Cloud Managed Server Appliances: Secure by Design & by Management

Zynstra: Security is a core design principle

Zynstra's Cloud Managed Server Appliances and the associated Zynstra Management Platform have been designed from the outset with security at their core and are technically managed as one holistic solution.

Security capabilities are tightly integrated into the Zynstra code base using proven technology and best in class design principles. Security is appropriately layered and the design isolates workloads, automatically keeps the operating systems and applications patched and protects ports from malicious access. The Management Platform constantly monitors the security status of the Server Appliances and proactively tests effectiveness.

Unified Threat Management provides multiple firewalls – one on the LAN side and one on the WAN side of the appliance, along with each VM being locked down to the services they should be supported. Content filtering and anti-virus for the Server Appliance and the users browsing the web through it, intrusion detection, (and anti-malware/anti-spam in the case a local e-mail server is deployed in a VM) are all included as standard.

Active Directory provides the basis of authentication and Single Sign on, whilst encryption is used to protect data in transit.

Additional Data Protection statements are available at http://www.zynstra.com/how-we-do-it/hybrid-cloud-service-levels/

Security Features:

1. Network Gateway

- Network Address Translation (NAT) Firewall isolating the customers Intranet from the Internet
- A single inbound port is opened on the Firewall to support inbound VPN connections. If VPN is not required, this port can be closed
- In-line anti-malware and anti-spyware filtering of web content

2. Authentication and Authorisation

- Delivered via Microsoft Active Directory running on dedicated VM on Server Appliance
- Central control of user login credentials for accessing Devices
- Centralised control of access to network services in particular file shares in 0ffice 365
- Supports mapping of users to groups
- Group policy enabled to mandate policy such as password complexity, change intervals etc
- Supports domain-joined endpoints, allowing security orientated group policy to be applied to networked PCs (e.g.to mandate up-to-date anti malware is present on all end points).
- Synchronised to Windows Azure Directory Services resulting in single set of user credentials for access to local and Office 365 resources

3. Fileshares

- Provided as Windows 2012 Fileserver running in a separate VM.
- Supports access control lists on files to restrict access to none, read only or read/write on a user and group basis (out of the box groups are mapped onto departments).
- Data is encrypted behind the local firewall before transmission to cloud backup into Windows Azure.
- File Server Anti-malware provided as standard.

4. Internal Security Features

- Centralised collection and storage based intrusion detection for all inter VM traffic
- Host based intrusion detection in all VMs based on real time log analysis
- Internal firewalls on all VMs configured to only expose required ports
- All platform (virtualisation and management VMs) protected by read only root configuration controlled by the Hypervisor

Security Management:

5. 'Keep Current' Service

- Zynstra seamlessly manage the application of recommended security patches for Windows/Linux VMs
- Patent pending intellectual property for secure patching mechanism.

6. MSP/Zynstra Support Access

- Authentication and Authorisation of access to platform controlled centrally in the Management Cloud
- Named user access provides full audit information at the individual operator level.