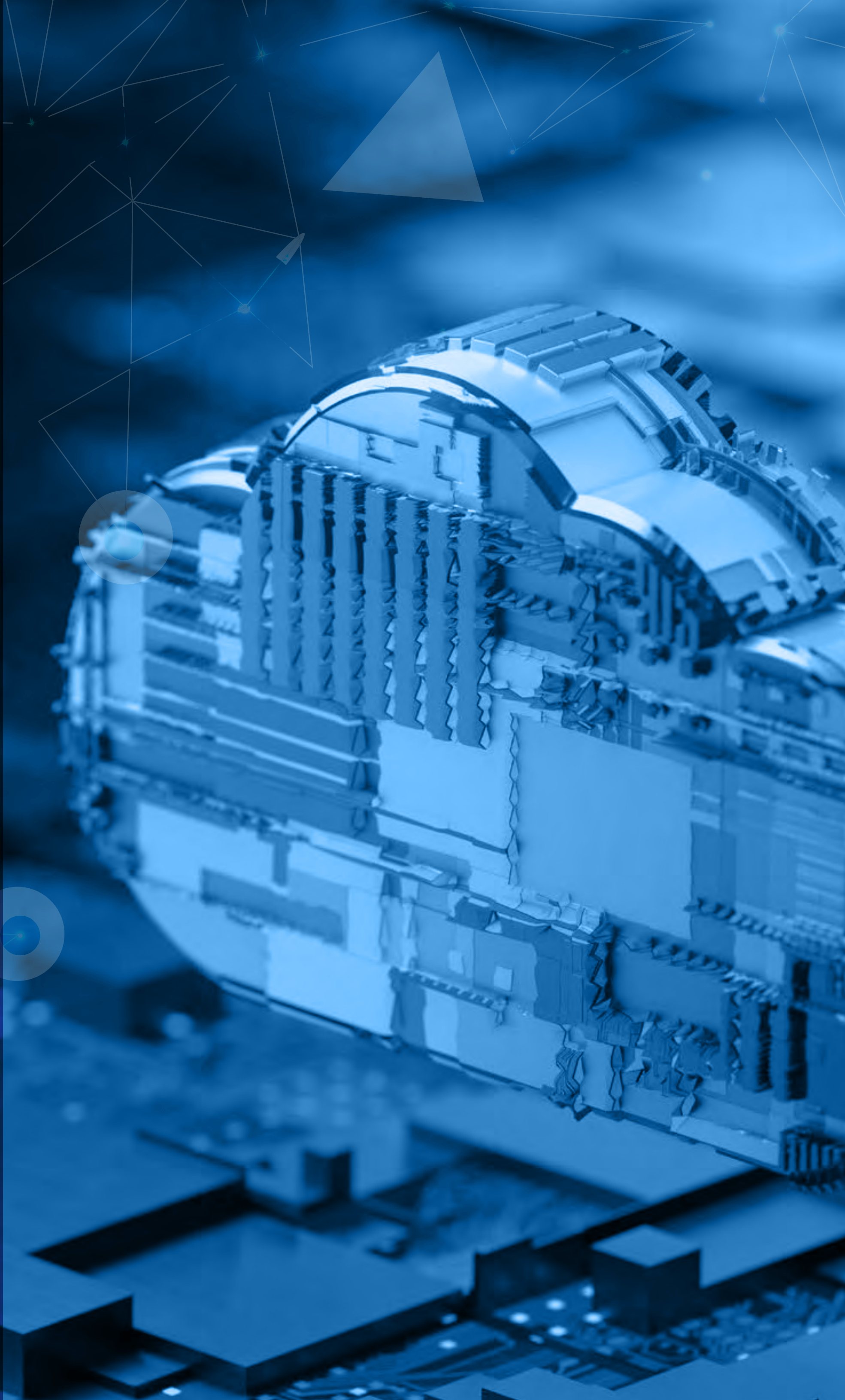
Liquid Web

Migrating Legacy Applications to the Cloud

How To Better Protect Your Traditional Software Past End-of-Life (EOL) with Private Cloud



You pride yourself on having the best software or application to empower your clients. After all, providing a highly-performant solution for your customers is necessary to compete with the cloud-native apps of today.

On the other side of the coin, you're probably dealing with some common hosting-related issues as an independent software vendor (ISV). For instance:

- A new client might have application hosting problems that their current host can't deal with
- A client might have latency issues with the data center
- You may experience downtime and need to migrate your software sooner rather than later
- You may simply want better IT support and performance
- You need a way to compete with applications born in the cloud, and you need it now

That's why rehosting your legacy applications in the cloud for additional security and flexibility is the answer you have been looking for.

In this eBook, you will learn the risks of running traditional software, how to rehost and gain protection while rewriting your software to work natively in the cloud, and why VMware Private Cloud at Liquid Web is the best choice for rehosting your application today.

Table of Contents

The Challenges of Running Software on EOL Operating Systems

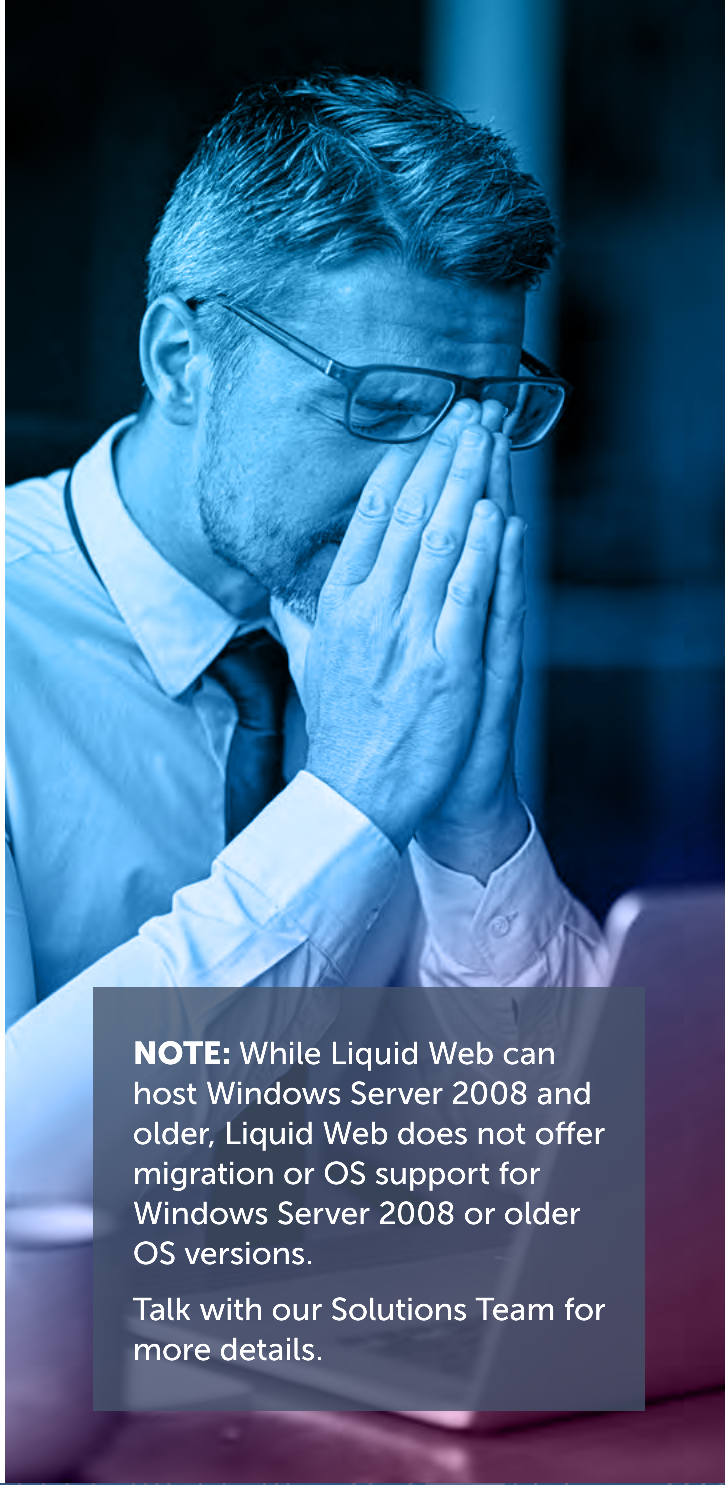
The business challenges ISVs face are substantial, and using software built on End-of-Life operating systems will only bring additional challenges. What does this mean? When software like Windows Server reaches its End-of-Life, the operating system will no longer receive routine security updates and patches, which affects the security and performance of any software built on top of that operating system.

For example, support for Windows Server 2008 ended in 2020. Other Windows Server versions have seen or will see the same fate:

- Windows Server 2000 reached its End-of-Life in **2005**
- Windows Server 2012 reached End-of-Life in **2018**
- Windows Server 2016 reached End-of-Life January **2022**
- Windows Server 2019 will reach End-of-Life in **2024**

This occurrence isn't new. Eventually, all operating systems reach EOL. You can still run your software, but doing so brings about inherent security and competitive risks. Apps built on EOL operating systems won't give you the performance you need to compete with today's native apps in the cloud — at least with on-premises systems infrastructure.

And that isn't even an exhaustive explanation of the risks involved when using software built on EOL operating systems. Read on to explore all of the risks.



NOTE: While Liquid Web can host Windows Server 2008 and older, Liquid Web does not offer migration or OS support for Windows Server 2008 or older OS versions.

Talk with our Solutions Team for more details.

Risks Associated With Running Traditional Software

There are several risks associated with running traditional software on EOL operating systems. They include security risks, regulatory compliance issues, compatibility, and performance issues. Let's take a close look at those risks.

Security Risks

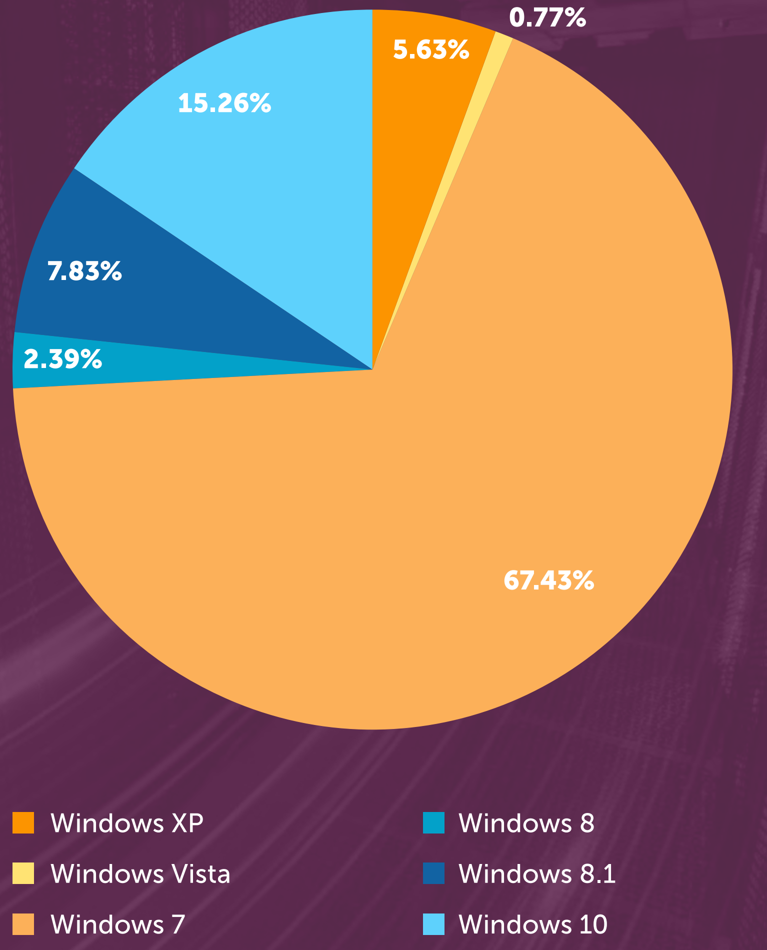
The biggest risk associated with running traditional software on outdated operating systems is the various security problems that can arise. Traditional software is easier for hackers to target and is more susceptible to data center breaches.

Outdated operating systems that haven't received any security updates or patches are more likely to have both critical and non-critical vulnerabilities that hackers can exploit. They can leverage those vulnerabilities to gain access to your network and sensitive information.

Hackers can then sell that sensitive information to your competitors or foreign countries. What's worse, they can hold the information for ransom — which is what happened with the WannaCry outbreak in 2017.

During that attack, over 67% of targeted computer systems were still using an outdated operating system.

Network Composition of IP Addresses Affected by WannaCry Ransomware



Source: How the Impact of WannaCry Ransomware Was Felt Around the World

Business Operations and Customer Support Disruption

Another risk associated with using applications on an outdated operating system is that many of your business applications and devices are connected to the network that's using the outdated operating system. As a result, **if your network gets breached or infected with malware, your critical business operations are likely to be disrupted**, resulting in a loss of revenue.

But business operations aren't the only thing that can be disrupted. You'll also run into issues providing quality customer support. If your company or organization relies on old software, there's a good chance that younger employees won't be familiar with it.

Ask yourself the following:

- How many of your employees have a deep knowledge of those old operating system versions?
- How many support inquiries can they handle daily?

If you only have one or two employees who know how the old operating system version works, chances are they won't be able to meet the support demands. Plus, finding replacements if these employees with specialized knowledge leave would be difficult. Also, note that the host will not support, patch, or update anything OS-related, and will only make the infrastructure and virtual machines migration ready.

Incompatibility Problems

If your software relies on other third-party apps or integrates with them, you could run into compatibility issues. Companies often optimize new applications for the latest operating systems. **Running applications on EOL operating systems means you can't upgrade to the latest version**. Instead, you have to rely on legacy releases. And those legacy releases are likely to reach their EOL soon, too, if they haven't already.

Compliance Issues

There are **numerous regulations and compliance mandates** that organizations have to follow and comply with. These mandates ensure that companies and organizations are compliant with security and privacy regulations. Since EOL software is vulnerable to security exploits, you're at risk of not being compliant with those regulations.

Performance Issues

Performance is another matter to consider. Often, applications using EOL software can't compete with modern-day solutions. The reason behind this is simple: **Aging servers and workstations have outdated specs that are nowhere near sufficient to run modern-day apps** that require high computing power.

And not having the latest features is another reason why performance suffers. For example, you can see the lack of features available on Windows Server 2008 to those available on Windows Server 2019:

- Windows Server 2019 supports the HTTP/2 protocol, delivering better security and improving the delivery of performance
- Windows Server 2019 offers Latency Optimized Background Transport

Older servers are also more prone to breaking and likely out-of-warranty — so if they do break, you'll be forced to upgrade to new technology. That means downtime for your business and unplanned costs for hardware replacement.

When you compare that to native-cloud apps, which benefit not only from the latest software technology but also top-tier hardware that ensures apps run fast, it's easy to see how your software can fail to meet the necessary expectations.

Three Common Paths To Protect Your Traditional Software

Now that you're better informed about the risks of running traditional software, let's talk about the common paths you can take to protect it and why legacy application modernization is so important.

1. Rewrite Your Software

You can opt to rewrite your software from the ground up in order to modernize your applications. Rewriting your software can:

- Speed up your applications
- Deliver new features
- Provide API access for better integration and extended functionality

But rewriting your software or applications is quite expensive. It's not economically viable for most ISVs to perform in a short time. But there is a better way.

Rewriting your software doesn't need to be a rushed, emergency situation. Consider that you can run a depreciated environment while spinning up a new virtual environment on a more modern Windows software version — with controls and logical separation — and begin to rewrite the code over time. Then, once the new software is ready and the migration is done, you can spin down the virtual machine with the old software and turn it off or secure it behind a firewall.

Bottom Line: Rewriting can speed up and secure software, but it is expensive and takes time.

2. Use Extended Security Updates

Another way to protect your software is to use Extended Security Updates (ESU) such as Microsoft's ESU. These updates can be used to patch your operating system. The benefit of this approach is that you gain an upgraded level of security without incurring high costs.

ESU is always recommended, even if you move to a private cloud for additional security. But it's important to note that even with a private cloud where you're behind a firewall, you're still vulnerable at port 80 to malware at the browser and website levels — both exposure to it and at risk of spreading it.

Also, ESU doesn't last forever. Eventually, the ESU ends too, and you'll be forced to find another alternative or rewrite your software.

Bottom Line: Utilizing ESU for your application built on legacy software is always a good idea.

3. Rehost in Private Cloud

Rehosting in the private cloud doesn't require you to rewrite your software (assuming it's technically-sound code), saving you time and money. Private cloud is a computing environment hosted in the cloud whose hardware and software resources are dedicated to a single customer. Rehosting in the cloud combines the benefits of cloud computing, such as scalability and easier service deliverability, with the benefits of on-premises cloud infrastructure, like access control and security.

A great example of a private cloud is Liquid Web's Private Cloud powered by VMware. It's a secure and isolated computer environment used to start, stop, and manage your virtual machines (VMs) with ease. Liquid Web manages your infrastructure and VMs, networking, hardware, software, and day-to-day operations. That also includes ensuring your new VMware environment is migration ready.

With AWS or Azure, you can't simply migrate your code and expect it to work — making private the better option every time.

Bottom Line: Save time and money while gaining security by rehosting legacy applications in private cloud.

Benefits of Migrating Legacy Applications to the Cloud

As we mentioned earlier, private cloud has several benefits. Let's take a closer look at those benefits and why migrating legacy applications to the cloud is the optimal solution to protect your traditional software.

Increased Security

One of the biggest benefits of migrating legacy applications to the cloud is increased security. **Modern cloud environments have feature-rich security measures in place** to protect your software from malware.

These measures typically include strong antivirus and firewall protection. But when it comes to security, a private cloud stands out because it is a single-tenant environment. That means the physical environment is easier to secure, and the environment is protected behind a firewall.

While nothing is ever 100% secure, private cloud can provide increased security for your software. Also, Liquid Web's team can scope access to your infrastructure in order to limit exposure.

Flexibility and Customization Options

Another benefit of migrating your legacy applications to the cloud is that you have **complete control over how you configure your server**. You can choose your operating system and any software you need to run your legacy apps. That also includes any security protocols and apps that tie in with the increased security we mentioned above.

Private cloud is also flexible in terms of hardware, not just the software that runs on it. Plus, you can start with the base model and then upgrade as your needs demand.

That means migrating from an on-premises solution is easier and has a higher success rate — which is critical when you want to benefit from the move.

NOTE: VMware Private Cloud at Liquid Web is compatible with ESET Antivirus for Windows Server 2008 (64 bit) and newer.

Scalability and Better Resource Management

Beyond security and flexibility in server customization, scalability is at the core of any cloud environment, including private cloud.

You can start with the basic package and then upgrade if you see that more resources are needed to complete the process of migrating your legacy applications to the cloud. And since it's a private cloud, there's no one to compete with you for more resources. That means **the server can quickly respond to meet your application's demands.** Scalability is only limited by the resource pool available from the hardware in the cluster (which is more than adequate for most businesses) — and if they need more, they can always add more nodes/resources.

Dedicated VMware solutions can also take advantage of more resources than physically present. That is referred to as "overcommitting resources." For example, on CPUs, we can often go to a 3:1 oversubscription depending on the workload.

But if you find that you aren't using nearly as many resources as your plan offers, you can easily scale back down.

Compliance With Necessary Regulations

As we noted earlier, if you rely on an operating system that reached its EOL, you run the risk of being non-compliant with various security and privacy regulations.

For example, PCI compliance and HIPAA compliance are two common regulations whose requirements can be challenging to meet. A private cloud is designed in a way that makes it **easier to meet those requirements without losing out on other benefits** offered by cloud hosting. This is largely due to overall isolation of workloads and the option to include encryption of data.*

*Moving to Private Cloud does not guarantee PCI or HIPAA compliance requirements will be met

Liquid Web offers single-tenancy on Dedicated VMware Private Cloud and same-day availability on Multi-Tenant VMware Private Cloud.

Reduced Costs

All of the benefits we mentioned above result in a **reduced total cost associated with maintaining your app**, even if your software is past EOL.

Since you can scale the server resources on an as-needed basis and you don't have to worry about rewriting your code in a rush, it's easy to see how moving to the cloud can save your business money in the long run. That's especially true when you consider how unpredictable public cloud costs can be. In fact, the more you use them, the more hidden costs tend to arise.

How Liquid Web's Private Cloud Can Protect Your Traditional Software

Now that you know the benefits of a private cloud, the next logical step is to find a private cloud hosting provider. That's where Liquid Web comes in. Our private cloud is powered by VMware, the number one virtualization solution globally, along with NetApp, a proven leader in data management. It combines the benefits of a traditional public cloud with a simple pricing model and a fully managed experience.

It's a complete white-glove service where Liquid Wed manages everything for you — from hardware to the cloud platform itself — so you can focus on producing the results your business needs. But what does that mean, exactly?

Fully Managed Cloud Services

With Liquid Web's Private Cloud, you don't have to worry about the technical and maintenance aspects of running your server. Instead, everything is taken care of for you. That includes both the hardware and the cloud platform.

No-Contract, Predictable Pricing

There are no surprise costs that will jeopardize your budget. You can simply buy the resources you need and then scale them as needed. You can upgrade your vCPUs, RAM, and storage as the needs of your applications grow without having to invest in additional hardware.

And you aren't required to sign a contract to use Liquid Web's Private Cloud. However, 12-month and 24-month contracts are available if you prefer that option.

Backups for Extra Peace of Mind

Accidents happen. But with Liquid Web's Private Cloud, you get additional peace of mind because Acronis Cyber Backups are available. Acronis is a leader in secure and remote backup solutions. However, it does not support older OS versions, including Windows 2000 or older.

24/7/365 Support

With Liquid Web's Private Cloud, you get access to around-the-clock support with response times on live chat or phone in 59 seconds or less, guaranteed. You can also reach support via email or ticket — whichever way is most convenient for you.

In other words, no matter what time of day or night you need help with your Private Cloud, **Liquid Web is always here to help**. There's no need to have a dedicated IT staff member on the clock, which can help you save costs on IT team salary.

It also means you don't have to learn how to worry about filling your knowledge gaps with additional training and courses. Liquid Web's technicians are experienced and certified in VMware, Windows, Cisco, and Red Hat Linux technologies.

On top of that, you get proactive security and cloud monitoring, thanks to Liquid Web's security teams that focus on monitoring the network, platform, and your servers.

High Availability

Private Cloud is fully backed by Liquid Web's industry-leading service-level agreements (SLAs) to ensure your cloud is always available. VMware High Availablity is able to restart your virtual machines on another host in the cluster. This means you never experience a service interruption.

Final Thoughts: Migrating Legacy Applications to the Cloud

Securing your EOL operating system when migrating legacy applications to the cloud is crucial if you want to ensure that your apps remain secure, compliant with regulations, and compatible with other apps. The best way to protect an EOL operating system is by rehosting it in the private cloud.

That empowers you to focus on producing results for your business while your software is protected. And on the reliable cloud platform, everything is managed for you — from the hardware to the cloud platform itself.

Liquid Web is a trusted cloud partner with over 25 years of experience and over 45,000 customers globally. Liquid Web knows cloud migrations, and Managed Private Cloud gives you cloud performance on a fast, secure enterprise infrastructure powered by VMware and NetApp.

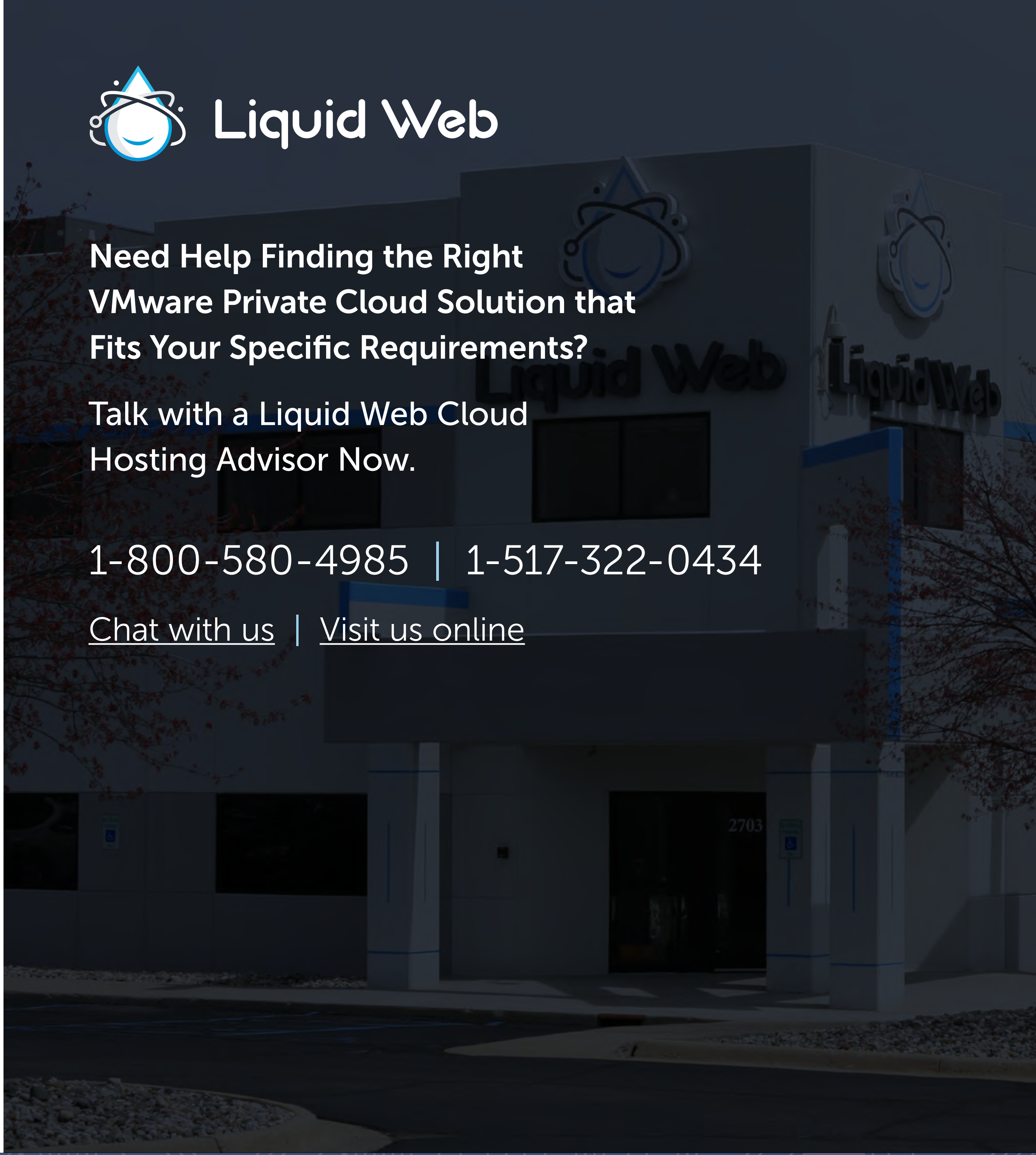
You get complete control over your hosting environment and simple pricing that gives you the power, performance, and reliability that matches industry-leading enterprise solutions.

Take the Next Step

VMware Private Cloud

- Fully Managed with 24/7/365 On-Site Support
- Scalable, Redundant, and Fully Customizable
- Fast 10 Gb Networking
- High-Performance NetApp Storage Area Network (SAN)
- Standard Distributed Denial of Service (DDoS) Protection
- Integrated Acronis Backups Available
- Secure Firewall
- Same-Day Availability on Multi-Tenant
- Single-Tenant Isolation on Dedicated

Cloud Service Providers who display the Cloud Verified badge offer services based on the most complete VMware-based cloud infrastructure technology available, providing compatibility, choice, and control of VMware Cloud Infrastructure at data center locations where this service is offered.



Liquid Web

Need Help Finding the Right VMware Private 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