Trend Micro™ Deep Security™

Advanced Security and Threat Protection for VMware® vCloud® Air™

Secure your journey to the public cloud with seamless protection

For years, organizations have employed VMware to virtualize their environments to create efficient modern data centers. And now, as your organization looks to expand to the public cloud, vCloud Air enables you to seamlessly move from on-premises or private cloud deployments to the public cloud. Of course, you still need to secure your workloads as required in the shared security responsibility model.

With traditional approaches to security, organizations wanting to extend their existing environments to the cloud have experienced time-consuming challenges with a very real risk of introducing potential security breaches and business disruptions for critical applications. Trend Micro Deep Security with vCloud Air addresses the challenges of securing hybrid deployments and secures your workloads in hybrid environments.

With Deep Security, you can seamlessly secure your on-premises, private, and public cloud deployments from a single console. It automatically detects Virtual Machines (VMs) across all environments and applies (via policy) a comprehensive range of security capabilities that have been proven with thousands of customers.

You can rest assured in knowing that all of your security policies and protections will be replicated while in the public cloud, providing consistent security from the modern data center and into the cloud. In addition, the Deep Security offering helps prevent breaches, minimize business disruptions, detect potential backdoors, and monitor sensitive deployments for unintended configuration changes.

VMware vCloud® Air is a secure, dedicated hybrid cloud service operated by VMware, built on the trusted foundation of VMware vSphere®. The service supports existing workloads and third party applications, as well as new application development, giving IT a common platform for seamlessly extending its data center into the cloud.

Trend Micro Deep Security for vCloud Air delivers highly efficient agentless and agent-based protection for physical, virtual, and cloud servers. In vCloud Air environments, you can seamlessly secure your on-premises, private, and public cloud deployments from a single console.
PREVENTING SECURITY BREACHES AND BUSINESS DISRUPTIONS IN THE CLOUD

Using traditional security as the default approach to protecting public cloud instances can lead to security gaps, business disruptions, and increased operational costs. Physical network security boxes used for on-premises or private cloud deployments can’t follow the workloads to the public cloud. Organizations often attempt to deploy separate security mechanisms for their public cloud workloads, introducing operational overlap and challenges in both security policy consistency as well as reporting, which can make compliance a challenge. For example, when issues like the recent Heartbleed vulnerability are discovered, emergency patching in the cloud can cause costly business disruptions that could include loss of revenue, service gaps, and more.

Deep Security’s Intrusion Prevention System (IPS) protects servers from security gaps in virtualized and vCloud Air deployments by using application layer packet inspection to detect and prevent attacks at the network - before they are processed by an application. By implementing inspection before packets can reach the application, intrusions are regularly blocked without downtime or code changes. Implementation of IPS for web applications helps enable compliance such as key PCI requirements for the protection of web applications by defending against web application vulnerabilities at transport and content layers.

Deep Security helps protect against unplanned emergency patching (via virtual patching) by shielding unpatched vulnerabilities in your applications, within vCloud Air deployments. Inspecting VM traffic enables detection and immediate blocking of suspicious and malicious activity. With Deep Security’s tight interoperability with vCloud Air, the Deep Security Agent on the VM is automatically updated with a rule set in real time that shields the VM from the exploit.
Key Solution Benefits
• Enables organizations to leverage the efficiency of the cloud without compromising security
• Reduces operational expenditures by extending security controls in a single solution across virtual and cloud environments, including automated security tasks that can reduce the effort to manage and support audits
• Eliminates potentially costly business disruptions through consistent security across all deployment environments
• Provides consistent protection against ongoing vulnerabilities with the flexibility to schedule downtime and remediation with minimal impact to business operations

Trend Micro has worked closely with VMware for the past six years and was first to market with its security innovation: agentless security for virtualized environments. Today, products from both companies continue to work together to secure virtualized environments, delivering highly optimized security solutions for the VMware hybrid cloud. This enables organizations like yours to realize the potential of cloud computing by seamlessly extending on-premises security to the cloud. Now you can use the same powerful tools that you’ve become accustomed to in your VMware on-premises or private cloud deployment, in the public cloud through the tightly interoperable Trend Micro-vCloud Air solution.

ADDITIONAL DEEP SECURITY CAPABILITIES FOR VCLOUD AIR

Protection from Cyber Threats and Attacks
• Organizations today leverage Trend Micro’s award-winning anti-malware capabilities to protect data on their virtual instances and quarantine or remove malicious or suspicious files. In addition, organizations control communications to trusted services through “domain whitelisting.”

Satisfying Regulatory Compliance Requirements
• Trend Micro provides file integrity monitoring and log inspection functionality that can detect and log unauthorized or malicious changes to files and services. Organizations can meet and exceed compliance requirements for regulations such as PCI by providing real-time and on-demand monitoring of files, services, ports, and registry keys.