ditno.

WHITEPAPER

Managing IT security risk with unified network governance

Increasing complexity makes it harder to protect the organisation's network

As organisations continue to digitally transform, protecting the network, data, assets, and systems grows in importance. The digital experience offered by an organisation can be a key competitive differentiator for its customers and its employees. However, IT networks are no longer contained within a set of easily defined firewalls and boundaries. Networks are rapidly becoming more dispersed with hundreds if not thousands of devices that are no longer constrained by perimeter protections.

As businesses move to the cloud, it can become even more challenging to gain an accurate and overarching view of the network and the interconnected devices. Given that it's impossible to secure what can't be seen, this presents an immediate and critical threat for businesses.

Many organisations look to solve these issues with various endpoint protection and siloed IT security solutions. This approach may provide a short-term fix for a specific problem but it rarely addresses the overarching challenge, which is to protect a distributed and growing network. Organisations need to approach this conundrum from an entirely different angle. Instead of plugging gaps as they emerge, businesses can prevent those gaps from emerging in the first place.

This can be done through network governance. This whitepaper will explore the concept of network governance and discuss how a unified network governance solution can help businesses strengthen their cybersecurity posture not just in response to specific threats but for the long term.

ditno.

Defining network governance

At its heart, network governance is a set of corporate policies and standards that determine how the network should be managed. This can include elements such as the security controls for connecting devices to the network, the access provided to various users, how the network is segmented, and more. Network governance policies should be developed according to the organisation's unique IT security requirements, risk tolerance, and potential threats. This means that no two network governance strategies are exactly alike.

Network governance is a tool that can determine which IT security solutions are appropriate for the business and how they should be configured. Essentially, it's a set of rules that everyone must play by. A unified network governance solution offers a simple and powerful way to ensure that all security controls in the organisation are compliant to reduce the attack surface and network exposure.

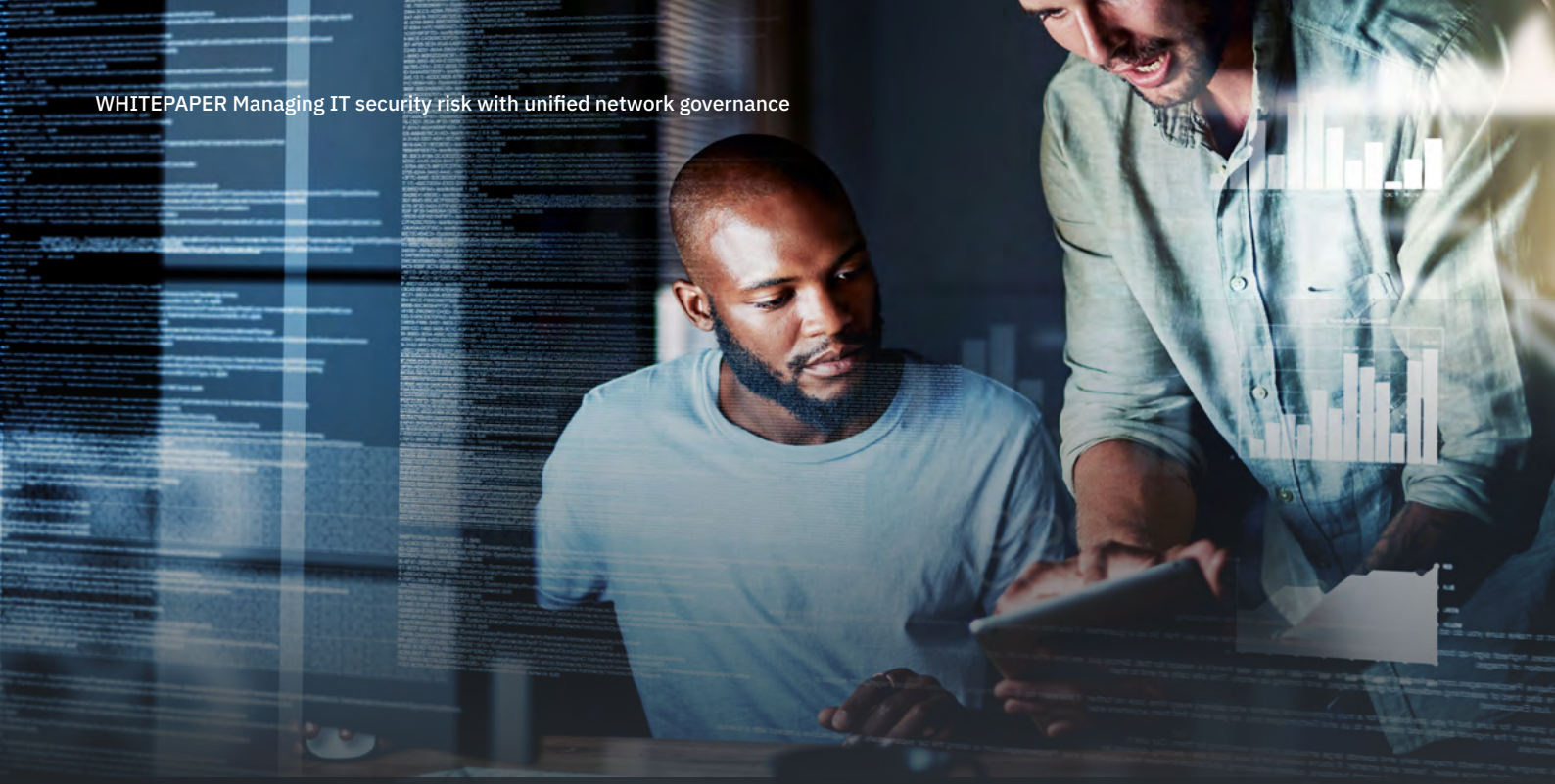
Barriers to effective network governance

Unfortunately, many organisations either don't develop an effective network governance strategy or fail to enforce the rules. Businesses may fail to enforce the rules because they lack the required visibility to understand what those rules are and how they're being broken. Moreover, the constant changes that occur in most organisations, especially those undergoing transformation, can mean that misconfiguration and other potential vulnerabilities can arise and go undetected.

When this happens, the organisation can apply security controls that don't comply with the governance model. This can mean that the organisation is no longer operating in line with its risk tolerance, and may be introducing new risks into the environment unknowingly. Therefore, applying network security controls without governance is not effective.

At the same time, developing a network governance plan without implementing the appropriate security tools is equally ineffective. Both are required to create a strong cybersecurity posture to protect an organisation's data, network, and systems.

ditno.



Managing risk with unified network governance

Managing risk is the number one role for IT security teams. While it's not possible to guarantee 100 percent protection across the entire network at all times, it is possible to identify and mitigate risk in a realistic and pragmatic way. Boards and business leaders need assurance that their investment in IT security will yield a strong return, protecting the business from the most dangerous threats.

Unified network governance plays a critical role in this. A unified network governance solution offers compliance categories that provide guidance regarding every security control created within the system. It provides real-time visibility to expose risk in the environment. This means that, when a security control is implemented, configured, or changed, the unified network governance solution automatically reviews it against the rules set out in the governance strategy. If the control isn't compliant, the solution marks it as non-compliant so that it can be remediated.

Organisations can use unified network governance tools to define any number of categories to meet the business's unique compliance requirements.

Compliance across the hybrid environment

Unified network governance provides a single view and automated solution to analyse and identify non-compliant network security configuration. The same governance model and policies can be seamlessly applied across on-premises and cloud environments, ensuring the business is appropriately secured across the entire network.

Every change, regardless of whether it's a new, updated, or decommissioned service, will be automatically monitored to maintain an acceptable risk exposure.

ditno.

What to look for in a unified network governance provider

There are four key capabilities to look for in a unified network governance provider:

1. CENTRALISED MANAGEMENT

The solution should let users harmonise security controls and governance from a centralised management platform. It should streamline IT service delivery by letting users manage firewall security controls from a single, unified platform. And, it should provide full visibility and control to manage operational risk effectively.

3. AUTOMATION

Using the power of data and machine learning techniques lets organisations quickly build a security baseline. This also lets IT security teams understand application dependencies and weaknesses to ensure business continuity and stability. Automation should also be used to conduct real-time audits so organisations don't have to dedicate manual resources to this time-consuming task.

2. NETWORK SECURITY GUIDELINES

The solution should let users create strategic network security guidelines, specifically for high-risk applications, so the organisation can rapidly innovate and progress without jeopardising stability and control.

4. REAL-TIME COMPLIANCE

The solution should evaluate each network security rule in real time to ensure it matches the organisation's compliance requirements and risk appetite.
The compliance report should clearly highlight configuration items that deviate from the governance model and let the organisation correct these quickly.

How ditno can help

Most organisations are looking for ways to strengthen their IT security as they digitally transform. Network and IT security compliance are essential for organisations to ensure a strong security posture. ditno provides a single unified management portal to create customised governance models that map to users' business requirements and risk appetite.

By enforcing all governance requirements and detecting non-compliant controls across on-premises, cloud, and hybrid environments, ditno's unified network governance solution can dramatically improve the effectiveness and efficiency of an organisation's security efforts.

ditno can provide network visibility in minutes and a fully governed network in just weeks.

To find out how ditno can help your business, contact the team today.

ditno.com
(02) 8011 4860
info@ditno.com

ditno.