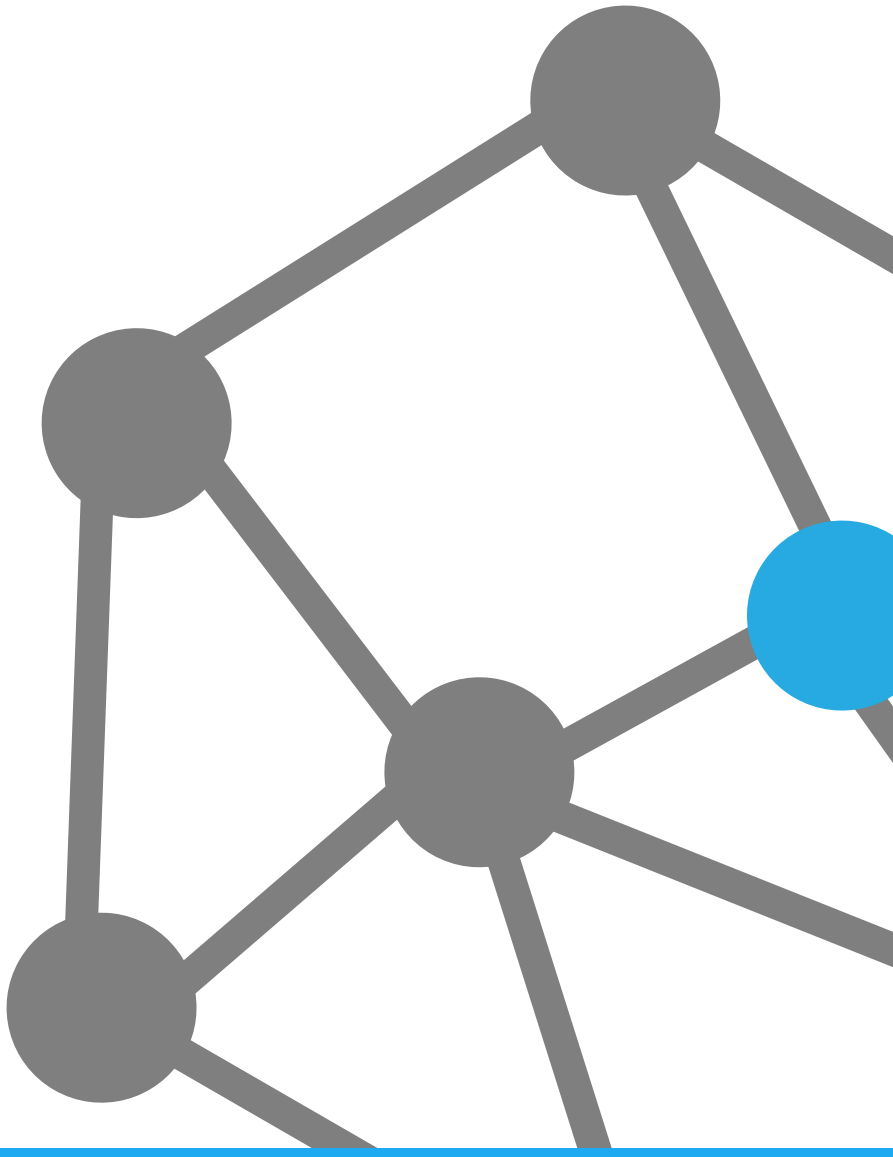
ditno.

White Paper January 2019

Importance of real-time Network Governance with Micro-segmentation



Contents

Introduction

Senior executives 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 insight and control to protect their critical assets. More importantly, their strategy demands a compliance-centric or risk-centric approach, allowing them to identify risks in real-time and having the ability to easily respond to a threat.

Is micro-segmentation effective

Micro-segmentation is now a popular security strategy, organisations should not automatically trust anything inside or outside its perimeter – protection per workload.

Organisations have been trying to manage their IT Service risk posture for years, it 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 very difficult to assess how effective the segmentation controls are.

For example, if one sensitive segment is allowed access to untrusted segment, what risk does this present to the organisation? More importantly, how would this be identified?

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

Micro-segmentation has been proven to be one of the most effective strategies to protect against 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 is following a clear set of approved network governance policies and standards. When a clear set of standards have been created, it makes the cybersecurity team objective easier – try to ensure all controls align to the governance model and focus and eliminate non-compliant controls.

No matter how many segments and controls have been created, if they cannot be assessed and compared to a governance model, how does anyone know they are correct?

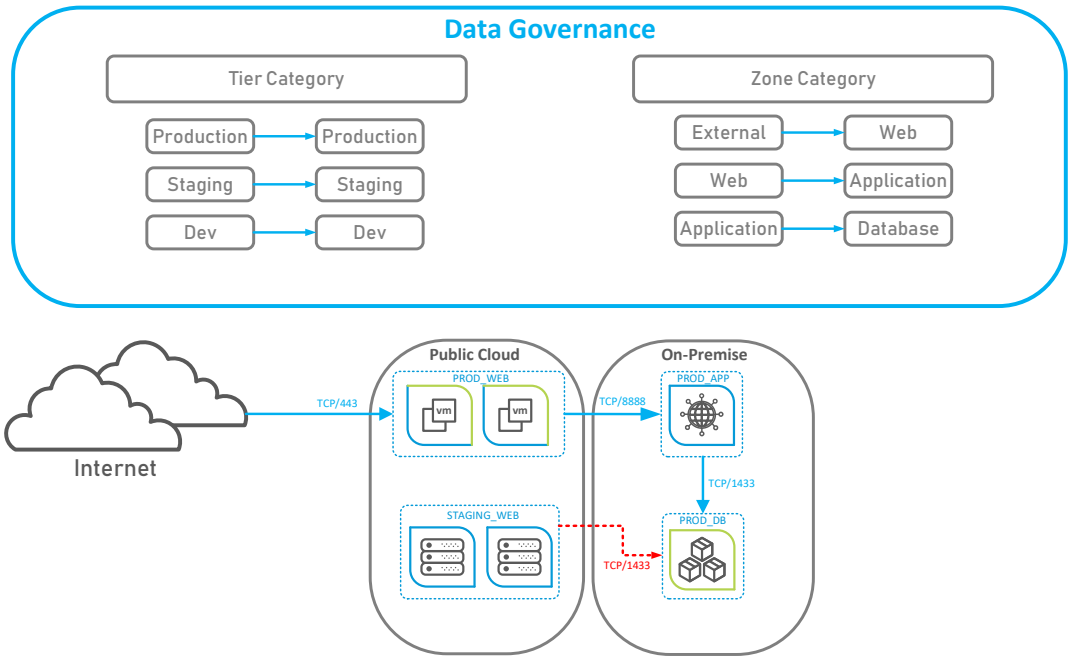
An organisation needs to have the ability to identify the purpose of all connected devices, the risk and importance they present to the business and how they should be protected.

Ditno unified network governance

Ditno provides a single management portal to create micro-segmentation across an Enterprise. More importantly, the same management portal provides the ability to create customised governance models according to the business requirements and risk appetite.

Users can easily analyse and identify non-compliant controls across all hosting environments which assists with secure transformation activities. A single view of Enterprise risk is invaluable, every change will be assessed to ensure an acceptable risk posture is maintained.

The below figure depicts a non-compliant flow between staging and production devices:



If you have any questions or need more information, please contact us at: **www.ditno.com**