Array NETWORKS

vmracks
secure cloud hosting

vxAG CASE STUDY

VM Racks

HIPAA compliant managed cloud provider uses vxAG virtual secure access gateways to provide scalable, secure, and customizable remote access for end-user customers to manage their virtual environments while securing data in-transit and at-rest.

Background

Launched in 2008, VM Racks offers managed HIPAA compliant hosted solutions for the medical, insurance, and other organizations that require a high degree of security and protection for sensitive personal health information, data and applications. VM Racks' cloud service offerings are audited and offer fully managed security, active compliance and strong data protection. Tenants are fully isolated, and data is encrypted at-rest and in-transit.

In addition to Web and application hosting, VM Racks offers a portfolio of HIPAA compliant solutions including SFTP, cloud drive, and email hosting services. The company maintains data centers in San Diego, Phoenix and elsewhere to meet the needs of its thousands-strong customer base located mainly in North America but increasingly in other world regions.

Industry:

HIPAA Compliant Managed Service Provider (MSP)

Challenges:

Assure the security of data at rest and in transit while allowing end-customers to manage and use their virtual environments

Provide simple-to-use but highly secure multifactor authentication

Automate account creation and role assignment to streamline workload and support scaling

Support multiple roles to allow users to access only authorized resources

Solution:

Two Array Networks vxAG virtual secure access gateways for high availability

Benefits:

Data in transit protected per HIPAA compliance requirements

Hardware ID-based multifactor authentication requires minimal effort by end-users

XML-RPC automates new account creation and role assignments

Roles can be layered and grouped to allow access only to authorized resources

Easy scaling by simply adding more vxAG virtual appliances

VM Racks' managed solutions place a high priority on customer service and support. Premium US-based service is available 24/7, and every hosting plan includes red-carpet onboarding to ease the ramp-up and roll-out processes.

Challenges

As a HIPAA compliant hosting provider, VM Racks must assure the security of both data at-rest within the data centers, as well as data in-transit between the customers' administrators and their own environment within the data center. For the latter, VM Racks used an SSL VPN product that was integrated into a firewall.

The integrated solution proved problematic, however. Connections were dropped periodically, frustrating the company's end-customers, and certain user operating systems were incompatible with the SSL VPN client. In addition, there were concerns about the SSL VPN's ability to scale up and out to support VM Racks' growing user base.

In addition, VM Racks required multifactor authentication in order to assure security of customer access to their hosted resources. The firewall/SSL VPN combo offered two-factor authentication via email, but that option placed an important piece of the authentication outside VM Racks' control. Google Authenticator quickly became complicated and unwieldy as an option.

"The release of Mac OS X El Capitan update was the ultimate problem," noted David Breise, network engineer and systems administrator for VM Racks. A fairly high percentage of customers were impacted by the SSL VPN's inability to support the latest Mac version.

Solution and Results

VM Racks began researching a new SSL VPN solution, but quickly encountered a problem. "We were surprised we couldn't find a solution that was not integrated with a firewall as an add-on feature," said Gil Vidals, the company's founder and chief technical officer. "We wanted a device that was made from the ground up for SSL VPN."

After an extended search, Breise downloaded and installed the free trial version of Array's vxAG virtual secure access gateway (SSL VPN) and tested it across all possible use cases and functions required by VM Racks' customer base. "I liked everything I saw in terms of functions and support," Breise said. "It's very customizable and flexible."

For multifactor authentication, Breise took advantage of one of the vxAG's native capabilities. "When I set up a new user, the vxAG automatically scans the PC they will use to access our datacenter and the hardware ID is recorded in the vxAG's local database," he said. A user that attempts to log in to the SSL VPN with the correct user credentials, but an incorrect hardware/machine ID, is rejected – providing rock-solid security. As an added benefit, this method makes it extremely easy for the end user, with no additional entries or codes required.

> ***"I liked everything I saw in terms of functions and support. It's very customizable and flexible."***
>
> David Breise
> Network Engineer & SysAdmin, VM Racks

To accommodate the growing user base, Breise also uses the vxAG's XML-RPC capability to automate the creation of new user accounts and assign roles. "We're using it to automate the new customer process from A to Z," he said.

The vxAG's flexible role-based access has also been a big benefit to VM Racks' operation. "Many of our users have multiple roles, which correlate to access to specific ports or resources," Breise noted. "Some can have up to 15 separate roles. To accommodate their access requirements, I can simply make a new group of roles, and attach it to the user account," he concluded.

Benefits

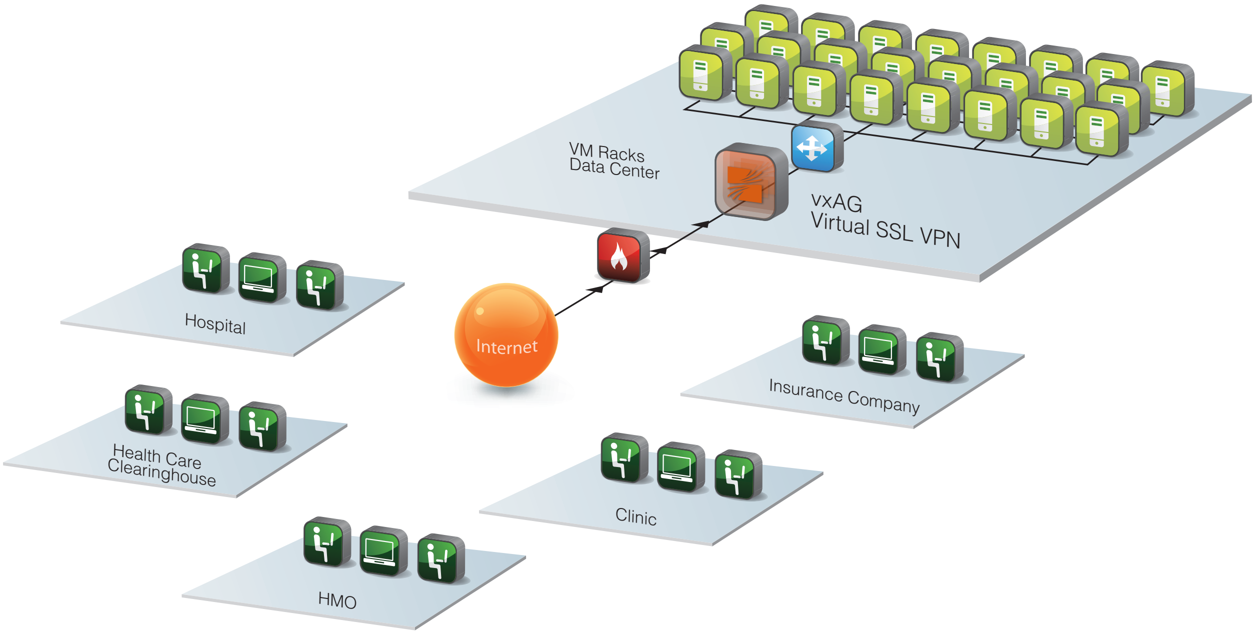
"The vxAG is very capable, customizable and flexible," Breise said. Since the initial deployment, the virtual appliances have been very stable, with no problems or issues.

"We also have no concerns of hitting any limits," he said. "If we need to, we'll just bring up a new virtual appliance." The vxAG SSL VPN has met VM Racks' goals of providing a scalable, flexible and highly secure access method fully compliant with HIPAA requirements.

Summary

For VM Racks, a managed cloud provider focused on meeting the stringent security requirements of HIPAA, Array's vxAG virtual appliance provides the security, flexibility and customization needed to meet the needs of their customers, while keeping patient/client personal health information safe.

Innovative features and capabilities, such as XML RPC, hardware ID-based multifactor authentication, and easy assignment of multiple roles or permissions for users, as well as easy scaling via additional vxAG virtual appliances, meet the exacting requirements of VM Racks now and position the company to continue to grow well into the future.


VM Racks
Data Center
vxAG
Virtual SSL VPN
Internet
Hospital
Health Care
Clearinghouse
HMO
Clinic
Insurance Company