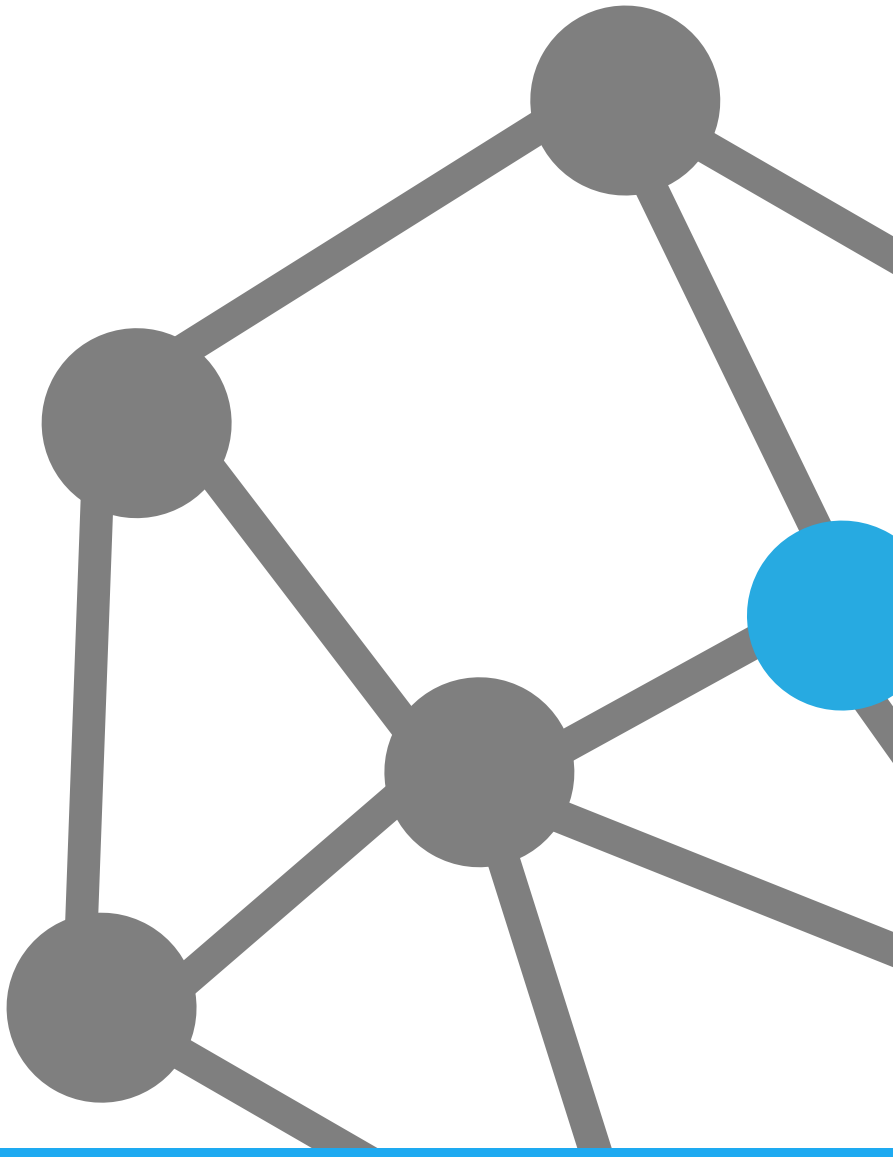
ditno.

Governance White Paper

Unified Network Governance



Contents

Defining a Network Governance Model

Introduction

Most 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 organisation?

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 risk posture for years, it has proven to be complex, expensive and an operational burden.

Many organisations opted for perimeter firewalls, internal firewalls and VLANs to mitigate risk exposure across services. It has been very difficult to assess how effective the segmentation controls are. More importantly, they are very 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 its perimeter.

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

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

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.

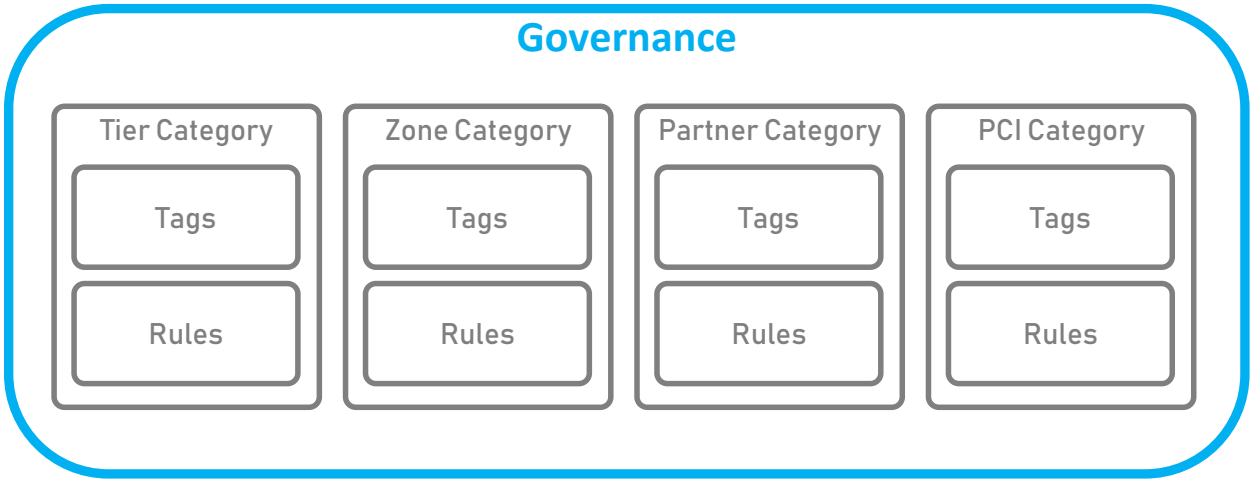
More importantly, it provides real-time visibility and control of risk exposure.

Compliance Categories and Tags

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

Our 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 against 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.

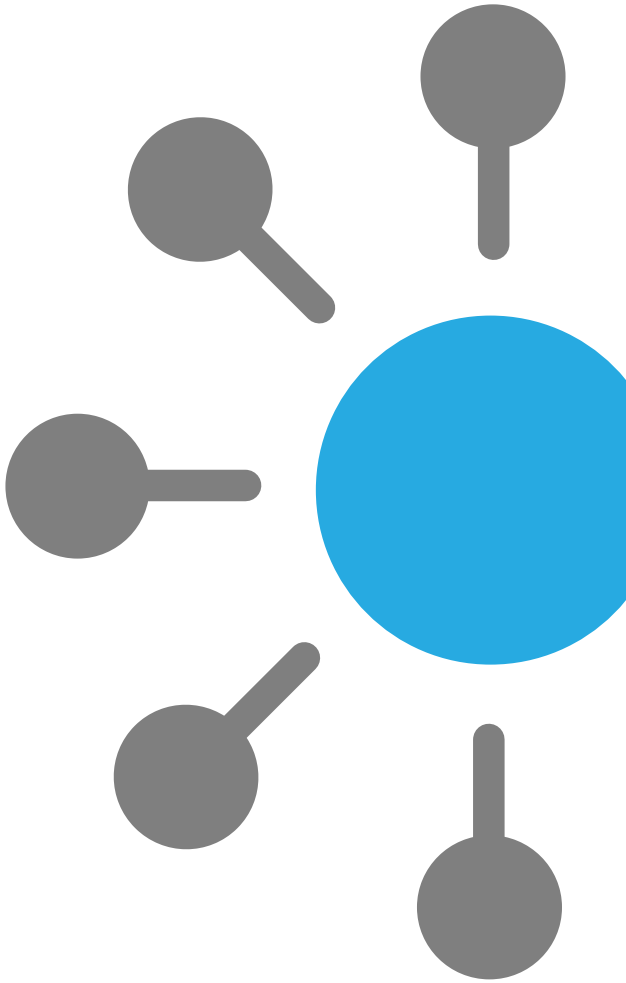
Automated Rule Building

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

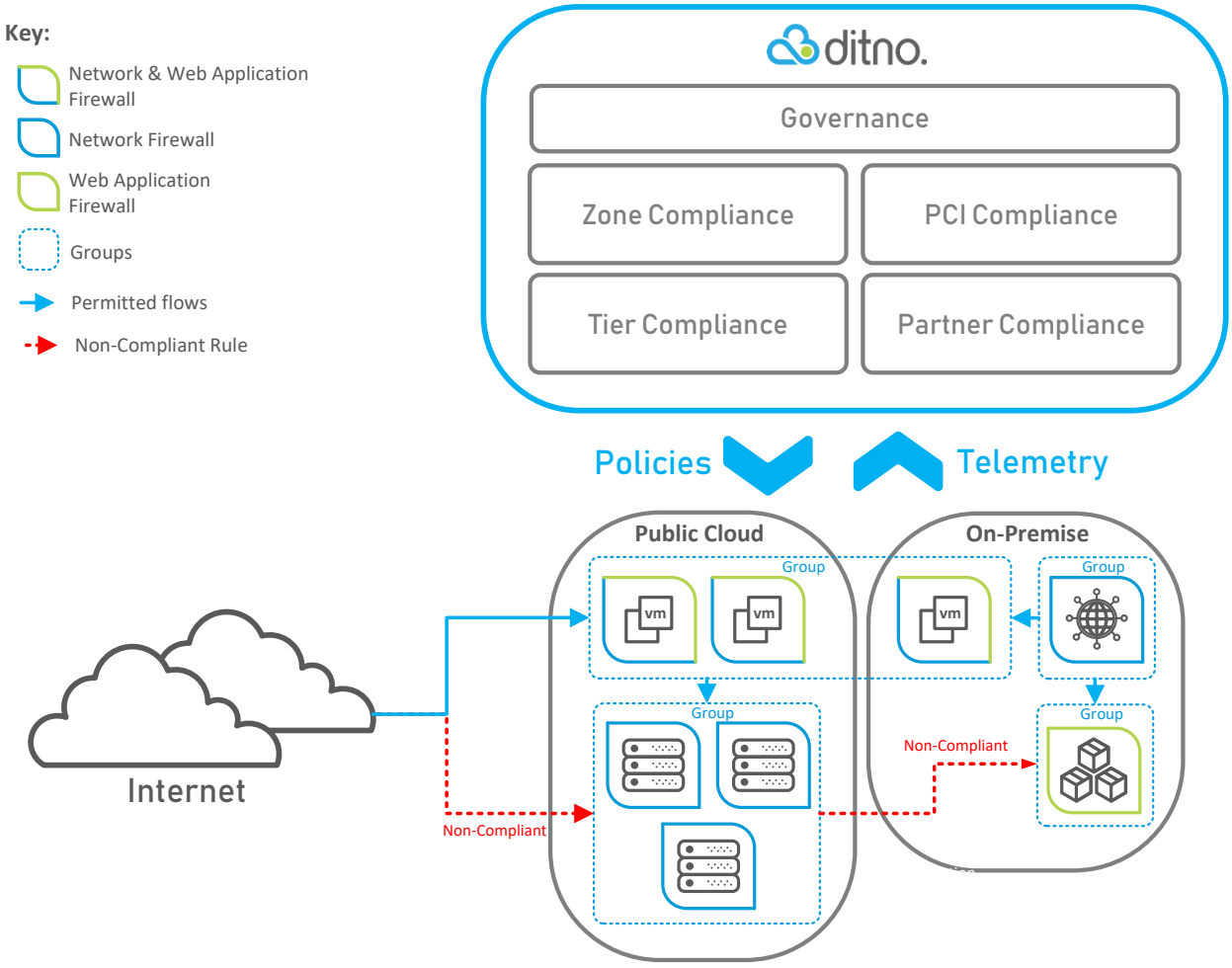
ditno's machine learning algorithms makes this easy. The system will learn application dependencies and build the necessary security rules required within your current environment.

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 page to easily analyse and identify non-compliant categories. This view is consistent across all hosting environments and assists with secure transformation activities. For example, you will maintain the same risk during public cloud migrations.

Category Compliance

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

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

Conclusion

Centralised Management

Managing endpoint firewall security controls from a single unified platform streamlines IT service delivery. It provides full visibility and control to manage organisational risk effectively.

Governance

The governance function is abstracted away from the security control function, providing clear separation of duties. Governance rules can be created, changed and analysed without affecting the underlying security controls.

Automation

Using the power of data and machine learning techniques enables an organisation to quickly to build a secure baseline using a Zero Trust Model.

Real-time compliance

ditno compliance evaluates every network security rule in real-time to ensure it adheres to the individual compliance categories.

The compliance report will highlight any configuration item deviating from the governance model and will allow the organisation to quickly take corrective actions.

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