The Shared Security Model for vCloud Air

The end-to-end security of VMware vCloud® Air™ (the “Service”) is shared between VMware and the customer. VMware provides security for the aspects of the Service over which it has sole physical, logical, and administrative level control. The customer is responsible for the aspects of the Service over which the customer has administrative level access or control. The primary areas of responsibility between VMware and the customer are outlined below.

VMware uses commercially reasonable efforts to provide:

• **Physical Security:** VMware protects the data centers housing vCloud Air from physical security breaches.

• **Information Security:** VMware protects the information systems used to deliver vCloud Air for which it has sole administrative level control.

• **Network Security:** VMware protects the networks containing its information systems up to the point where the customer has some control, permission, or access to modify the customer’s networks.

• **Security Monitoring:** VMware monitors for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of vCloud Air for which it has sole administrative level control over. This responsibility stops at any point where the customer has some control, permission, or access to modify an aspect of the Service.

• **Patching & Vulnerability Management:** VMware maintains the systems it uses to deliver the Service, including the application of patches it deems critical for the target systems. VMware will perform routine vulnerability scans to surface critical risk areas for the systems it uses to deliver the Service offering. Critical vulnerabilities will be addressed in a timely manner.

The customer should address:

• **Information Security:** The customer is responsible for ensuring adequate protection of the information systems, data, content or applications that the customer deploys and/or accesses on vCloud Air. This includes, but is not limited to, any level of patching, security fixes, data encryption, access controls, roles and permissions granted to the customer’s internal, external, or third party users, etc.

• **Network Security:** The customer is responsible for the security of the networks over which the customer has administrative level control. This includes, but is not limited to, maintaining effective firewall rules, exposing communication ports that are only necessary to conduct business, locking down access to only authorized users and other similar controls.

• **Security Monitoring:** The customer is responsible for the detection, classification, and remediation of all security events that are isolated within the customer’s vCloud Air account, including virtual machines, operating systems, applications, data, or content, surfaced through vulnerability scanning tools or required for a compliance or certification program in which the customer is required to participate and which is not serviced under another VMware security program.
VMware vCloud Air Security

Managing Security Threats

The following section describes the various security threats currently addressed by VMware within the vCloud Air platform:

Virtualization/Hypervisor Layer Security

VMware vCloud Air leverages VMware vSphere® virtualization and the VMkernel. VMkernel is fully dedicated to supporting virtual machines and leverages memory hardening, digital signing for integrity and authenticity, and the Intel Trusted Platform Module/Trusted Execution Technology (TPM/TXT) to provide remote attestation of the hypervisor image based on hardware root of trust. The vSphere platform is regularly reviewed for Common Criteria Certification and the latest certifications are available here: http://www.vmware.com/security/certifications


Data Security

From a storage perspective, all storage is logically isolated between tenants using VMware vCloud Director® and storage profiles. Block storage is carved up and assigned to each tenant. Each tenant can only access his or her own storage block. VMware supports in-guest encryption where customers can encrypt their data within the virtual machine to ensure privacy and compliance.

Data Inflight Encryption:

VMware vCloud Air requires customers to set up encrypted SSL VPN/IPsec VPN or Direct connect to ensure data inflight between the customer site and vCloud Air site is encrypted.

Data at Rest Encryption:

VMware vCloud Air strongly recommends the use of in-guest encryption tools to protect customer data at rest within our service. We have partnered up with CloudLink which can help encrypt your data using your existing Key Management solution. Details of the solution can be found here: https://solutionexchange.vmware.com/store/products/94790
Network Security
The vCloud Air Virtual Private Cloud (VPC) offering is a logically isolated set of resources with its own internal network and a virtual network Edge Gateway where customers can set up their own firewall and NAT rules. Network segmentation is achieved through virtual extensible LANs (VxLANs) allowing for a large range of isolated networks for customers. Customers can connect to their virtual machines over IPsec VPN tunnels.

The vCloud Air Dedicated Cloud offering provides physically isolated and reserved compute resources from all other vCloud Air tenants, paired with one or more virtual network Edge Gateways where customers can set up their own firewall and NAT rules. Network segmentation is achieved through VxLANs allowing for a large range of isolated networks for customers. Customers can connect to their VMs over IPsec VPN tunnels.

Physical Security
VMware uses well-established data center providers to host their workloads. These providers have been examined and reviewed by an independent third party auditor to meet the physical security requirements for ISO/IEC 27001 certification, SOC 1 Type 2/SSAE 16/ISAE 3402 and SOC 2 Type 2. Full AT101 reports outlining these specifications are available upon request.

Compliance Certifications
vCloud Air has completed ISO 27001 certification and examinations against SSAE16 SOC2 Type 2 and HIPAA by an independent third party auditor. The Service is in the process of certifying against the SSAE 16 SOC3 and the PCI DSS 2.0 standards. VMware is also setting up a separate community cloud under the vCloud Government Service name that is in process getting certified against FedRAMP criteria by the Joint Authorization Board (JAB) to achieve provisional authority to operate.

Patch Management
VMware targets deployment of applicable patches within 30 days; any security related patches that have a critical or high rating are addressed on a case-by-case basis depending on the scope and affected component.

Security Incident Response Process
VMware will provide security incident response (e.g., detection, severity/threat classification, forensics, and resolution) pertaining to management infrastructure over which VMware has direct, administrative, and/or physical access and control, such as the vCloud Air servers, storage, applications, and network devices. These processes are internal to VMware service operations and used to ensure a high quality standard to VMware customers.

Data Breach Monitoring and Notification
If VMware determines that there has been unauthorized access to, or use or disclosure of customer content, VMware will use commercially reasonable efforts to notify customers taking into account any applicable law, regulation, or governmental request.

Intrusion Detection Process
VMware monitors for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of vCloud Air for which VMware have sole administrative level control over. The goal of this process is to identify security incidents and respond to it proactively. This responsibility stops at any point where customers have control, permission, or access to modify any aspect of the service offering.

The customer is responsible for the security of the networks over which they have administrative level control. This includes, but is not limited to, maintaining effective firewall rules, exposing communication ports that are only necessary to conduct business, locking down promiscuous access, and other such capabilities.
Proactive Security Monitoring over Internet and Social Media (e.g. searching filesharing sites for customer data, seeding data with honey tokens)

VMware security teams perform OSINT monitoring on the Internet for all VMware products and services. This includes harvesting data from search engines, file sharing, and social networking sites. This data is analyzed for keywords and other specific indicators.

With regards to potential data leaks, the customer is solely responsible for protecting the security of his or her content, including any access provided to employees, customers or third parties.

vCloud Air provides certain software and functionality to help protect content from unauthorized access such as firewalls, load balancers, and IPsec VPNs. Customers are encouraged to deploy additional security mechanisms similar to what exists in their current data center to address other security controls such as data encryption, intrusion detection, file integrity monitoring, and other such concerns relevant to the sector and regulatory requirements that apply to the specific business of a customer.

Security Organization and Operations

VMware maintains multiple security teams responsible for different aspects of delivering both products and services, as well as protecting VMware corporate networks.

VMware has a dedicated Security Product Line Manager responsible for ensuring adequate security controls and features within the VMware Service offering.

VMware has a product security team responsible for evaluating VMware software and products for vulnerabilities. They work closely with R&D and engineering teams to ensure secure coding practices and publish security-related advisories.

VMware has an Information Security team responsible for securing VMware cloud services, setting security standards and policy, and the deployment and implementation of new security technologies.

VMware has a dedicated 24/7/365 Security Operations team that is responsible for monitoring VMware cloud services. They perform incident response, forensic investigations, and OSINT monitoring. They also ensure adherence to internal policies and standards.

VMware security teams hold multiple certifications from ISC2, GIAC, as well as others relevant for their particular areas of expertise and focus.

Several VMware security team members also hold security clearances with the Department of Defense, and are members of other organizations such as the FBI Infragard program and the HTcia.

All VMware employees participate in continuing education, training, and certification.

VMware performs background checks on all new hires. This includes verifying SSN, deemed export control/DPL, education, employment, as well as criminal history.