmentation



# IT Silos Continue to Impact Progress



- Lack of understanding
- Manifests Complexity
- Delays in strategy and deployment
- Lack of Documentation
- Standards and Procedures are unclear or not created



Your files will be lost on :

**71 : 58**

[About bitcoin](#)

[How to buy bitcoins?](#)

[Contact Us](#)

## Oooooops All Your Files Are Encrypted ,NoCry

Can I Recover My Files ?

**Yes, You Can Recover All Your Files Easily And Quickly**

**But How ?**

**Send The Required Amount And  
I Will Send The Key To You For Decryption**

**See You Soon (0\_0)**



**Send \$100 worth of bitcoin to this address:**

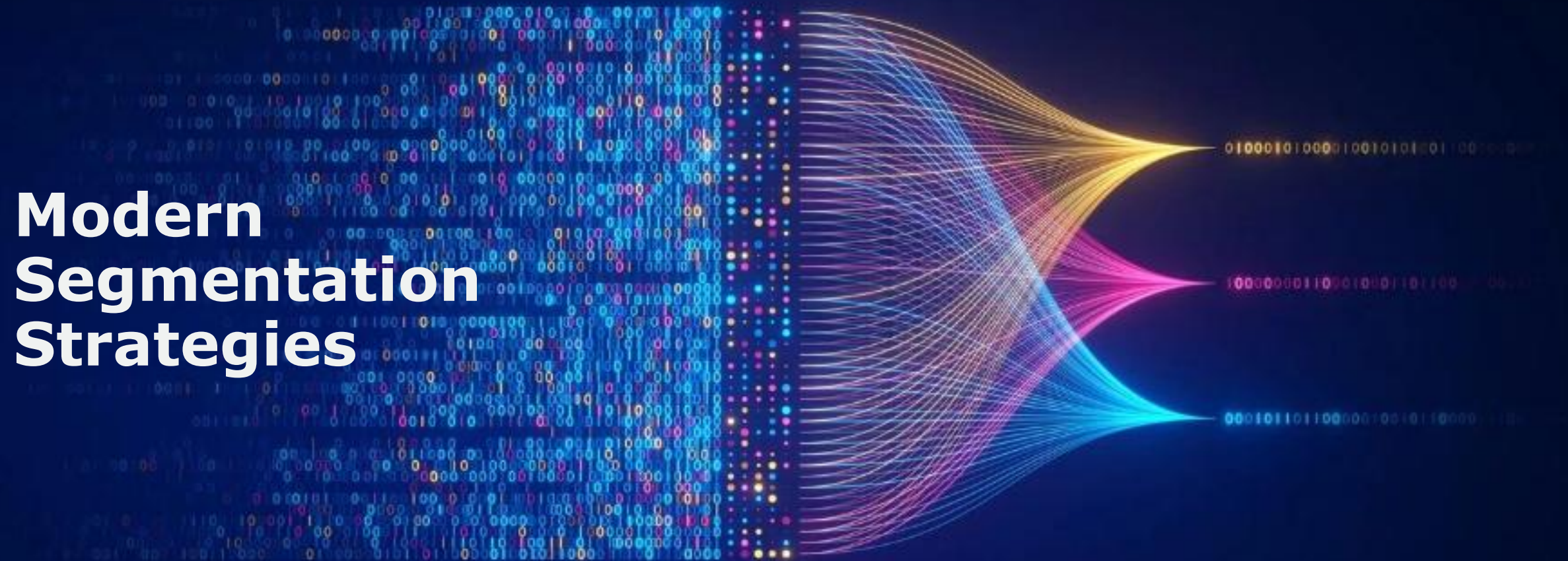
1LHaSk425DzEoR6dT8t6gc4wkoKnQ4iVwK

Copy

Show Encrypted Files

Decrypt

# Modern Segmentation Strategies





# The Need, Why Now?



	Likelihood of Threat		
	Low (0.1)	Medium (0.5)	High (1)
	Low-risk level (1)	Low-risk level (5)	Medium risk level (10)
	Low-risk level (5)	Medium-risk level (25)	High-risk level (50)
High (100)	Medium-risk level (10)	High-risk level (50)	Critical-risk level (100)
Medium (50)	Low-risk level (5)	Medium-risk level (25)	High-risk level (50)
Low (10)	Low-risk level (1)	Low-risk level (5)	Medium risk level (10)



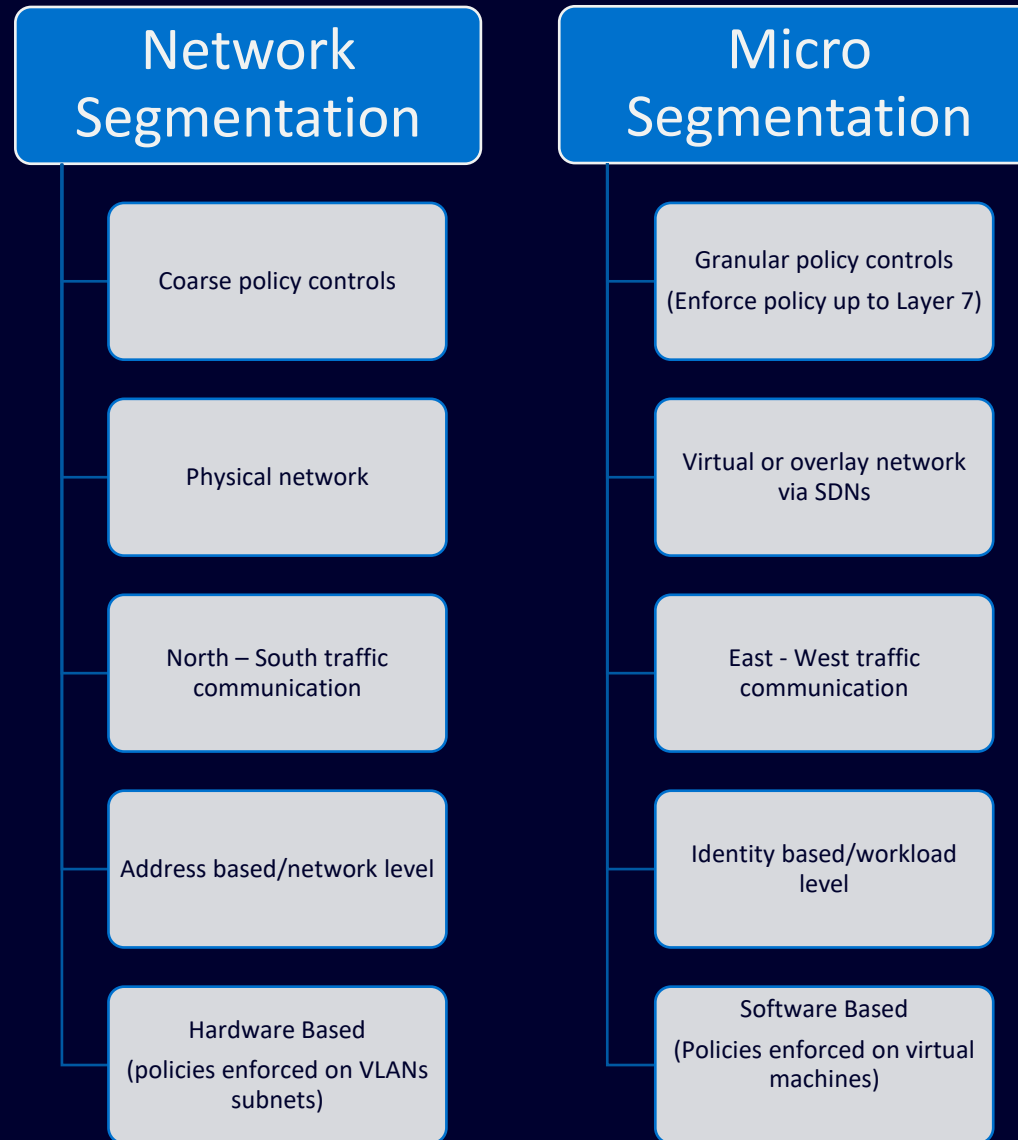
## Microsegmentation vs Zero Trust

Think of microsegmentation as a helpful tool that is part of the bigger Zero Trust security approach. Here's how they compare:

Aspect	Microsegmentation	Zero Trust
Focus	Isolating network segments	Verifying every user and device
Implementation	Granular policies for traffic control	Continuous verification of all entities
Scope	Network - centric	Holistic, including users, devices, etc..
Goal	Minimize lateral movement	Never trust, always verify

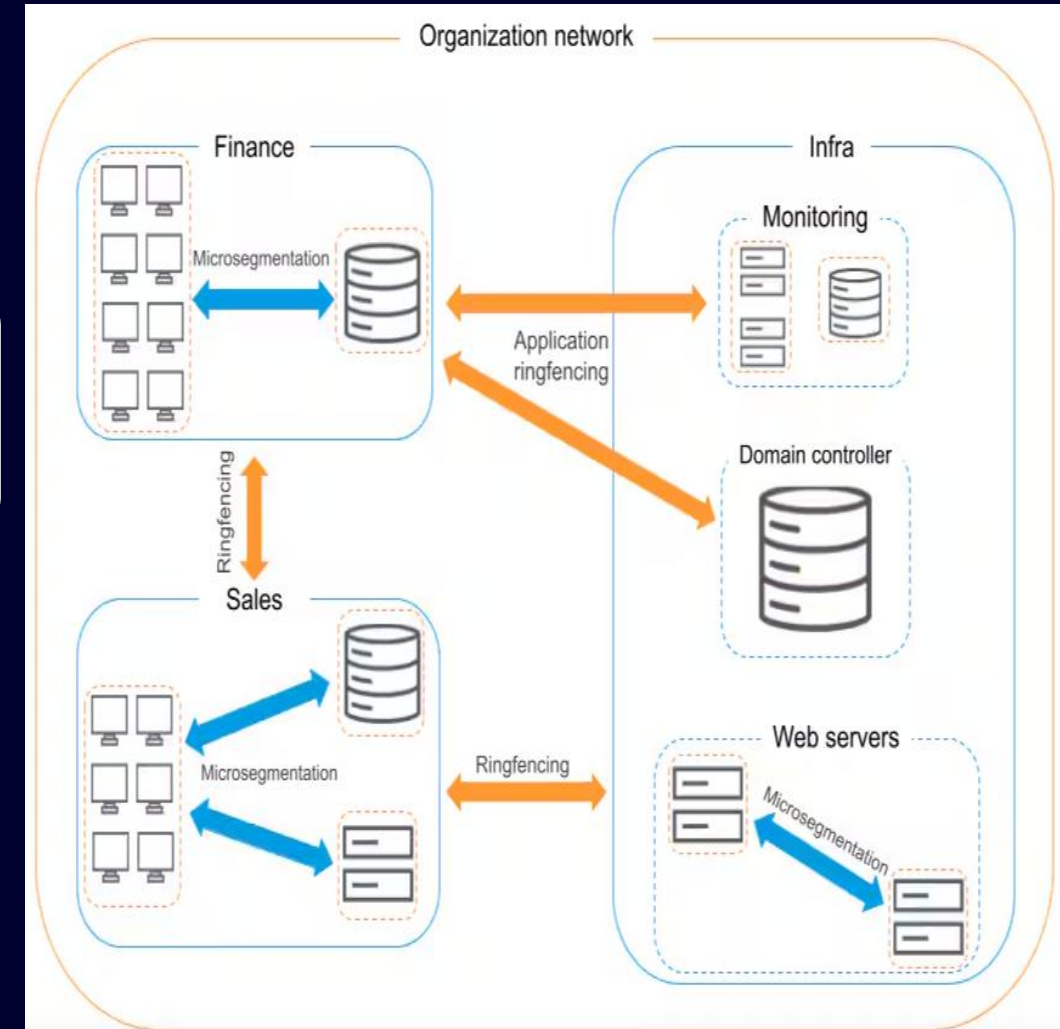
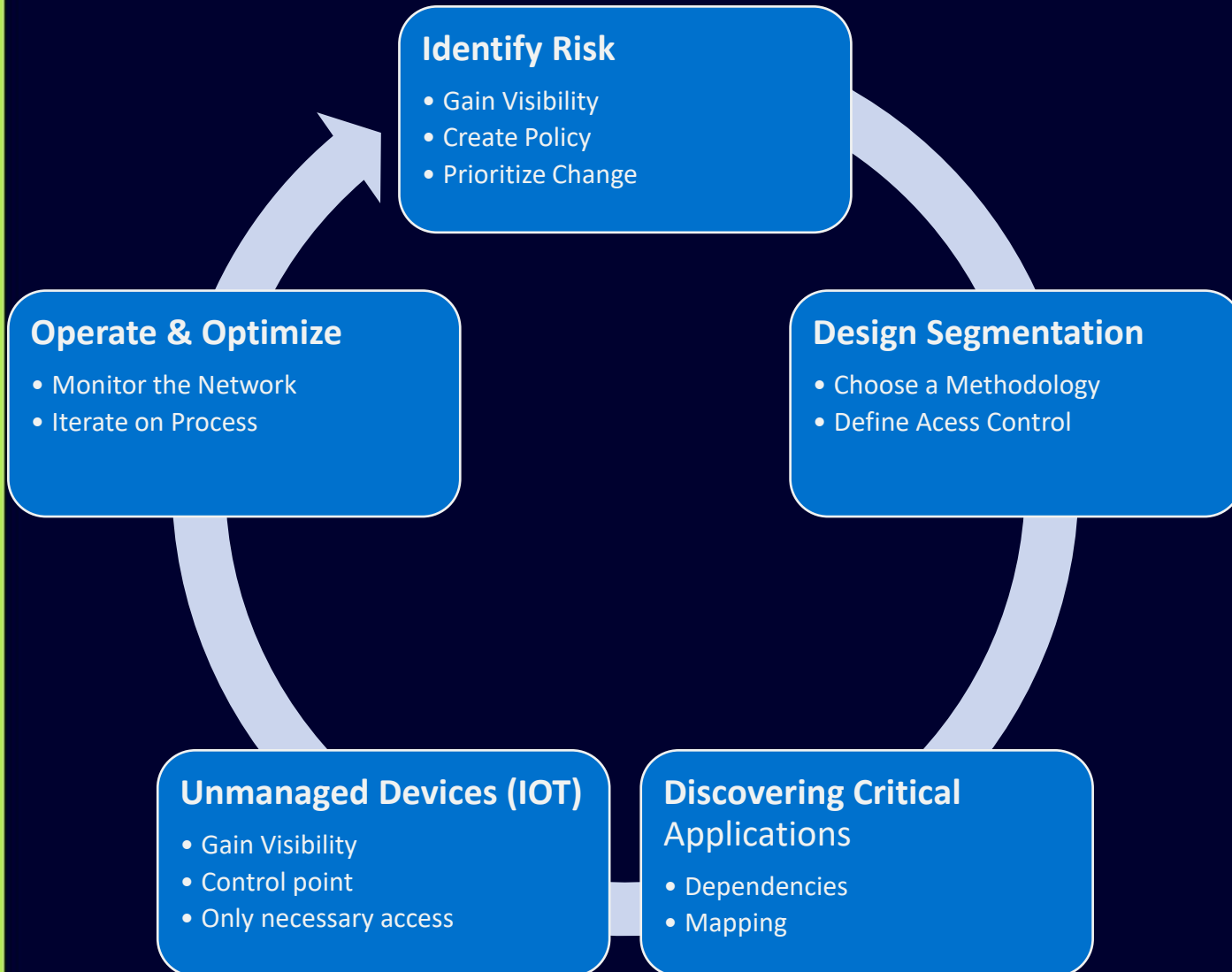
Microsegmentation works well with Zero Trust by focusing on network security, while Zero Trust covers a bigger overall security plan

# Network Segmentation vs Micro Segmentation





# Tackle segmentation as a program and not a project



# Benefits Gained Through Micro Segmentation

## Simplify Compliance

Map and isolate compliance related applications and systems. Granular visualization will help you understand how best to reduce the risk of breaches quickly

## Protect Essential Systems

**Separate critical applications such as money transfers, payments, and customer applications from the general IT infrastructure.**

## Stop Lateral Movement

Isolate IoT and third-party access. Manage access routes and terminate access at the target applications. Preventing further movement within the data center.

## Adopt Tech Securely

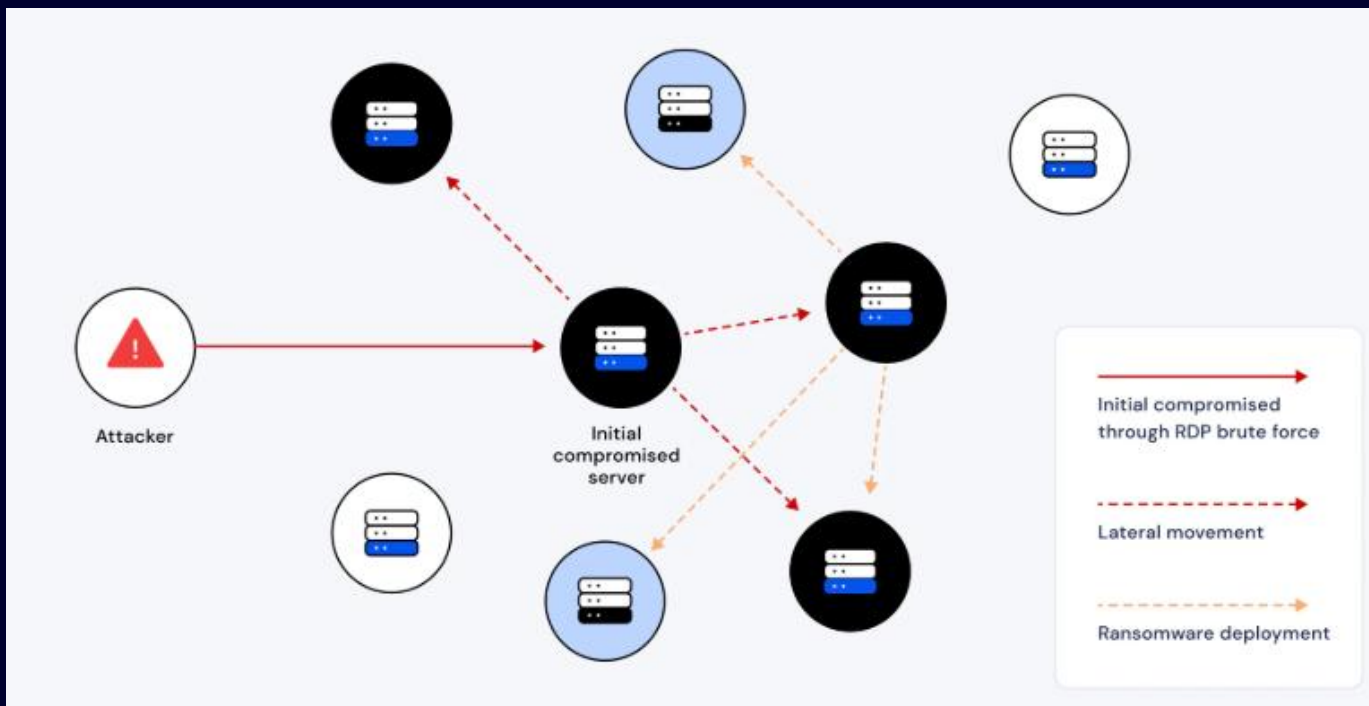
Use a single pane of glass for visibility and setting security policy across all infrastructure (Cloud, PaaS, etc.). Be sure you enforce security via a unified set of tools.



# Reduction Of the “Blast Radius”



According to [Forrester's latest analysis](#), in 2024, the top 35 global breaches alone **exposed more than 5.4 billion records**, and privacy violations related to this sensitive data **cost organizations US\$3.1 billion** in fines.



TRENDS REPORT

## Lessons Learned From The World's Biggest Data Breaches And Privacy Abuses, 2024

March 25, 2025

By Janet Worthington, Enza Iannopolo, Heidi Shey, Andras Cser, Alla Valente, Sandy Carielli, Allie Mellen, Madelein van der Hout with Amy DeMartine, Danielle Chittum, Peter Harrison

FORRESTER

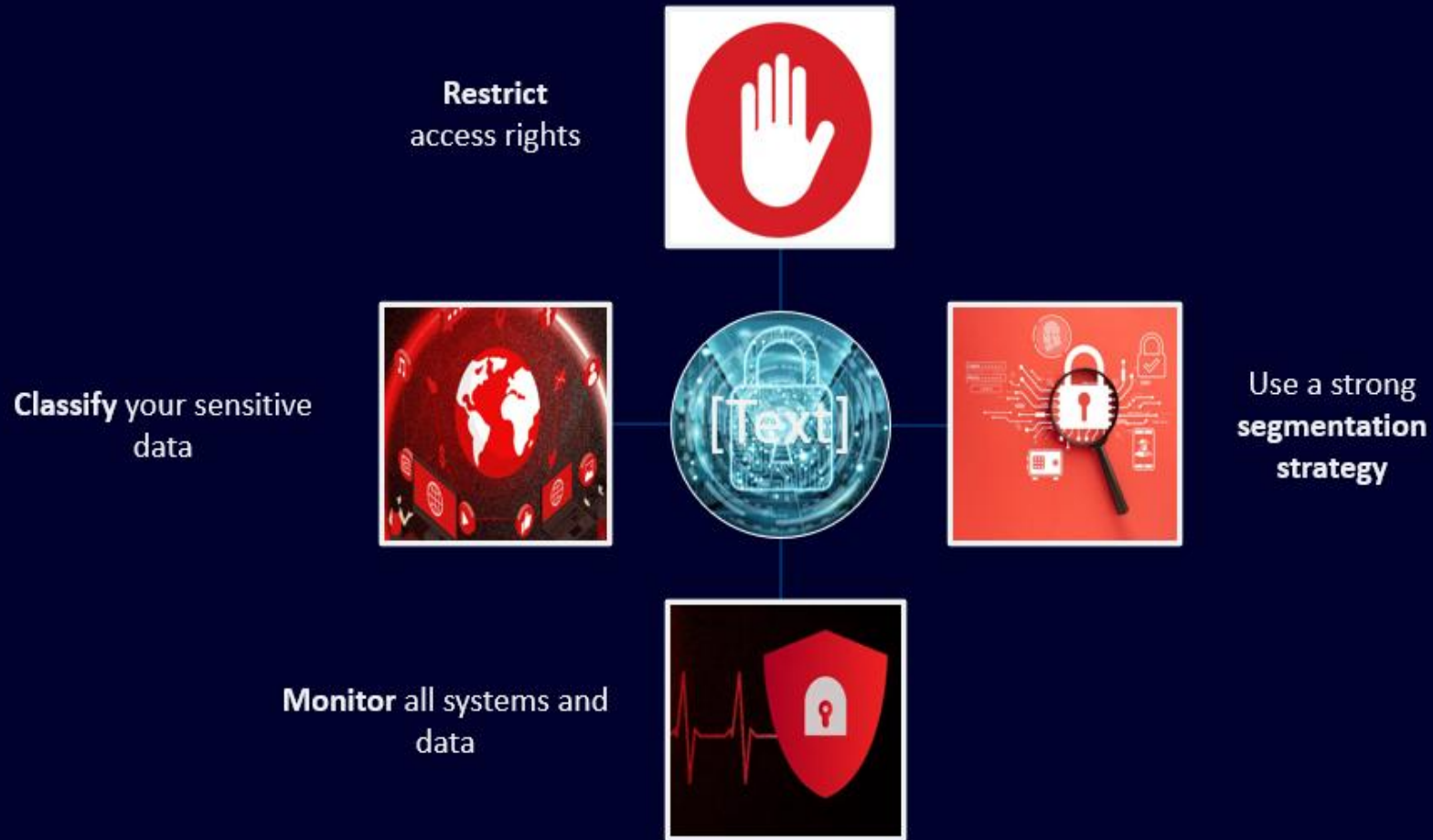
### Summary

Forrester analyzed the top global breaches and worst privacy abuses of 2024 and identified key trends and lessons learned. With more than 5.4 billion records exposed in the top 35 breaches alone and almost \$3.1 billion in fines levied on the top 35 violators — both up from 2023 — lessons abound for security teams. Security and privacy leaders should use this report to understand the key breaches and lessons from the past year and augment their security and privacy strategies accordingly.

© 2025 Forrester Research, Inc. All trademarks are property of their respective owners. For more information, see the [Privacy Policy](#), contact [support@forrester.com](#), or call +1 866-367-7378.



## Key concepts of reducing the blast radius



## Controlling Risk

- Avoid Risk
- Reduce Risk
- Risk Transfer
- Risk Confirmation
- Risk Containment
- Risk environment reevaluation

# Key Benefits of Micro-Segmentation Reducing The Blast Radius



## Breach containment

Implementing micro-segmentation prevents the lateral movement of attackers when they inevitably gain initial access. Each workload operates in its own secure enclave with granular control, dramatically limiting the blast radius of any compromise.



## Third-party risk mitigation

By segmenting third-party access and implementing least-privilege principles, organizations can continue to work with vendors like Snowflake or Fortinet while minimizing exposure if those relationships are compromised.



## API protection

Application-aware policies ensure that API communications follow predefined security rules, preventing the kind of unrestricted access that led to the Twilio and Dell breaches.



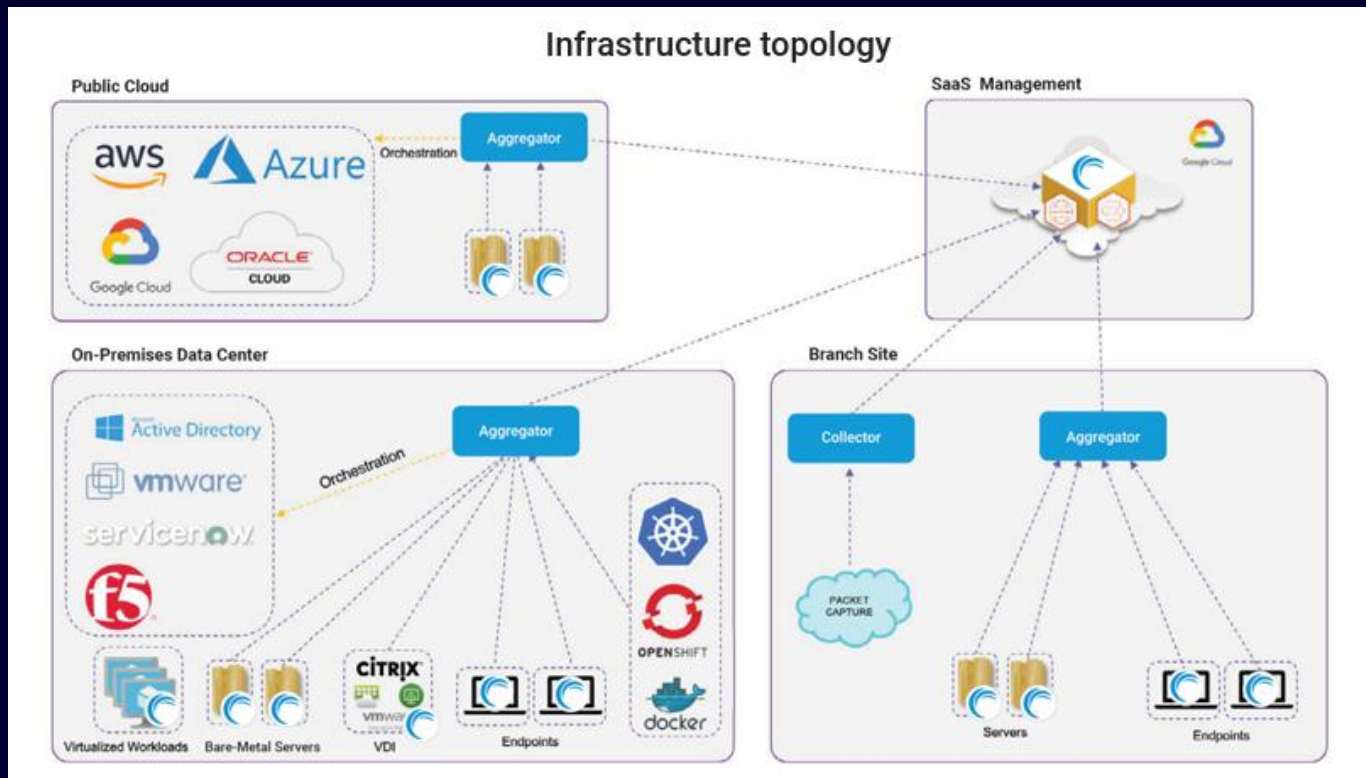
## Compliance support

The ability to demonstrate granular data protection controls becomes essential to help meet compliance and regulatory requirements.



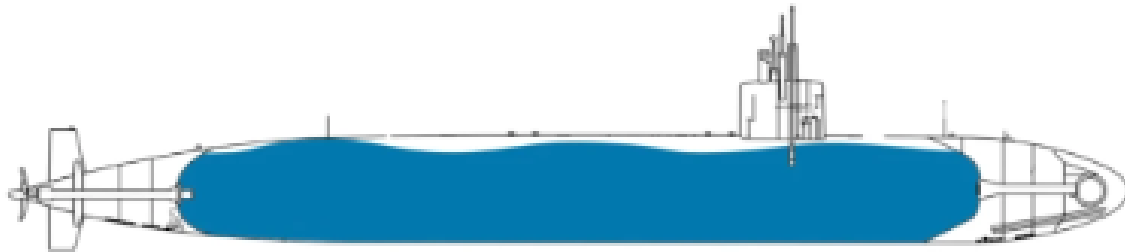
# Strengthen with Defense in Depth

**“CISA releases ‘Journey to Zero Trust’ series, guides federal agencies on micro-segmentation to boost adoption”**

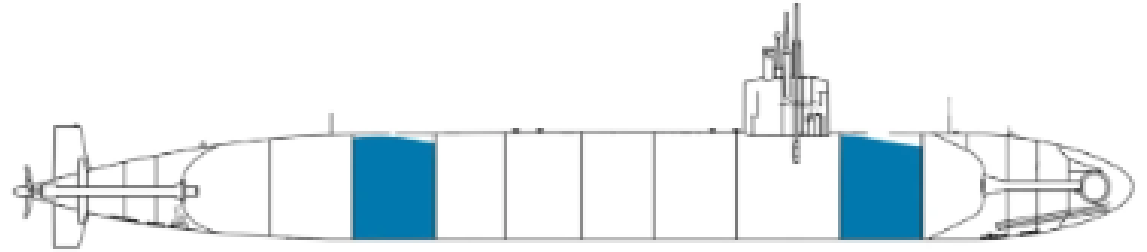


**The Need is now**

**Without  
Micro-Segmentation**



**With  
Micro-Segmentation**





**Thank you!**

---