



Liquid Web

How VMware Improves Cloud Security for Your Clients



Digital Transformation

The growing demand for digital transformation has accelerated cloud adoption, prompting more and more managed service providers to help migrate customers to new environments. This modernization of infrastructure, demanded by businesses and delivered by their IT or managed service partners, presents a new set of challenges for all parties. The primary challenge? Keeping workloads and applications safe.

Regardless of business size or sector, securing cloud environments is top of mind for business leaders the world over. A [2020 survey by Barracuda Networks](#) found that more than 70% of business executives say security concerns are slowing their adoption of cloud technologies.

70% of business executives say security concerns are slowing their adoption of cloud technologies.



Improving Cloud Security with VMware

When clients move to the cloud, managed service providers (MSPs) are still needed to manage infrastructure and provide new solutions. However, they're also not charged with the significant capital expenditures of buying servers nor the associated headaches of caring for owned or leased infrastructure. As for clients, pricing based on utilization, improved performance, and increased capabilities make the cloud appealing, regardless of their business size or sector.

However, just because the cloud can provide benefits to clients and their managed service partners does not mean that the path to recognizing those benefits is easy. Managed service providers have valid concerns about security not just during their transition to the cloud, but also once their clients are reliant on the cloud on a daily basis.

In this guide, we will compare and contrast the security of cloud infrastructure compared to on-premise hardware and detail how VMware improves cloud security.



Cloud Security Best Practices

While there are other roadblocks on the way to the cloud, **security is the one most likely to worry managed service providers**. It is incumbent on managed service providers to assuage security concerns for their clients.

To do so, however, requires the MSP first addressing those concerns for themselves. Only then can a cloud solution be offered to clients with the necessary confidence. The good news is that many of the [best practices of cloud security](#) share some commonalities with on-premise security that managed service providers are already familiar with.

Consider the following components of infrastructure security that often fall to the responsibility of a managed service provider.

Monitoring and Scanning

From malware scanning to [intrusion monitoring systems](#), infrastructure security cannot be effective without a system keeping track of what is actually happening. On-premise monitoring and scanning have long been a part of operating systems and available via additional software. The cloud is much the same with one added benefit: most cloud providers offer a myriad of **options built for monitoring and scanning**. This means that MSPs don't have to mix and match operating systems and monitoring tools or worry about incompatibility. With the cloud, this critical piece of the software stack fits like a glove from day one.

Remediation

Even in the best of circumstances and setups, problems do happen. When infrastructure is **wholly managed by a managed service provider**, owning the fix without having to engage anyone else can definitely have some appeal. In the cloud, being reliant on a cloud provider in any way can be a little scary, especially when an engineer is used to complete control. Again, however, there are a number of tools and systems available to MSPs to help with remediation rather than slow things down.

Physical Security

One place where on-premise and cloud security differ is when it comes to physical security. Public cloud providers deny access to everyone not employed by their company. Private cloud providers have access restrictions as well. Both groups often possess **data center certifications and have available audit reports** to allay any concerns about physical security.

Access Controls

Whether in the cloud or on-premise, managing and monitoring who is accessing what (and how) is critical to infrastructure and application security. **Only authorized users should be accessing software and infrastructure** in the first place, and when they do, they should only be performing authorized activities. Thankfully, cloud infrastructure places a similar priority on this security control through ample software integrations both above and below the operating system.

Cloud Security Has Never Been Better

As a managed service provider thinking of security, it is important to understand that cloud providers usually provide security as part of the solution. Additionally, a number of tools exist already to help with security in the cloud. **From activity monitoring and encryption tools to intrusion prevention and remediation systems, software for protecting the cloud has never been better.** In fact, trying out different security options and software can be done at low cost and without the burdens of training or complicated integration.

From activity monitoring and encryption tools to intrusion prevention and remediation systems, software for protecting the cloud has never been better.

Born of Security – VMware in the Cloud

One security tool in your toolbelt as a managed service provider moving clients to the cloud is VMware itself. Surprised? VMware's virtualization technology has long been a favorite of managed service providers, and part of that reputation is rooted in the security-first approach that each of

its technologies is built around. VMware adopts a comprehensive approach to security, enabling you to fully isolate containers and implement granular security policy definitions, starting at the endpoints and running all the way to microservices on your containers. VMware's **enterprise-grade environment** also allows you to encrypt data both in flight and at rest, and detect anomalies at every level of your infrastructure.

VMware includes the following security controls in its offerings:



Identity and Access Management

The first step in great cloud security is identity and access management. VMware helps managed service providers by including controls that allow you to set and maintain the appropriate level of access for users across a client organization.



Operations Monitoring

VMware cloud solutions constantly [monitor activity](#) across all deployments, giving managed service providers a full view of what is happening and where across their cloud environments.



Network and Data Security

Different components are separated and protected by firewalls to ensure there is no spillover of data or breach that spreads across the network. Above and beyond traditional security, VMware offers distributed firewalls, micro-segmentation and scores of other similar options to best protect the environment. Users can also deploy traditional third-party security devices and appliances, recognizing the security benefits of all worlds.



Patch, Update, and Vulnerability Management

VMware includes access to third-party [vulnerability scanning](#) and penetration testing tools. These tools are developed specifically to serve VMware cloud solutions, giving managed service providers confidence.



Software Security

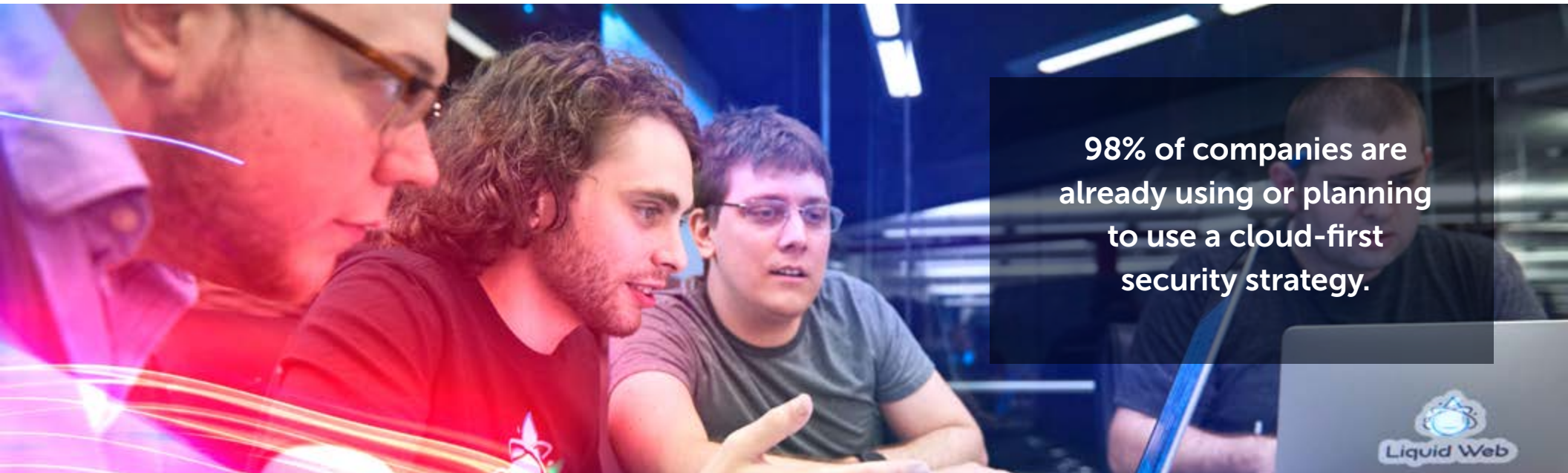
VMware ensures that all operational functions of the software meet industry best practices and follow strict lifecycle controls.

What VMware in the Cloud Means for MSPs

Managed service providers should feel confident that the security offered in the cloud is more than sufficient for their clients. [98% of companies are already using or planning to use a cloud-first security strategy](#). Furthermore, leveraging cutting-edge technology like VMware not only helps meet customer needs, it also opens a new revenue stream for the provider. Offering clients VMware allows your MSP to expand their portfolio with new managed and professional services. Also, your managed services or IT firm may recognize your licensing revenue. VMware can help enable digital transformation for businesses of all sizes and provide the ongoing features, benefits, and security those clients need.

[Recent investments and diversification by VMware](#) are inching the company closer to a leading position in cloud security offerings. Partnerships with companies like Dell further mean that organizations and enterprises can count on VMware to secure their cloud workloads.

Success with VMware in the cloud starts with having the right cloud partner as a foundation. VMware is a powerful tool for virtualization and modernization, but only when deployed correctly. That means a recognition of what is important to your clients and their use cases as well as understanding the expertise and capabilities you already have available. Liquid Web has been helping managed service providers deploy, manage, and maintain VMware for years and can provide the partnership your own VMware practice needs to thrive.



98% of companies are already using or planning to use a cloud-first security strategy.

Take The Next Step

We are experts at working closely with IT professionals, listening intently, and helping you develop a custom cloud solution that meets today's needs and tomorrow's goals – with you involved every step of the way.

Cloud Solutions:

- VMware Private Clouds
- Public Cloud Servers
- High Availability Hosting
- Hybrid Clouds
- Custom Solutions

All Solutions Include:

- Full Management with 24/7/365 On-Site Expert Support
- Standard DDoS Protection & Firewall
- Server Secure Hardening
- Proactive Monitoring & Maintenance



Liquid Web

Need Help Finding a Cloud Solution that Fits Your Specific Requirements?

Talk with a Liquid Web Cloud Hosting Advisor Now.

1-800-580-4985 | 1-517-322-0434

[Chat with us](#) | [Visit us online](#)

¹ Speed Up Your Digital Business Transformation by Jackie Wiles, Gartner
<https://www.gartner.com/smarterwithgartner/speed-up-your-digital-business-transformation/>