ditno.

Security Made Simple

INTRODUCTION

Cyberattacks are changing. Insider threats continue to increase and remain one of the largest unsolved issues in cybersecurity. A network is only as strong as its weakest link and a single data breach may have devastating consequences to an organisation.

Many organisations do not understand or have visibility of their IT services, what they connect to, where and how much data they transfer, or even if a rogue device is present. This demonstrates a gap between the perceived and actual risk landscape. Many major data breaches have been active for months if not years. Security strategies need to change. Each workload requires autonomy while providing real-time visibility of activity.

ditno.

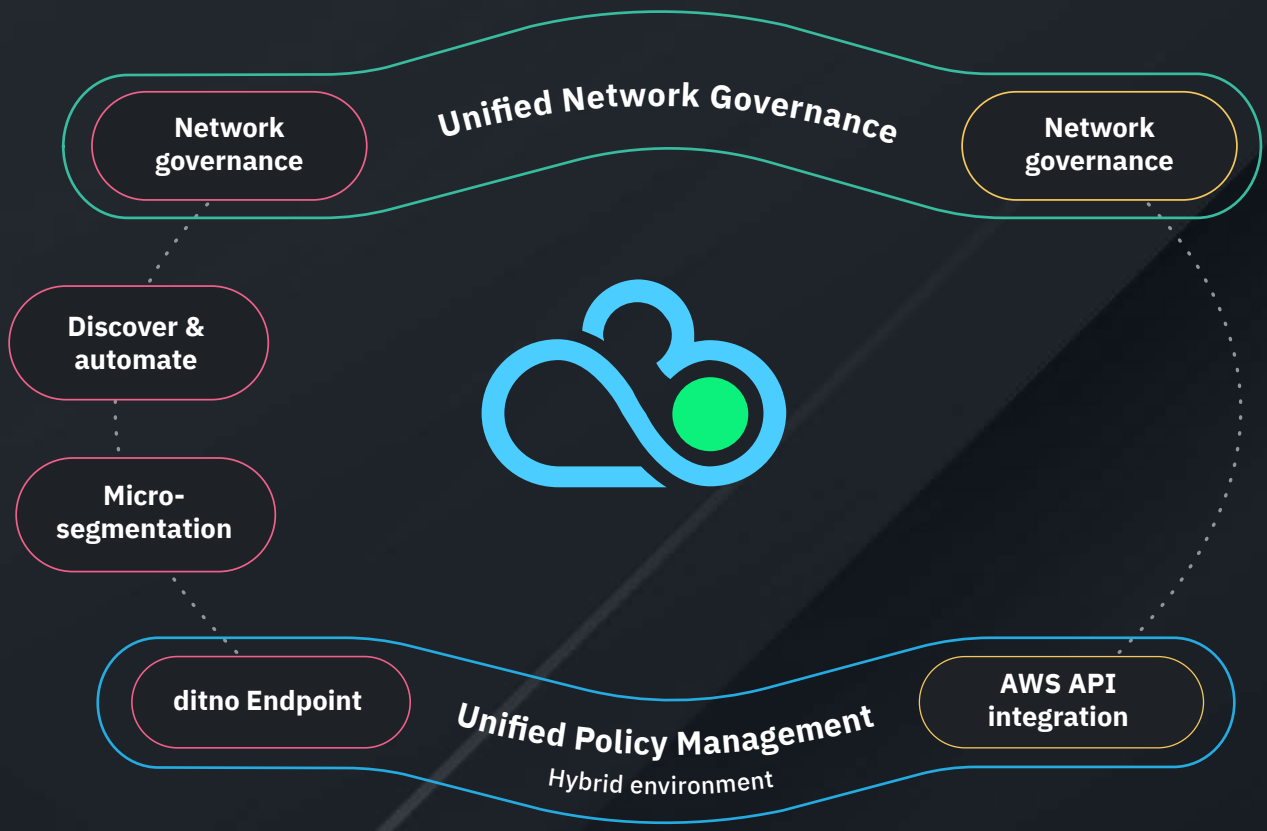
Network Security Policy Management (NSPM) made simple with ditno

Network security is all about zero trust. Organisations should not automatically trust anything inside or outside its perimeter.

Combining real-time network governance and micro-segmentation is a huge step towards a secure environment. With the right software solution, a strengthened security posture can be quickly achieved by using data and automation.

At ditno our NSPM software:

- provides a suite of unified network security tools for enforcing policies across Hybrid environments.
- prevents non-compliant controls being deployed without the necessary approvals and privileges.
- enables centralised visibility across hybrid networks, providing risk analysis, real-time compliance and application mapping.



ditno.

Discover & automate

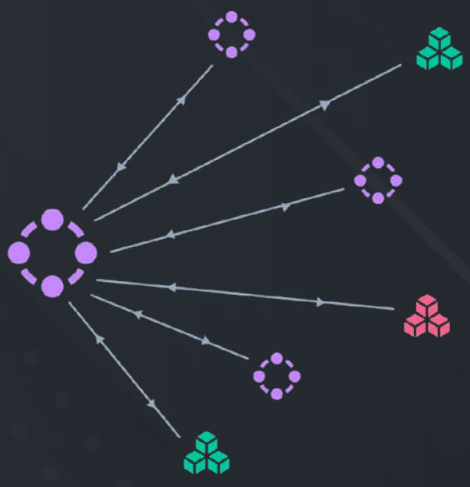
You already know that your data is one of the most important assets your company owns. Difficulty in protecting that data is ever growing thanks to distributed workforces and a less defined perimeter. Your crucial assets need to be placed in a secure bubble that enhances security, while enabling mobility and agility.

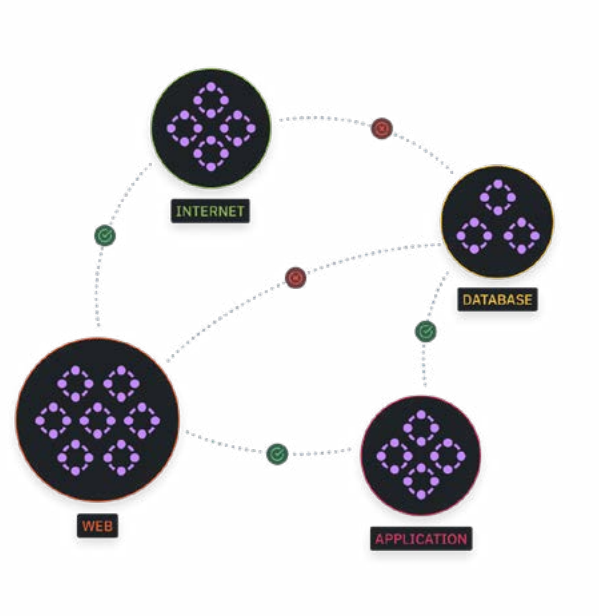
You need to discover IT service dependencies to create a secure baseline. A baseline helps define future strategies and improves project and operational efficiencies.

ditno's endpoint firewall enables telemetry, autonomy, and automation of endpoint security.

- Telemetry provides insights into IT service dependencies and identifies where risk exposure exists and adjustments needs to be made.
- Endpoint autonomy ensures all unauthorised pathways are closed. This protection is consistent across dispersed environments which significantly improve an organisation's risk profile.
- Automation increases the efficiency of deployment and operational processes by suggesting the necessary rules and actively managing rule usage.

Combining endpoint telemetry, autonomy and automation creates an effective risk management





Network governance

Security starts with knowing what can connect to your network and the risks this presents to your business. Alongside your network security software, it's essential to build strategic network governance to identify risk areas on premises and in the cloud. Then, it's essential to ensure that all zero trust network solutions and security controls align with the governance model and to eliminate all controls that don't meet network compliance requirements.

A zero trust environment requires a compliance and risk-centric approach that lets cybersecurity teams detect control breakdowns in real time and respond quickly to threats. With the right IT security platform, you can gain stronger visibility, governance, and control over your systems and achieve a zero trust environment.

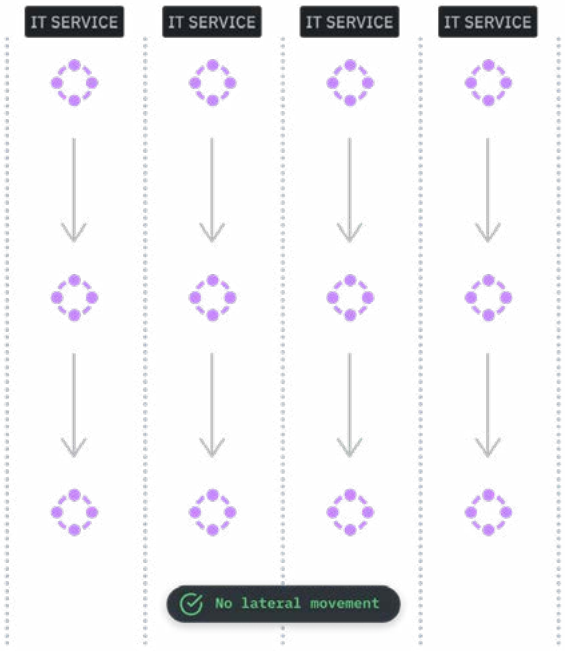
ditno provides a single unified management portal to create customised governance models, according to your business requirements and risk appetite, and create micro-segmentation across an enterprise. Non-compliant controls can be detected across hybrid hosting environments. A single view of enterprise risks is invaluable, so every change can be assessed to maintain an acceptable risk appetite.

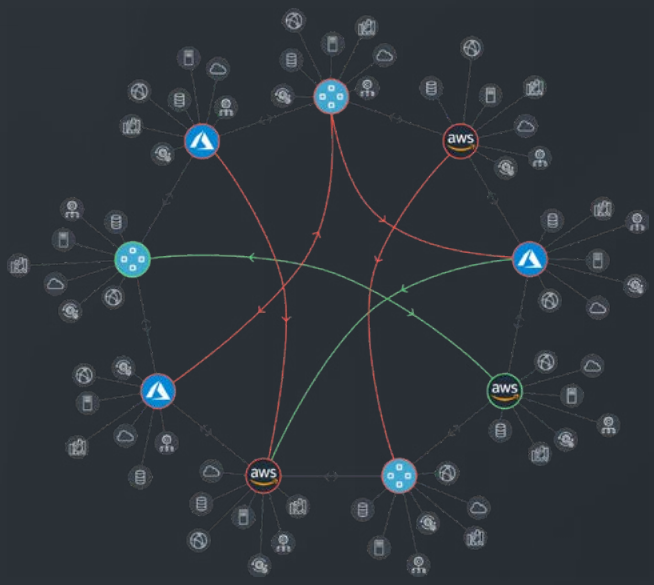
ditno.

Micro-segmentation

Senior executives and board members have started to realise their organisation needs to approach 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 respond to a threat quickly.

You can achieve greater control and visibility over your network with advanced micro-segmentation security technology. ditno's micro-segmentation security software keeps your critical network assets logically separated. That means you can identify and contain network breaches to a defined network segment, application, or even device, all in real time.





Hybrid environment

If you're just starting to explore your move to the cloud, ditno has you covered. We've extended our cybersecurity management platform to cover the AWS cloud environment, with other platforms coming soon. This lets you see your risk exposure at a glance when using native cloud security controls. For example, misconfiguration in the cloud environment can happen by mistake without you even being aware, and can create significant risk.

ditno's security governance layer goes above control and segmentation. This solution assesses every network control that goes into the cloud environment against best-practice governance models in real time. This illuminates risk and ensures the same network governance is applied seamlessly across any environment.

Using ditno's hybrid-ready cybersecurity software solution avoids the need to have separate security solutions to cover on-premises and cloud environments, letting you innovate and transform services without adding risk. Your security posture will remain consistent even as you evolve towards more cloud usage.

ditno.

THE BENEFITS

Reduce risks without compromising costs
By only paying for what you use, you can avoid upfront costs and mirror business demand

Central management platform
One centralised management portal to manage network access, contain threats and assess network exposure

No hardware required
Within minutes, have the environment up and running, and start understanding your environment

Hybrid security
Continuous security and governance across hosting environments (AWS and on-premises) with leading cybersecurity software.

Getting started couldn't be easier

Transforming your network from a vulnerable flat network to a real-time, governed, zero trust environment faster and easier than you thought possible. Here's how we do it:

1. **Build strategic network governance**
   Define & visualise network security posture across your hosting environments (AWS and on-premises)
2. **Discover application dependencies**
   Use ditno's power of machine learning to identify current state
3. **Automatically build a zero trust network**
   Use ditno's automation tools to build your secure foundation
4. **Autonomous assessment of network exposure**
   Combining governance and control allows you to make informed decisions to properly protect your environment.

ditno can give you the visibility you need in just minutes and a fully governed network in weeks. Schedule a demo today and learn how ditno solutions achieve advanced protection from ever-evolving cybersecurity threats to your organisation.

Request a demo

ditno.com

(02) 8011 4860