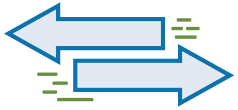
5 Steps to Leveraging Micro-Segmentation to **Build Zero-Trust Architecture**

Traditional Security Models **Are No Longer Enough**

If you're like most IT leaders, security and agility are at the top of your priority list. Unfortunately, the traditional security paradigm is too rigid and leaves too many gaps for you to achieve your security and agility goals.

Here's why:



Traditional models leave your East-West data center traffic exposed in the event of a perimeter breach.

Approximately 80% of data center traffic is East-West, yet 75% of organizations rely solely on traditional perimeter security.[1]

These models aren't strong enough to protect you from new, sophisticated threats like ransomware.

Seven out of ten targeted networks will be successfully infiltrated by ransomware attackers.[2]

They aren't flexible enough to secure a mobile-enabled network.

79% of companies admit securing mobile devices is becoming increasingly difficult.[3]

They create blind spots to your internal traffic…

58% of organizations have zero visibility into their East-West traffic.[1]

80% lack visibility into their unstructured data.[4]

…all of which lead you into creating one-size-fits-all security practices, insufficient compliance procedures and costly, labor-intensive management processes.

Almost half of organizations admit their security appliances don't extend to cover their mobility requirements.[5]

They present challenges to securing your cloud environments.

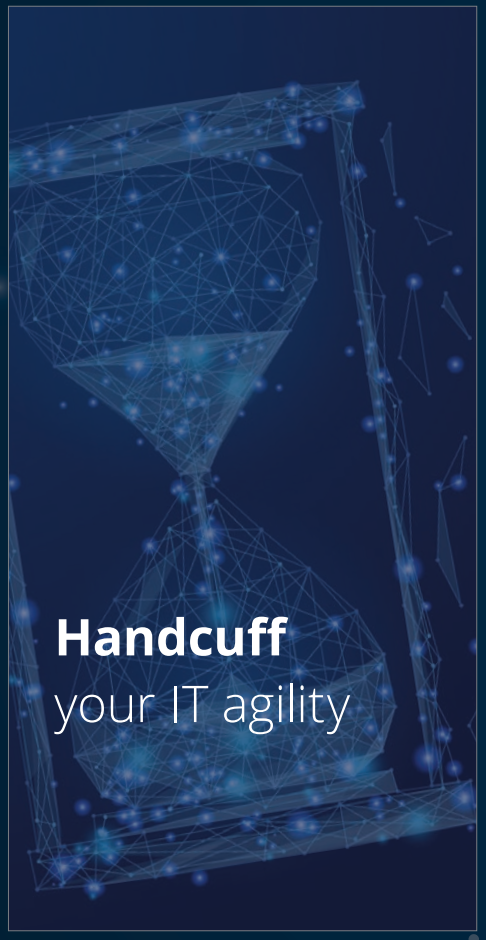
Nearly half of companies are delaying cloud deployments due to cybersecurity skills gaps.[6]

ConRes
CONTINENTAL RESOURCES

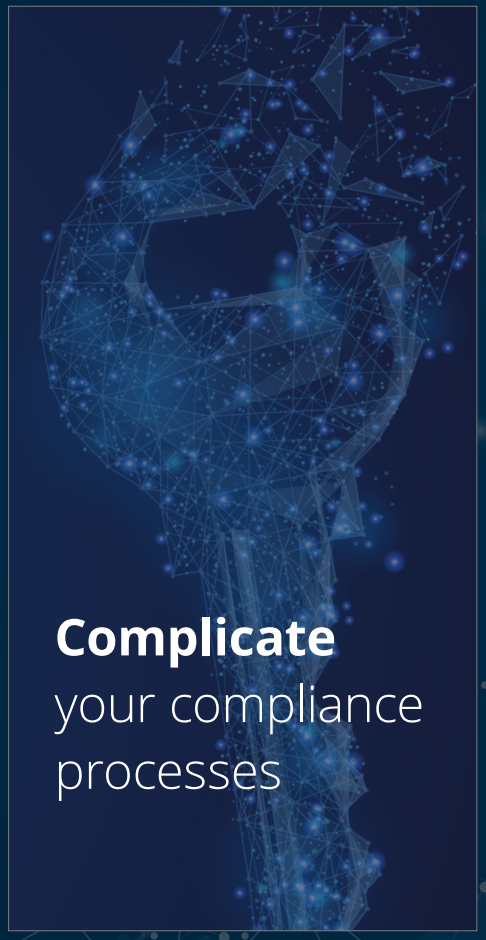
The **Bottom Line**

Traditional security models...

Inhibit
your security



Handcuff
your IT agility



Complicate
your compliance processes

Introduce
higher costs and greater complexities

So what's the solution?

Today's Networks Require **Zero-Trust Architecture**

Never Trust, Always Verify

The limitations of traditional security models combined with the onslaught of threats, concerns and vulnerabilities facing your staff leave you with only one solution — trust nothing.

Enter **Zero-Trust Architecture**.

Coined by John Kindervag, a former principal analyst at Forrester Research, the Zero-Trust architecture or Zero-Trust network operates under the assumption that no asset is safe within your network. While traditional "castle-and-moat" models focus on securing the perimeter of your network from external threats, Zero-Trust security models go a level deeper to secure the assets inside your network. That way, if your perimeter is breached or an insider threat pops up inside your data center, your applications, workloads and data remain protected.

The Goals of Zero-Trust Architecture

- Workload-centric security
- Increased network visibility
- Granular network control

Achieving the goals of the Zero-Trust model is driving many IT leaders to consider the technique of micro-segmentation.

> *"If I have 20 calls, 17 are about Zero Trust. CISOs, CIOs and CEOs are all interested, and companies of various sizes are interested... And in three years, I think Zero Trust will be cited as one of the big-time frameworks in cybersecurity. Period."*
>
> CHASE CUNNINGHAM, PRINCIPAL ANALYST, FORRESTER

Micro-Segmentation

/'mīkrō/ /,segmen'tāSH(ə)n/

noun

A security technique that enables organizations to logically divide the data center into distinct security segments down to the individual workload level, then define security controls and deliver services for each unique segment, thus enabling you to create and enforce a Zero-Trust security model across your network.

Why IT Leaders Use Network Micro-Segmentation:

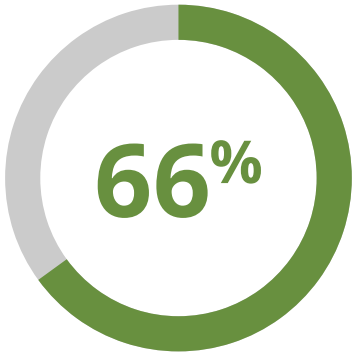
- To enable protection for their East-West traffic.
- To provide greater visibility and context for interactions between users, applications and data across the network.
- To create isolation between networks and workloads. In the case of network virtualization, these elements are isolated from physical infrastructure.
- To simplify the management and control of network security.

Comparing Micro-Segmentation **Implementation Methods**

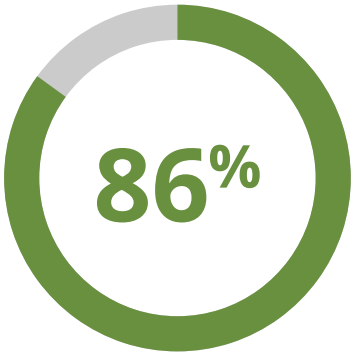
In the past, micro-segmentation was implemented using **traditional firewalls** to block or allow workload-level traffic based on established rules. This technique proved to be costly and time-intensive for your staff to manage. Not only does manually configuring firewalls around individual workloads get tedious and cumbersome as you add workloads and your network expands, but it also puts you on the fast-track to irreparable firewall sprawl.

Network virtualization enables a more scalable alternative to this "death-by-firewall" segmentation model. Through virtualization, you can define, manage and adjust workload-specific security policies from a single pane of glass at the hypervisor level instead of manually configuring them for each asset. Automation also lets you provision your Zero-Trust policies as soon as a workload is created, and those policies will travel with the workload as it moves throughout your data center, enabling increased IT agility and massive CapEx and OpEx savings. Micro-segmentation also enables you to secure your workloads as they move to and from the cloud.

Network virtualization and micro-segmentation have been proven to deliver:



*Up to **66% in CapEx savings**[7]*



*Up to **86% in OpEx savings**[7]*

ConRes
CONTINENTAL RESOURCES

Implementing Micro-Segmentation to **Achieve Zero-Trust Architecture**

Implementing micro-segmentation isn't as straightforward as its dictionary definition lets on. Not only are there a variety of ways to deploy micro-segmentation, but there are also a number of business and technical decision points to cover before you can even consider investing in a solution.

Here are the five steps to leveraging micro-segmentation to build Zero-Trust architecture:

1. Achieve Buy-In
2. Assess Your Workloads
3. Map Your Connections
4. Design Your Micro-Segmentation Strategy
5. Test, Validate and Deploy

1 Achieve Buy-In

Implementing micro-segmentation to create Zero-Trust is no different from any other business investment — it requires collaboration and unity at the top of the food chain. Be sure to communicate with all major stakeholders to establish the goals, expectations and guard rails for the project. This will likely involve communicating with decision-makers from different business functions, including IT, DevOps, operations and finance. The buy-in process is also a time to receive and respond to early feedback on your micro-segmentation plans and identify potential roadblocks in deployment.

Questions to Answer During this Step:

- Who needs to be involved at the decision-making level?
- What's the budget for the project and any ongoing support?
- What IT resources will we need to carry out our micro-segmentation strategy?
- What's the project timeline?

2

Assess Your Workloads

Next, you must differentiate your high-value, high-risk systems, applications and data from your lower-priority network assets. Doing this helps you prioritize efforts for your most critical assets. It also helps you start to define security requirements for these differing workloads. For most companies, high-priority assets include databases housing customer or personnel information, communication platforms used by staff and applications that enable specific business functions. You may also want to prioritize workloads that fall under industry compliance standards like PCI and HIPAA — micro-segmenting these workloads and applying stringent security profiles makes it easier to manage and automate compliance processes.

Questions to Answer During this Step:

- Which of my workloads are mission-critical?
- Which workloads have specific compliance specifications?
- Are these workloads on premises or in the cloud?
- Are any of these systems hosted in VMs?
- Do these workloads need to move to and from the cloud?

ConRes
CONTINENTAL RESOURCES

3

Map Your Connections

Now you can map the connections between your workloads, your users and the rest of your network environment. These connections carry communication to and from the servers within your data center, and they represent jackpots for attackers in the event of a perimeter breach. Infiltrating these East-West data paths is how attackers jump from server to server throughout your data center and gain access to your organization's most critical assets if micro-segmentation isn't in place. For this reason, it's essential that you understand which parts of your network are most connected, who needs access to what inside your data center and where micro-segmentation boundaries need to be established.

Questions to Answer During this Step:

- Who's accessing my critical workloads, applications and data?
- For what purpose are users accessing these workloads?
- What devices are they using?
- Where are these interactions taking place within my network?
- Where are their potential/current bottlenecks?

ConRes
CONTINENTAL RESOURCES

4

Design Your Micro-Segmentation Strategy

Set a starting point for designing your micro-segmentation strategy. Odds are your high-priority workloads will require more sophisticated segmentation than your lower-priority ones. Because of this, you may want to start the design process by addressing your mission-critical assets first then work down the ladder from there.

Questions to Answer During this Step:

- Where should my enclave boundaries be?
- Where are the endpoints?
- Will we require new hardware?
- How do we need to manage and administer our security policies across workloads?
- What role can automation play in our strategy?
- Are we able to secure workloads moving to and from the cloud?

ConRes
CONTINENTAL RESOURCES

5

Test, Validate and Deploy

Testing and validation is essential to deploying an effective micro-segmentation strategy. Micro-segmentation ignites a major evolution for your IT infrastructure and transforms the operations of your data center. It's critical you identify any technical glitches and points of failure early on so you can avoid expensive retroactive fixes down the road. This is where working with an expert third-party resource can pay dividends by offering you an objective, pull-no-punches view of your micro-segmentation strategy and how to optimize it.

Questions to Answer During this Step:

- How much work will the testing process add for our internal staff?
- Which of our systems will experience downtime during implementation?
- How are we managing disaster recovery and backups?

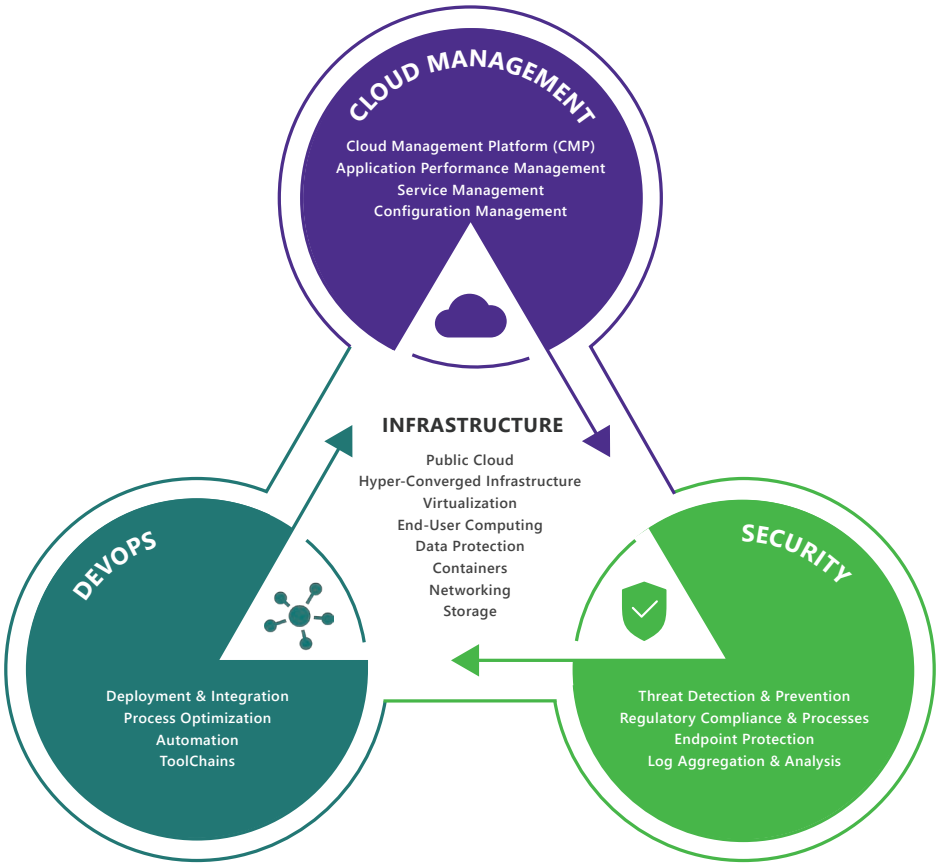
ConRes
CONTINENTAL RESOURCES

Zero-Trust & Micro-Segmentation:
A Match Made in Heaven

Given the velocity of today's cyberthreats and the dynamism of today's networks, the Zero-Trust security model is not a "nice-to-have" — it's a "must-have." Leveraging micro-segmentation enables you to implement a Zero-Trust architecture that meets your security and agility requirements, offering a solution that provides granular security and visibility of your workloads without handcuffing the flexibility and speed of your network.

How **ConRes Can Help**

ConRes is transforming the way enterprises approach IT service delivery. Backed by more than 50 years in business, ConRes combines industry-leading networking and security solutions like VMware NSX with a one-of-a-kind, structured approach to optimizing your IT infrastructure and enabling the software-defined data center (SDDC) at your organization.



As with most things in business, there is no one-size-fits-all solution. Using the ConRes Software-Defined Data Center (SDDC) Framework, we work closely with you to create a holistic solution that ensures every element of your infrastructure and services contributes to meeting the demands of your business. Along with your team, we complete a virtual network assessment to understand all traffic across your network. Next, we'll define a plan to gradually roll out micro-segmentation to different applications, testing and refining along the way. Although it is a staged implementation, you will start seeing the benefits of micro-segmentation right away as traffic and workloads become more visible.

As experts in IT and networking for more than 50 years, we offer leading virtualization solutions like VMware NSX to help clients address their security and networking concerns, including:

- **Protecting** East-West traffic
- **Reducing** costs and complexities
- **Meeting** compliance requirements
- **Improving** enterprise agility

Our team has earned more than 500 technology certifications and our configuration, testing and validation facility enables unparalleled validation of customer solutions in a live environment. Simply put, we offer the most advanced IT solutions delivered by the most experienced team while providing you with industry-leading personal service and support.

ConRes
CONTINENTAL RESOURCES

ConRes takes a comprehensive view of your technology environment to help make your IT more efficient, effective and simpler to manage. We have the expertise to design, test, implement and manage, combining flexibility and experience to create future-ready solutions for your organization.

800-937-4688 | www.conres.com

[1]Illumio. Best Practices to Contain Cyberattacks.

[2]Crowe, J, 2016. *Cyber Attack Statistics: Majority of Victims Aren't Changing Their Security in 2017.* Barkly.

[3]Dimensional Research, 2017. *The Growing Threat of Mobile Device Security Breaches: A Global Survey of Security Professionals.*

[4]Ciklum, 2017. *Big Data and the Challenge of Unstructured Data.*

[5]Cato, 2016. *Top Networking and Security Challenges in the Organization: Planned Network Investments in 2017.*

[6]McAfee, 2018. *Navigating a Cloudy Sky.*

[7]VMware, 2016. *Why Businesses Are Adopting Network Virtualization.*