ditno.

Security made simple.

MICRO-SEGMENTATION

TABLE OF CONTENTS

INTRODUCTION

Senior executives and board members have started to realise their organisation needs to approach IT security differently. Their current solutions limit innovation, lack flexibility and scalability and do not provide the necessary insights and controls to protect their critical information assets. More importantly, their strategy demands a compliance-centric and risk-centric approach, allowing them to detect control breakdowns in real-time and having the ability to timely respond to a threat.

What is micro-segmentation?

Traditional firewalls are designed to inspect and secure traffic coming into an environment - north-south direction. Micro-segmentation provides greater control and visibility over the growing amount of east-west traffic across the organisation which bypass the traditional firewalls.

The aim of micro-segmentation is to apply Zero Trust security controls around the individual IT service workload. Managing controls at a micro level, prevents unauthorised lateral movements between servers - only explicitly permitted flows are allowed. As a result, if a breach does occur, the initial compromised device has limited access to other devices and is restricted from lateral movement exploration.

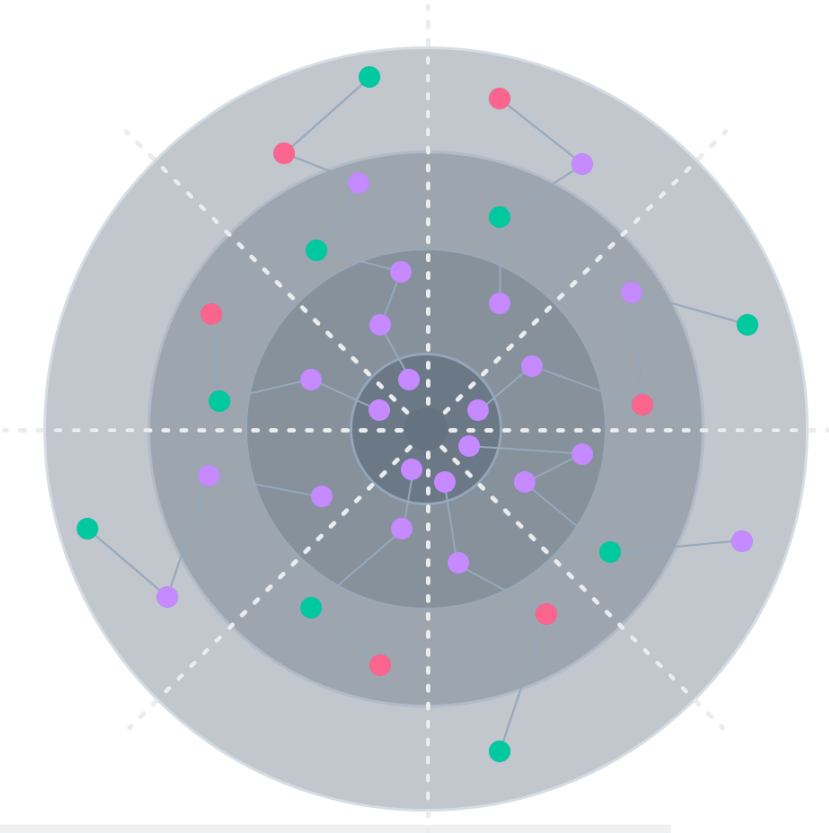
The first step of defining micro-segmentation controls is to understand the current environment and map application dependencies. This task will not be easy as many enterprises lack this visibility.

The next challenge is to deploy several security devices and apply necessary network controls to restrict access to each workload.

Using traditional strategies like physical firewalls and VLANs would be costly and time consuming.

ditno combines the power of software and data science to discover, visualise and build workload-based security controls to create a Zero Trust network, which significantly reduces costs while increases operational efficiencies.

Fine-grained controls to isolate individual IT service



Is micro-segmentation effective

Micro-segmentation is now considered an essential security strategy, organisations should not automatically trust anything inside or outside perimeter- protection per workload.

Organisations have been trying to manage their IT service risks, which has proven to be complex, expensive and an operational burden.

Due to the amount of controls required to implement micro-segmented network, it has been difficult to assess how effective the segmentation controls are.

If one sensitive segment is allowed access to untrusted segment, what risk does this present to the organisation? More importantly, how would this be detected?

A network is only as strong as the weakest link and a single data breach may have devastating consequences to an organisation.

Micro-segmentation has been proven to be one of the most effective strategies to protect against cyber threats. However, the key to success is to ensure each control aligns to the corporate risk and compliance framework.

Micro-segmentation is now a popular security strategy, but is there a weakest link?

Ensure effective controls with real-time governance

Senior management needs to ensure the organisation has a clear set of approved network governance policies and standards, which is followed by its cybersecurity team to ensure all controls align with the governance model and eliminate non-compliant controls.

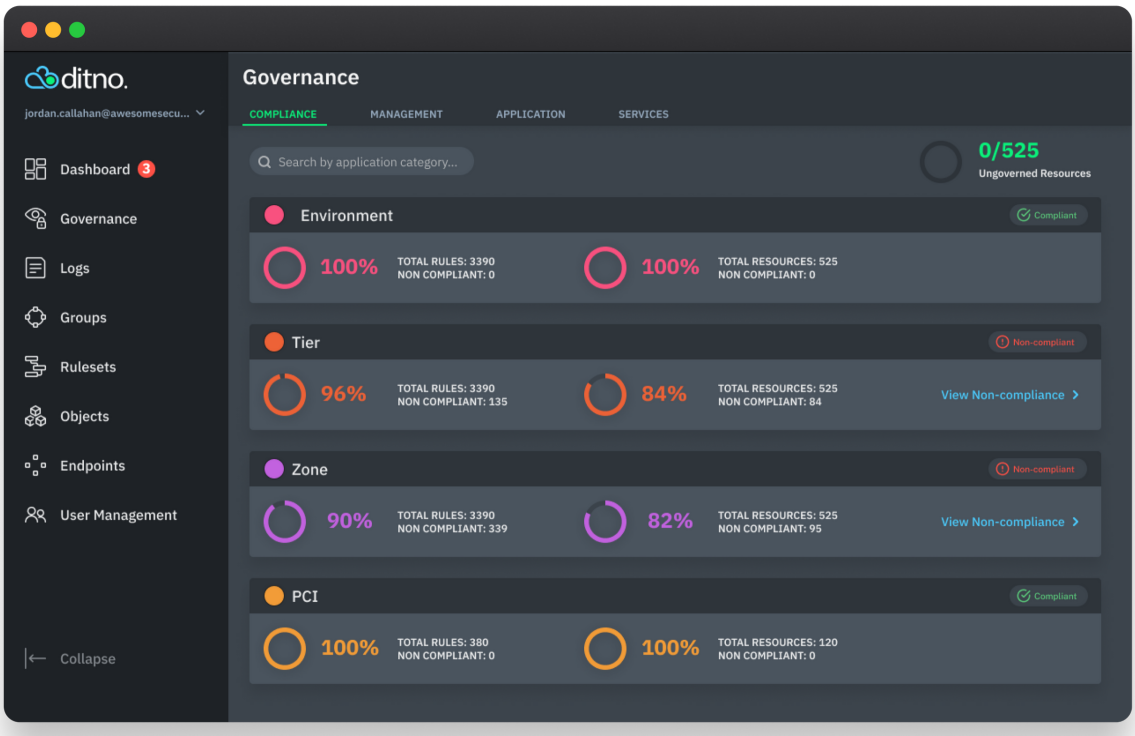
No matter how many segments and controls have been created, if they cannot be assessed and compared to the governance model, how is anyone sure they are designed correctly and operating effectively?

An organisation needs to have the ability to identify the purpose of all connected devices, the risks and importance they present to the business and how they should be protected.

Unified network governance

ditno provides a single unified management portal to create customised governance models, according to the business requirements and risk appetite, and create micro-segmentation across an Enterprise.

Non-compliant controls can be detected across Hybrid hosting environments. A single view of Enterprise risks is invaluable, every change can be assessed to ensure an acceptable risk appetite is maintained.



Have a question?

If you have any questions or want to learn more, contact us via ditno.com or send an email to info@ditno.com. We look forward to hearing from you!