



Security made simple.



UNIFIED NETWORK GOVERNANCE

TABLE OF CONTENTS

Defining a Network Governance Model	2
Introduction	2
Applying security controls without governance is not effective	2
Implementing Network Governance	3
Governance model	3
Compliance categories and tags	3
Building a secure baseline	4
Endpoint telemetry	4
Endpoint trust groups	4
Automated rule building	4
Compliance	5
Compliance summary	5
Compliance category	5
How can ditno make security simple	6
Centralised management	6
Network security guidelines	6
Automation	6
Real-time compliance	6

DEFINING A NETWORK GOVERNANCE MODEL

Introduction

Organisations should adhere to a set of corporate policies and standards. However, creating a policy is one thing but having the ability to prove and maintain compliance is another. For example, do you know what can connect to your critical services and the risks it presents to your organization?

This paper will explain how ditno transforms an open network into a compliant Zero Trust Network.

Applying security controls without governance is not effective

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

Many organisations have opted for perimeter firewalls, internal firewalls and VLANs to reduce risk exposures across services. It has been very difficult to assess how effective the segmentation controls are. More importantly, they are static. do not protect every device and cannot be transferred to public cloud.

Zero Trust is now a popular security strategy, organisations should not automatically trust anything inside or outside perimeter.

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

A horizontal blue bar.

Zero Trust is now a popular security strategy, but is there a weakest link?

A large, stylized graphic consisting of several overlapping, rounded, teardrop-shaped loops. The top loop is grey, the middle loop is blue, and the bottom loop is grey.

IMPLEMENTING NETWORK GOVERNANCE

Governance model

Before installing any endpoint software, ditno's management portal enables organisations to implement strategic governance models.

These models are based on independent compliance categories which provide guidance to every security control created within the system.

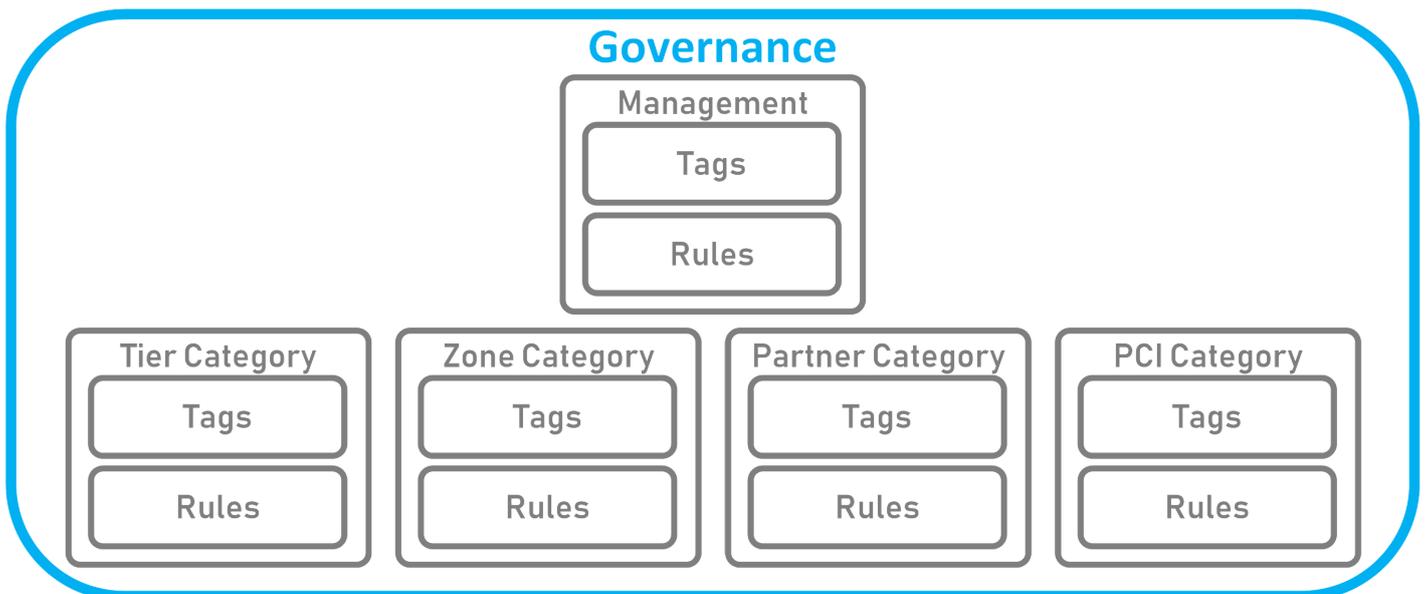
More importantly, it provides real-time visibility and identification of risk events.

Compliance categories and tags

Categories are configured using resource tags and compliance rules. An organisation can create a number of categories to meet their compliance requirements.

Once a category has been defined, resources are tagged and compliance rules are created between those tags e.g Application -> Database.

The following diagram is an example of a network governance structure:



BUILDING A SECURE BASELINE

Endpoint telemetry

Endpoint telemetry provides visibility and understanding of IT service relationships and dependencies. Each host-based network firewall contributes to a holistic picture of the network, combining these logs reveal the current IT landscape.

Endpoint trust groups

ditno's machine learning techniques can visualise endpoint connectivity and behavioral patterns. These patterns help identify the correct trust group for each endpoint.

After a few clicks, an entire network will be micro-segmented. These groups can then be tagged with the appropriate governance tags. This immediately creates meaning and allows the system to automatically assess every security rule created within the system.

Compliance Assurance is now active.

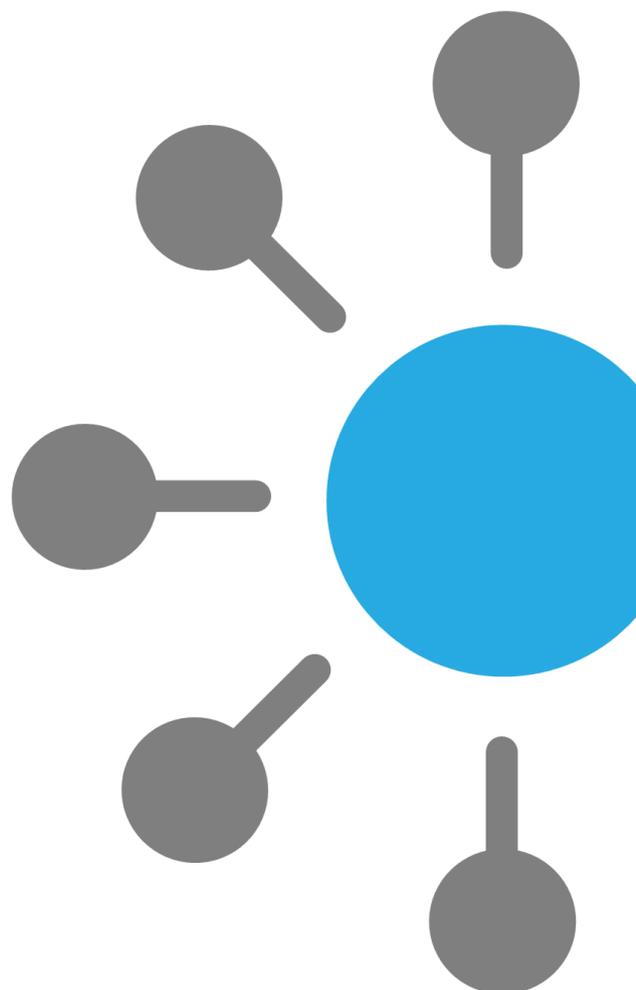
Automated rule building

One of the biggest challenges of building a Zero Trust Model is getting started.

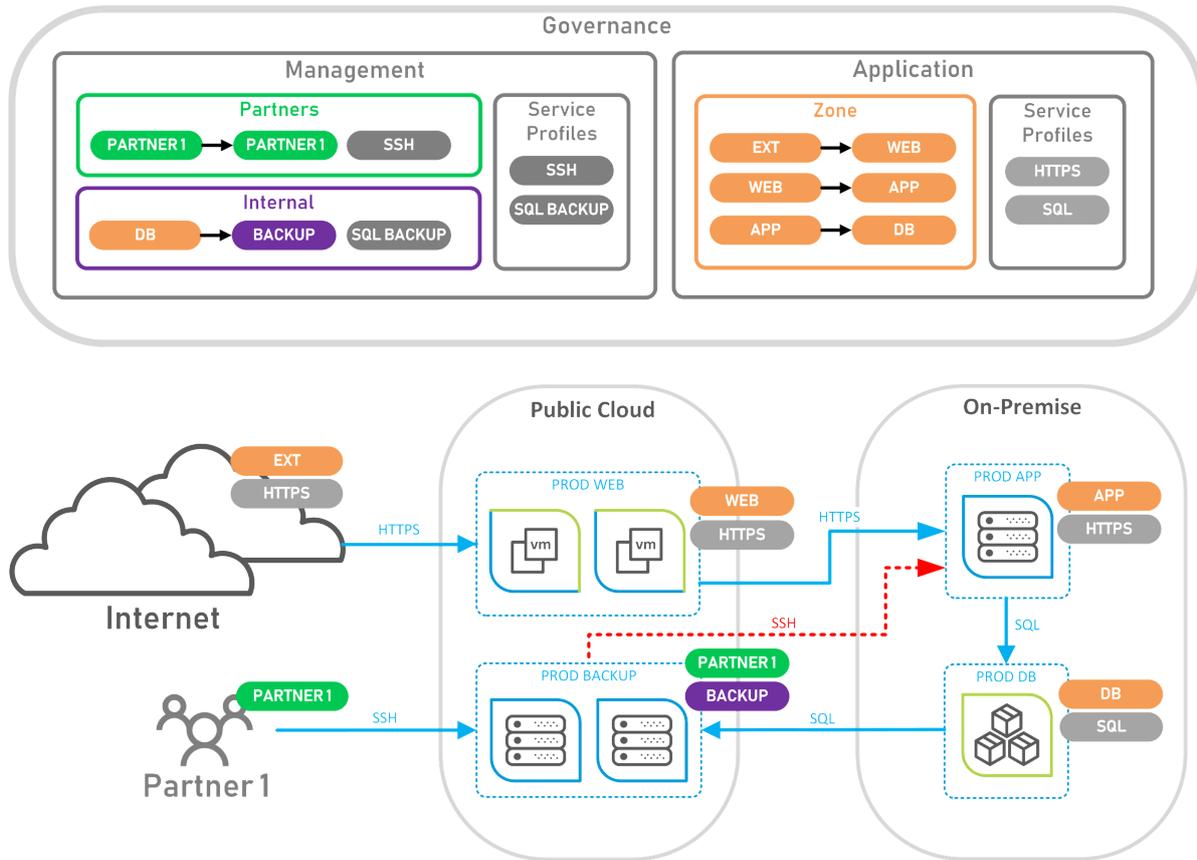
ditno's machine learning algorithms makes this easy. The system will learn application dependencies and build the necessary security rules required within your current environment.

This does not mean every rule will be compliant, it will however, ensure there is no IT service outage while building the rules. Once the base rules have been built, you will be able to identify and manage all non-compliant rules currently required throughout your environment e.g External devices can access your crown jewels.

Isolation of your systems is one of the best countermeasures to data breaches



COMPLIANCE



Compliance summary

ditno provides a single view to easily analyse and identify non-compliant network security configuration. This view is consistent across all hosting environments and assists with secure transformation activities.

Compliance category

If a category is non-compliant, you can drill into the specific category to identify non-compliant tag pairs, then the system will list the exact rules permitting non-compliant flows.

A single view for Enterprise risk exposure is invaluable. Every change, regardless if it's a new, updated or decommissioned service, will be automatically monitored to ensure an acceptable risk exposure is maintained.

HOW CAN DITNO MAKE SECURITY SIMPLE



Centralised management

Harmonise security controls and governance from a centralised management platform. Manage endpoint firewall security controls from a single unified platform streamlines IT service delivery. Provide full visibility and control to manage organisational risk effectively.



Network security guidelines

Create strategic network security guidelines, specifically for high risk applications, so the organisation has the ability to rapidly innovate and progress without jeopardising stability and risk.



Automation

Enable an organisation to quickly build a secure baseline by using the power of data and machine learning techniques. Understand application dependencies and weaknesses to ensure business continuity and stability.



Real-time compliance

Evaluate each network security rule in real-time to ensure it adheres to the organisation's compliance requirements and risk appetite. The compliance report will highlight configuration items which deviate from the governance model and allow the organisation to quickly take corrective actions.



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!