ditno.

Security made simple.

UNIFIED ENDPOINT FIREWALL SECURITY

TABLE OF CONTENTS

© 2020 ditno.

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 offers 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 risks 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 perimeter.

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

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

© 2020 ditno.

PATHWAYS TO YOUR CRITICAL DATA

Compliance reviews and audits should no longer be manual or scheduled activities

IT services and data are extremely valuable to an organisation and its 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, an adversarial threat 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 manual or scheduled activities, IT operations teams need to be actively monitoring to ensure each IT service is within the appropriate risk tolerance. If controls are misconfigured and therefore expose an organisation, a threat adversary will not wait for the next governance review and remediation activities to attack.

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'.

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

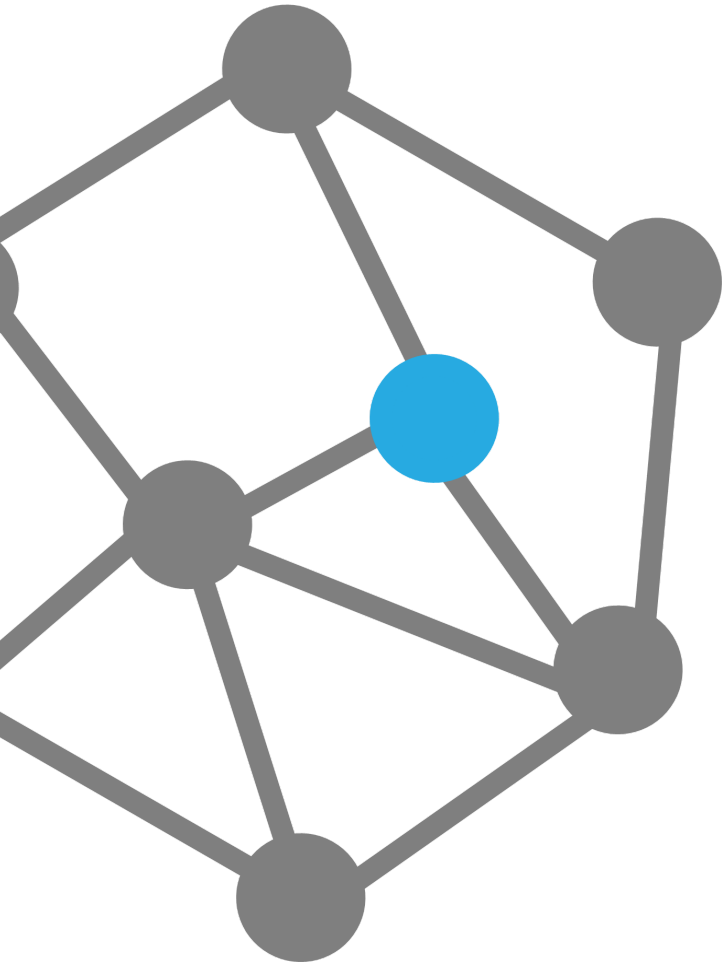
© 2020 ditno.

HYBRID ENVIRONMENTS

Hybrid environments and the proliferation of new types of endpoints (e.g. loT 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 therefore presents a state of undetected 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, not only will the risk likelihood increase but also the costs to manage those environments 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.

© 2020 ditno.

DELIVERING AND MANAGING IT SECURITY WEAKNESSES

Risk reduction without compromising cost

When analysing risk versus cost, it is important to consider all aspects, from upfront and ongoing costs, to personal and impact value. For example, adverse cyber-related publications and data breach investigation can put the average cost of a breach in excess of $5 million.

As ditno is offered as a pay-as-you-go service, it immediately removes upfront and ongoing commitment costs.

ditno's unified firewall solutions enable 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.

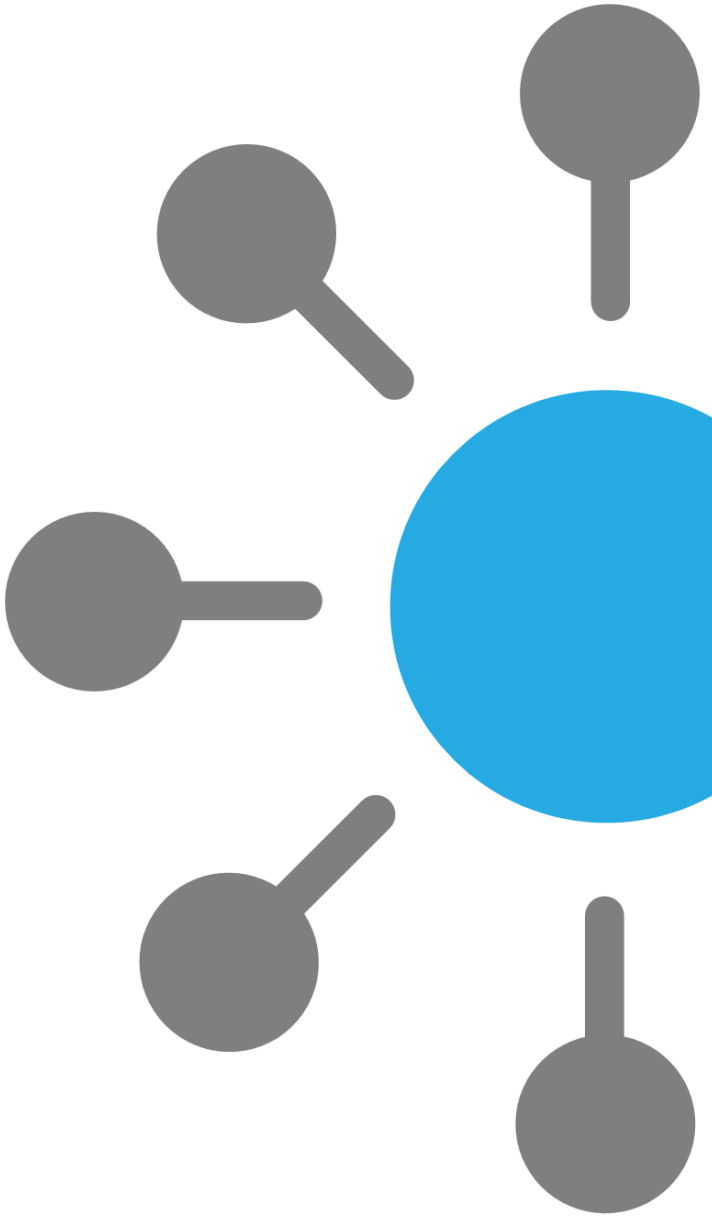
Endpoint autonomy ensures all unauthorized pathways are closed. This protection is consistent across dispersed environments which significantly improve an organisation's risk profile.

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 solution with minimal effort and cost.

Isolation of your system 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



© 2020 ditno.

Simplification and streamlining resistance to change

ditno's solution is platform agnostic, which allows 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, which creates a consistency in streamlining resistance to change and accelerates the security life cycle across the organisation.

For example, the National Institute of Standards and Technology (NIST) Cybersecurity 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 diagram demonstrates how ditno aligns with the NIST Cybersecurity Framework:

© 2020 ditno.

Real time IT security governance

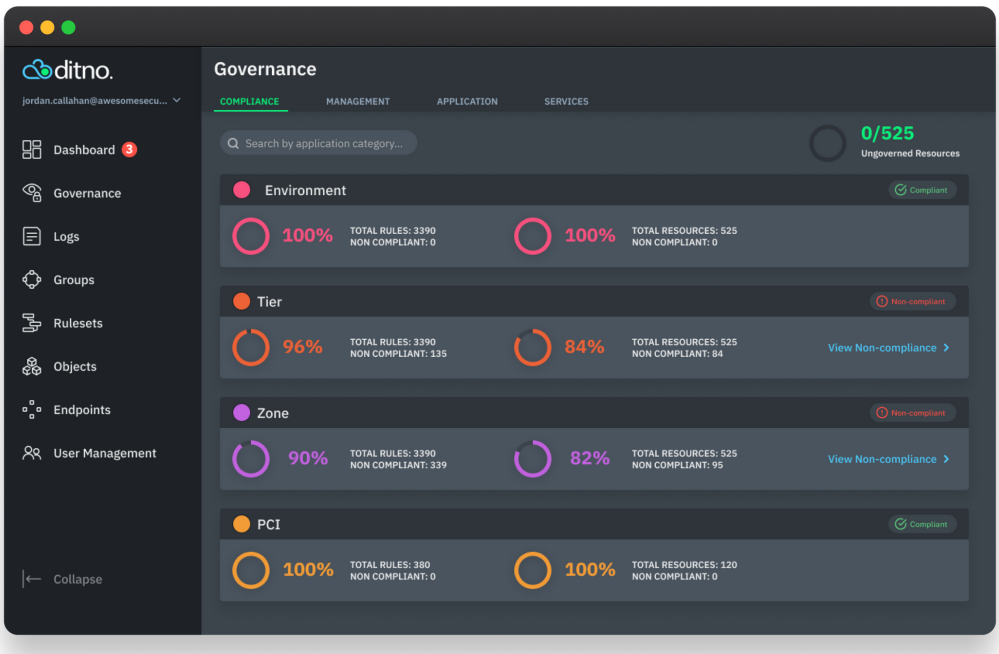
ditno's security governance is the key ingredient that binds together diverse environments in an organisation to create an effective risk management and organisational awareness of its risk exposure.

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 confirmation 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 definitely not.

Network governance is the mechanism by which IT services are actively assessed to ensure non-compliant controls are timely detected and reported for investigation. This will enhance the speed of delivery and provide comfort to explore and leverage innovative solutions to improve business solutions.

Network Governance is the mechanism by which IT services are actively assessed to ensure that non-compliant controls are timely detected and reported for investigation.



© 2020 ditno.

HOW CAN DITNO MAKE SECURITY SIMPLE

Centralised management

Manage 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 significantly lower risks.

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 are within an organisation’s risk appetite - if one endpoint goes ‘astray' it should be immediately contained to reduce the impact.

Active governance

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

Cost effectiveness

All endpoints adhere to the current risk and security framework. Removing the concerns and effort of managing different risk profiles allows an organisation to focus on the IT services. Delivering innovative solutions facilitates increased revenue whilst improving operational efficiencies.

Have a question?

If you have any questions or want to learn more, just reach out to us on our website, ditno.com. We will be happy to answer questions or show you a demo of our platform.

© 2020 ditno.