OnApp Cloud

Security datasheet

Cloud security with OnApp

OnApp Cloud has a multi-layered security model. It is designed to maximize cloud security, while enabling hosts and their customers to customize security measures at the network, hypervisor and virtual machine layer.

Virtualization approach

OnApp's hardware virtualization architecture provides the foundation for a secure cloud hosting service, by maintaining isolation of virtual machine and hypervisor operating systems.

This approach is more reliable in a hosted cloud service than, for example, container-based virtualization, where virtual machines and hosts share core OS components. In an OnApp cloud, an attack on the host OS has no impact on client virtual machines.

Hypervisor security

OnApp makes full use of security features built into the Xen and KVM hypervisor platforms used to host virtual machines.

Hypervisors, networks and data stores can also be allocated to individual users or companies in order to create private clouds – that is, where all of a user's cloud resources reside on dedicated hardware, and are not shared with other users.

Customer Isolation Module (CIM)

OnApp's Customer Isolation Module has three main functions:

- **Secure VLAN sharing**: CIM enables secure sharing of VLANs among multiple virtual machines, managing multiple VLANs in the cloud and their assigned IPs.
- **Private VLANs**: with CIM client isolation, every user is secure in their own section of the cloud. OnApp gives you the security of a private VLAN system with less overhead.
- **CIM firewall**: CIM provides an additional layer of firewall security on hypervisors (see below).

Four level firewall security

An OnApp cloud has, as standard, four layers of firewall protection. This includes firewalls on the network, firewalls on hypervisors and firewalls on individual virtual machines.

This may, of course, be extended with additional hardware/software firewalling at the network infrastructure, hypervisor and virtual machine layer.

- **Network/infrastructure firewalls**: hardware firewalls built into the cloud host's network infrastructure/datacenter infrastructure.
- **Hypervisor firewall features**: OnApp makes full use of firewalling and other security features built into supported hypervisor platforms to maintain complete isolation of virtual machines and their data.
- **CIM firewalls**: OnApp also features proprietary firewall technology built into hypervisors as part of the CIM module. This provides additional anti-spoofing and anti-sniffing protection to ensure VMs cannot interact with other VMs' data, except where explicitly allowed. The firewall examine packets entering and leaving virtual machines, blocks any that do not meet rules set by the OnApp Controller server.
- **Virtual machine firewalls**: the final layer is an end-user firewall that is configurable on each individual virtual machine. Each VM can be configured to accept or drop traffic from specified IPs.

Enhanced security VM templates

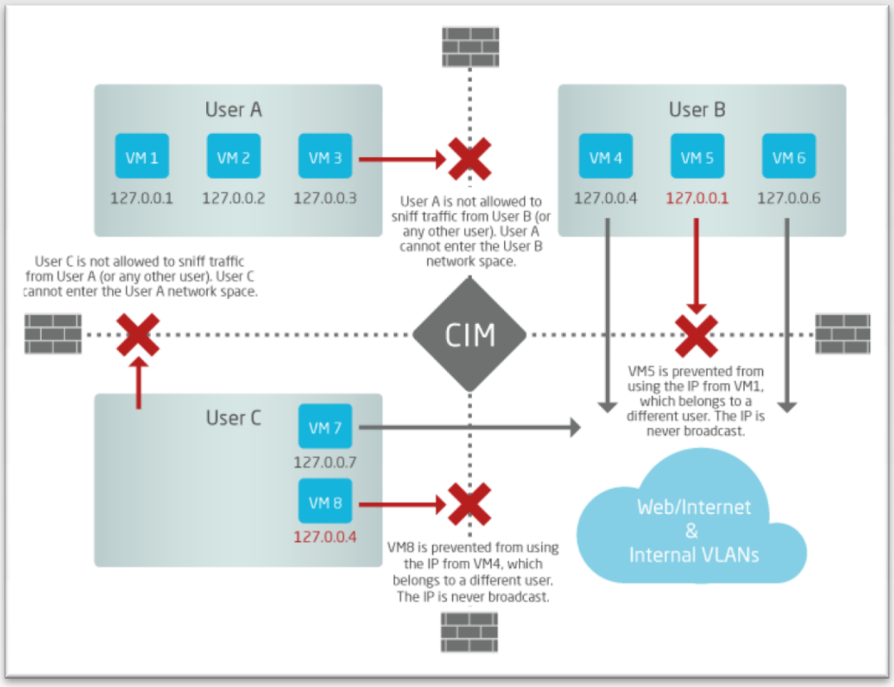
OnApp virtual machine templates can easily be configured with dedicated security technologies, such as Gazzang encryption.

By incorporating additional security technologies into virtual machines, cloud hosts (and their customers) can easily configure virtual machines to support additional security and compliance requirements, such as PCI.

Permissions engine

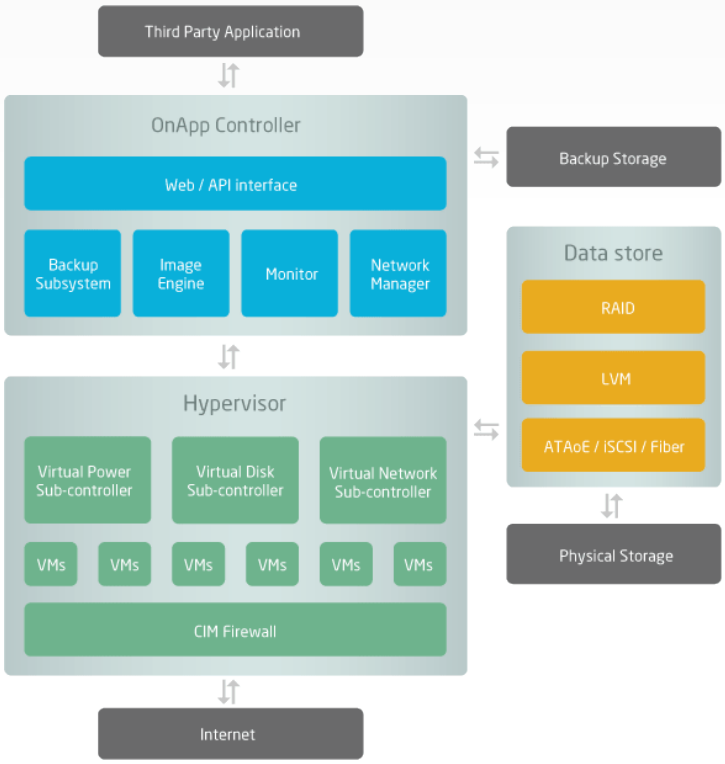
OnApp's detailed permissions engine offers a further level of security. Every function in an OnApp cloud can be enabled or disabled for any user.

This can be used to prevent unauthorized users from modifying hypervisor, network, data store and other sensitive elements of the cloud, as well as more fundamental tasks such as preventing one user from seeing another user's virtual machine.



Customer Isolation Module

The Customer Isolation Module provides additional firewall security on hypervisors; enables secure VLAN sharing among multiple VMs; and isolates clients, giving the security of private VLANs with less overhead.



OnApp architecture

The OnApp Controller (base server) manages every aspect of your cloud, including resources, health monitoring, user management and permissions, billing calculations and failover procedures.

Hypervisors host virtual machines and give them access to virtualized hardware resources. The CIM firewall resides on hypervisor servers.

Data Stores can use almost any storage configuration you're likely to need: RAID, LVM, ATAoE, iSCSI and Fibre.

For a demo and more information:

Tel: (UK) 0800 158 8600
Tel: (US) 866 234 3240
Web: www.onapp.com
Email: info@onapp.com