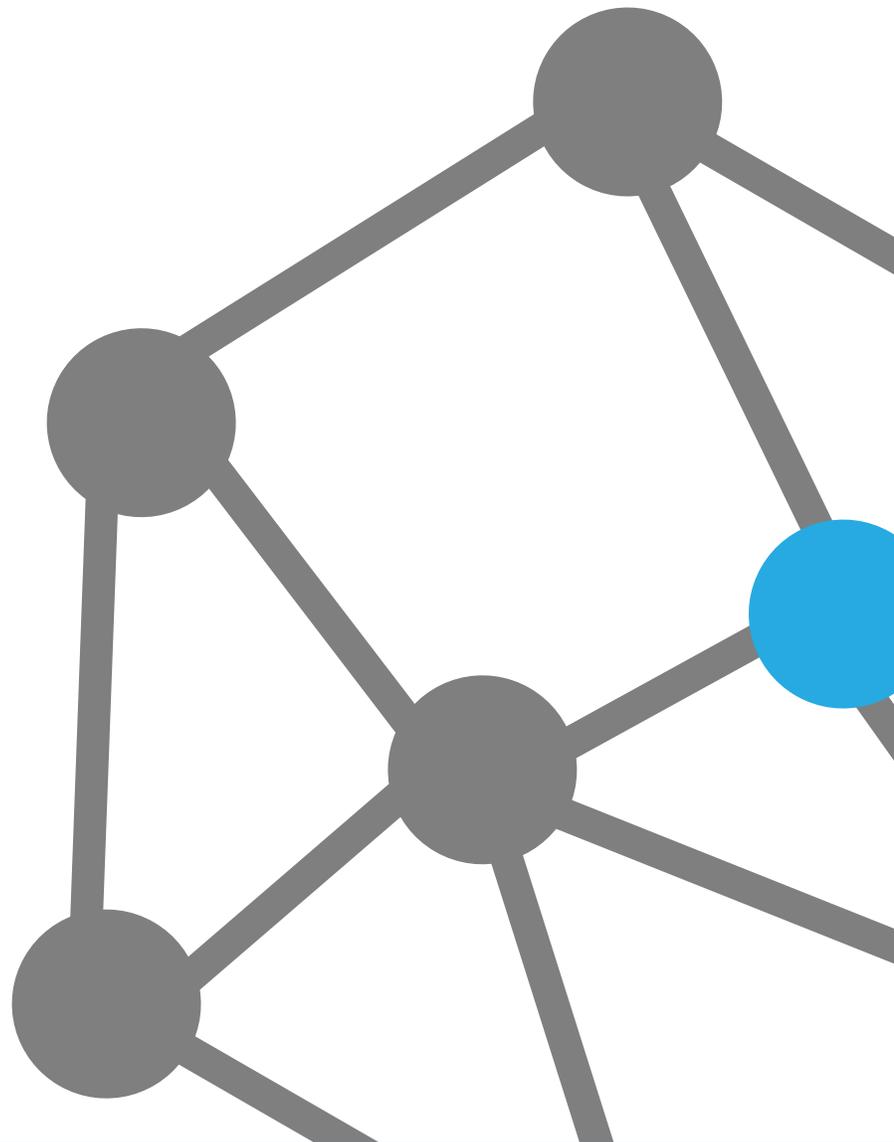


Executive White Paper

Unified Endpoint Firewall Security



Contents

● Understanding IT security weaknesses	2
○ Introduction	2
○ Defending the perimeter is no longer an effective strategy	2
○ Pathways to your critical data	3
○ False sense of security	3
○ Hybrid environments	4
● Delivering and managing IT security differently	5
○ Risk reduction without compromising cost	5
○ Simplification and streamlining resistance to change	6
○ Real time IT security governance	7
● How can ditno make security easy	8
○ Unified Management	8
○ Discovery and visibility	8
○ Minimise threat impact	8
○ Active governance	8
○ Cost effectiveness	8

Understanding IT security weaknesses

Introduction

We are living in a time of continual change, organisations are increasingly reliant on their IT teams and partners to enable digital transformation in order to successfully compete and in some cases to retain relevance.

As part of this transformation it is common to review the infrastructure that underpins an organisation's services; public cloud is now an attractive option providing access to services that offer agility, scale and typically lower costs when compared to on-premises alternatives. A number of business drivers preclude many organisations from shifting completely to the cloud with the majority moving to a hybrid model enabling workload specific placement decisions to be made.

Defending the perimeter is no longer an effective strategy

Organisations have been managing their own data centres for years, these have typically grown organically as business needs shifted. Until now, this has satisfied the organisation's risk appetite but cyberattacks are changing, insider threats continue to increase and remain one of the largest unsolved issues in cybersecurity.

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, organisations should not automatically trust anything inside or outside its perimeter



Compliance reviews and audits should no longer be a manual or scheduled activity

Pathways to your critical data

IT services and their data are extremely valuable to an organisation and it's customers. Therefore, it is necessary to understand all pathways to your 'crown jewels', are they open to everyone? Can threat actors move 'sideways' throughout the network?, what is a normal trend for a service?

Recently, many data breaches have occurred due to 'open' networks, a threat adversary targets a vulnerable outer edge networked device then easily 'moves' throughout the network to compromise critical systems.

Compliance reviews and audits should no longer be a manual or scheduled activity, operations teams need to be actively monitoring to ensure every IT service is within the appropriate risk tolerance threshold. If controls are misconfigured and expose an organisation, a threat adversary will not wait for the next governance review and remediation activities to take place.

Every endpoint should enrich the holistic data set to create a powerful 'network effect'

False sense of security

Many organisations do not understand or have visibility of their connected endpoints, what they connect to, where and how much data they transfer or if a rogue endpoint is present. This demonstrates a gap between the perceived and actual risk landscape - a lot of major data breaches have been active for months if not years.

Therefore, security strategies need to change, each endpoint requires autonomy whilst providing real-time visibility of activity. Every endpoint should enrich the holistic data set to create a powerful 'network effect'.

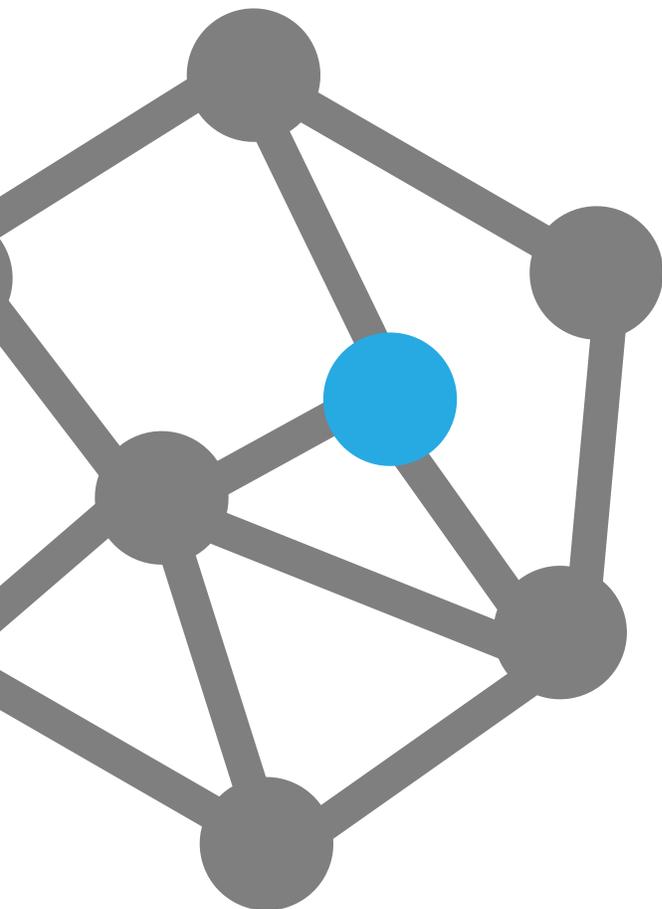


Hybrid environments

Hybrid environments and the proliferation of new types of endpoint (e.g. IoT devices) create a mesh of network connections and additional attack vectors. Managing these complex environments is a critical part of day-to-day activities and risk management.

Organisations strive to maintain security policies and procedures across their environments, but may not have implemented them consistently. Without a central management platform and an overarching governance model, inconsistencies are difficult to identify and presents a state of uncontrolled risk.

A major concern for both senior executives and board members is the ability for an organisation to effectively manage the risks relating to cyber incidents. If a hybrid environment is not configured to provide consistent governance then not only will the risk profile increase but the costs to manage those environments will also increase and changes will take longer to implement.



IoT alone is expected to create
50 billion endpoints
by 2020 and
75% of organisations
plan to use hybrid environments.

These two areas present a large variety of opportunities for threat adversaries to attack.

Delivering and managing IT security differently

Risk reduction without compromising cost

When analysing risk and cost, it is important to consider all aspects, upfront, ongoing, personnel and impact value. For example, cyber publications investigating the impact of data breaches put the cost of the average breach in excess of \$5 million.

As ditno is offered as a service, it immediately removes upfront and commitment costs.

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

Telemetry provides insights into IT service dependencies and identifies where risk exposure exists and adjustments need to be made.

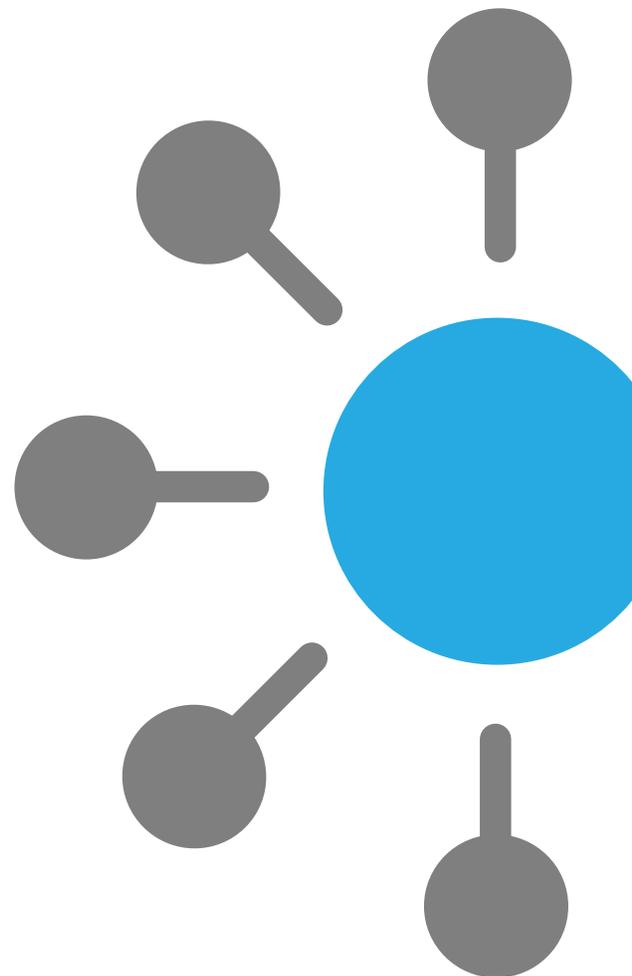
Endpoint autonomy ensures all unauthorised pathways are closed. This protection is consistent across dispersed environments which dramatically improve an organisation's risk profile.

Automation improves the efficiency of deployment and operational processes by suggesting the necessary rules and actively and managing rule usage.

Combining endpoint telemetry, autonomy and automation creates an effective risk management solution with minimal effort and cost.

Isolation of your systems is one of the best countermeasures to data breaches, ditno can easily segment your systems to contain threats which immediately demonstrates good ROI.

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



Simplification and streamlining resistance to change

ditno's solution is platform agnostic, allowing organisations to standardise security controls and securely move workloads between different infrastructure providers. For example, when an endpoint is migrated from an on-premises to a public cloud environment, the security policies dynamically adapt to maintain the same level of trust.

This presents an opportunity to simplify and standardise deployments and operational processes. This consistency streamlines resistance to change and accelerates the security life cycle across the organisation.

For example, the NIST framework can be used to define and manage an organisation's risk posture and encourage continuous improvement. ditno eliminates the need to duplicate designs and implementations across environments which will improve efficiencies and ensure the same risk posture.

The following example demonstrates how ditno aligns to the NIST framework:



Real time IT security governance

ditno's security governance is the key ingredient that binds together diverse environments to create an effective risk management solution. It creates awareness of an organisation's risk exposure.

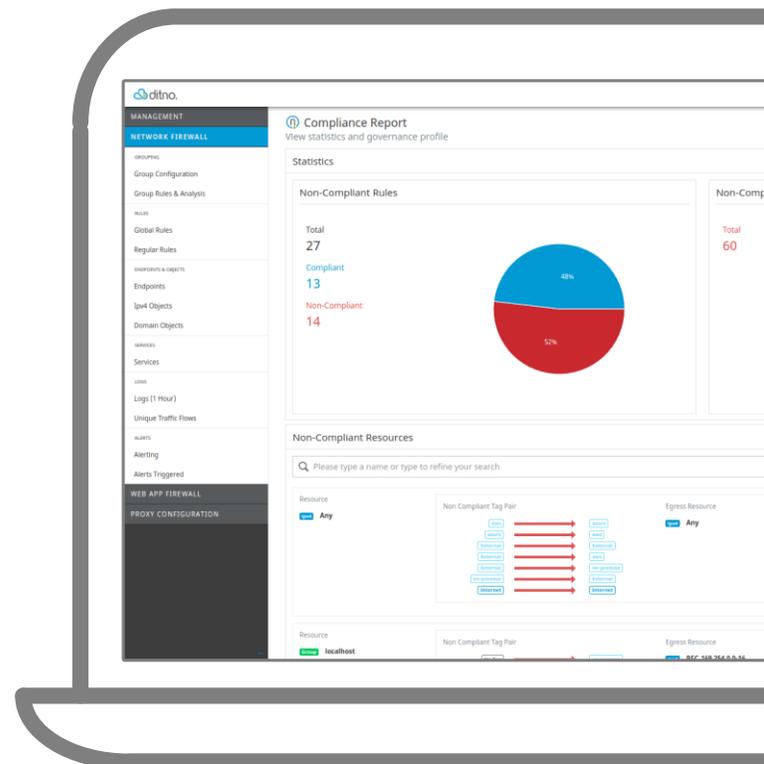
Security controls cannot exist alone, they must be part of a broader risk management strategy. ditno separates the duties of security policy management and security governance. Security governance provides assurance that the security controls will remain compliant with a defined governance model.

The organisation must have a risk tolerance threshold, this threshold may vary by IT service. For example, some IT services may be accessible from the internet and others should definitely not be.

Governance is the mechanism by which IT services will be actively assessed to ensure that non-compliant controls are highlighted or reported for further investigation.

This assurance enhances speed of delivery and provides comfort to explore and leverage innovative solutions to improve business solutions.

Governance is the mechanism by which IT services will be actively assessed to ensure that non-compliant controls are highlighted or reported for further investigation.



How can ditno make security easy



Centralised management

Managing endpoint firewall security controls from a single unified platform streamlines IT service delivery. Implementation and operational activities can be standardised to simplify operational processes and dramatically lower risk.



Discovery and visibility

Discover IT service dependencies to create a secure baseline. A baseline helps define future strategies and improves project and operational efficiencies. Additionally, endpoint telemetry is complemented by event management and SIEM integration to detect anomalies across the organisation.



Minimise threat impact

A breach of one endpoint can be enough for a threat adversary to bring devastation to an organisation. Security controls need to change, they need to be present on every endpoint and ensure they fit within an organisation's risk threshold - if one endpoint goes 'astray' it should be immediately contained to mitigate the impact.



Active governance

ditno's centralised management solution harmonises security policies and security governance across any environment. This ensures security controls are being consistently applied and they are within the organisational risk appetite.



Cost effectiveness

All endpoints need to adhere to the current risk and security framework. Removing the concerns and effort of managing differing risk profiles enables an organisation to focus on the IT service itself. Delivering innovative new solutions facilitates increased revenue whilst improving operational efficiencies.

If you have any questions or need more information, please contact us at:

www.ditno.com