ditno.

SECURITY MADE SIMPLE

ditno. De-perimeterisation: Securing Data in the Cloud

Version: 1.1

Last Modified: 05/06/2016

In the days before virtualization of networks, servers and services, the sole approach to securing IT services was perimeterisation. By grouping and isolating elements of an enterprise's IT components and services, it enabled the creation of security tiers that were easier and simpler to manage, configure, and protect.

The term perimeterisation originates from the original concept of "castle-and-moat"– that is, the construction of an impregnable wall for isolation, protection, and deflection. Most IT departments have used this same approach – creating a defined perimeter using large-scale firewalls, switches, routers and other elements to manage and secure the services contained within.

The information in this document has been compiled with care, but ditno makes no warranties as to its accuracy or completeness. The document and software described herein may be changed or enhanced from time to time. This information does not constitute a commitment or representation by ditno and is subject to change without notice. No part of this document may be reproduced or transmitted, in any form, by any means (electronic, photocopying, recording or otherwise) without the express written consent of ditno. All information communicated in this document is in confidence and subject to the confidentiality clause/s in ditno's Customer/Partner Agreement. Any product or company names referred to in this document may be the trademarks of their respective owners.

ditno: Solving the Security Problem in De-Perimeterised Environments

ditno’s solution enables businesses to deliver services anywhere securely, flexibly and with a Pay-As-You-Go (PAYG) model.

Businesses can easily de-perimeterise their networks, providing an 'agile' approach to security.

Automating the protection of every host has essentially created an elastic perimeter. This offers companies great flexibility so that they can focus on business requirements and improve productivity.

Problems with Perimeterisation

While perimeterisation is a sound concept, it does have some drawbacks: it is cumbersome to manage and difficult to scale.

Perimeters had to be built to be large enough for future growth. Typically, Product Managers and company stakeholders took a 5-year view on such perimeter environments, which required committed demand for that period of time. A high level of predictability in consumption was required, which was neither an agile nor elastic approach. A massive initial capital expenditure investment was also needed which could not be completely realised until full capacity was reached.

In a 5-year period, many changes can be expected to take place and businesses must grow or contract accordingly. Trends shift and demand for products rises and falls over time. With the variable nature of the IT industry, a rigid perimeter is problematic; while it locks unwanted elements and threats out, it also keeps businesses locked in to finite parameters, hardware vendor dependence, and stifled growth.

An organisation’s ability to deliver services then, is determined only by how it can fit them into its perimeter. Perimeterisation makes delivering localised services and consuming external services harder, and interacting with third parties becomes difficult or even impossible.

Removing the Walls: Advantages of De-Perimeterisation

Customer demand indicates that current services should be flexible, scalable, risk averse, and match business requirements. To meet these needs, businesses now turn to internal and external cloud environments rather than dedicated, in-house perimeter environments.

The advantages of de-perimeterisation relate directly to the problems of the perimeter model: namely, capacity management, flexibility, and scale.

De-perimeterisation is agile and elastic, removing the need for expensive and heavy hardware devices. Without the need for a 5-year committed demand plan, Product Managers and company stakeholders are free to focus on delivering IT services that improve productivity and business growth.

Businesses can move to any hosting environment to improve speed to market and customer services, while maintaining the same risk profile. Thus, the business can efficiently consume external services and interact with third parties.

De-perimeterisation approaches security in the same way infrastructure approaches cloud; elastic, movable and scalable.

Moving to a De-perimeterised Environment

Organizations now have choices that greatly increase flexibility while allowing businesses to scale in real-time, rather than a 5-year plan as with a perimeterised model. Options for organizations now include public, private, or hybrid cloud computing to off-load resources to other locations.

Infrastructure as a Service (IaaS) is one way to take advantage of various cloud offerings in order to highly optimize resources while significantly keeping costs down. Those who utilize IaaS typically have their own purchased licenses and contracts for the middle of the stack (database, middleware, and applications), thus requiring only the hardware and operating system components. Two of the largest vendors that offer IaaS include Amazon Web Services (AWS) and Microsoft Azure.

Securing a Borderless Perimeter

By removing borders around the perimeter, organizations must now apply consistent, standardised security controls across dispersed services, enabling elastic, movable and scalable solutions.

In this new de-perimeterised environment, security delivery is not the obstruction or 'police' of an organisation’s perimeter services, but rather a flexible and mobile element that moves with the servers. This allows the data, services, and business to go virtually anywhere. On matters of security, three key principles emerge:

Flexibility for On-Premise or Off-Premise Systems

Securing servers must have built-in flexibility to support an organization’s ongoing and ever-changing needs. Ditno’s product suite creates a virtual data centre, enabling continuous security and centralised analytics across legacy (hardware based), private, public, and hybrid cloud models.

Network Firewall Capability

In today’s newer infrastructure, legacy firewalls are no longer applicable. Replacing your hardware-based firewall with a software-defined firewall is key to protecting your data.

ditno Network Firewall is a direct replacement for legacy firewalls, providing the same robust and continuous protection, but with lower cost, utilizing a pay-as-you-go (PAYG) service model approach. ditno Network Firewall is a light-weight, embedded agent that secures your servers regardless of operating system or location, allowing configuration of firewall policies regardless of where the servers are hosted. ditno’s host-based layer 4 provides micro-segmentation throughout the entire server fleet.

Web Application Firewall Security

In a de-perimeterised environment, the security landscape has changed considerably. Legacy approaches such as Intrusion Detection Prevention (IDP), Endpoint Detection Platforms (EDP), and Endpoint Detection and Response (EDR) have had to evolve in capability, delivery and modularity.

Best practices now indicate that a layered modular security approach, as well as the ability to work seamlessly with other components in a varied environment, offer the best results. In a de-perimeterised environment, Intrusion Protection Systems (IPS) and Intrusion Detection Systems (IDS) are taking on a more focused means of delivery; Web Application Firewall (WAF), being considered a modular form of IDP, provides purpose-built, modular Intrusion capabilities for todays business.

ditno WAF is a robust, lightweight Layer 7 Web Application Firewall that not only protects web applications and data residing on your servers, but offers the flexibility to work with other existing components without the need to purchase additional functionality.

Centralised Management

In today's environments, technology components and services are spread out across a combination of on-premise, private internal, private external, and public cloud providers. It is imperative that you have the ability to manage your security devices across all of these platforms. ditno Management Portal is a single pane of glass that enables you to perform repeatable, elastic and flexible deployments of security policies to each ditno Network Firewall and ditno WAF (host or reverse proxy) instance.

If you have any questions or need further information, please contact us by:

Telephone:	+61 (0)280 114 860
Email:	info@ditno.com
Website:	www.ditno.com