What is SkyBridge?

SkyBridge is Software as a Service

What is Software as a service (SaaS)?

Main article: Software as a service

The NIST's definition of cloud computing defines Software as a Service as:

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

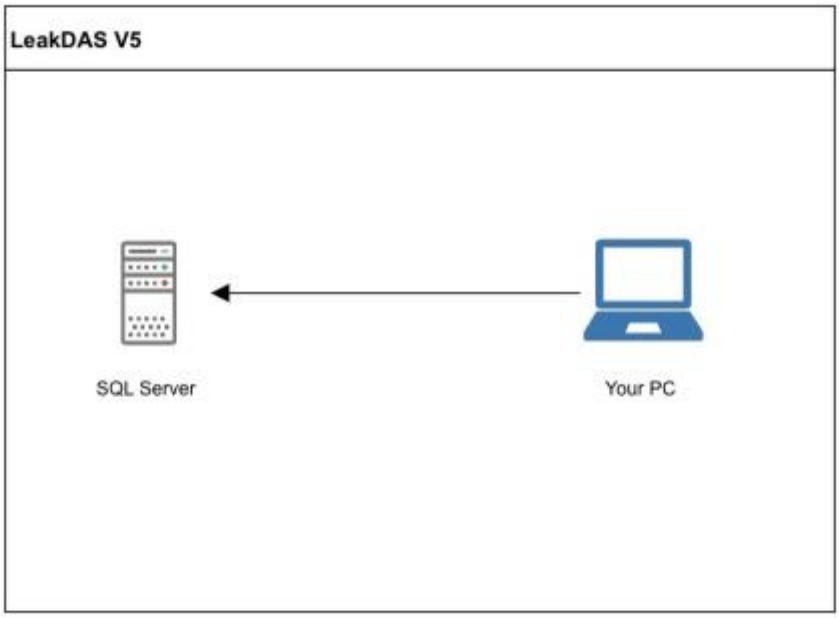
Examples of SaaS: Salesforce, Slack, Office365, Dropbox, Ring Doorbell

How does that differ from LeakDAS?

LeakDAS V5 is a "Windows 32bit desktop application"

That means that in order to run LeakDAS you must install the application on every computer that needs to use it and all of those computers must have unrestricted access to your LDAR data. And that's fine as long as you know that your connection to the database is secure, that the data is always backed up and recoverable, your network is secure, and that your personal computer is not compromised in any way by viruses, or hackers, or ever left in unsecured locations. And when you need a bug fix or new version update you have to reinstall on all of those same computers.

With LeakDAS your personal computer connects directly to your LDAR data



*1 - **LeakDAS on your network***

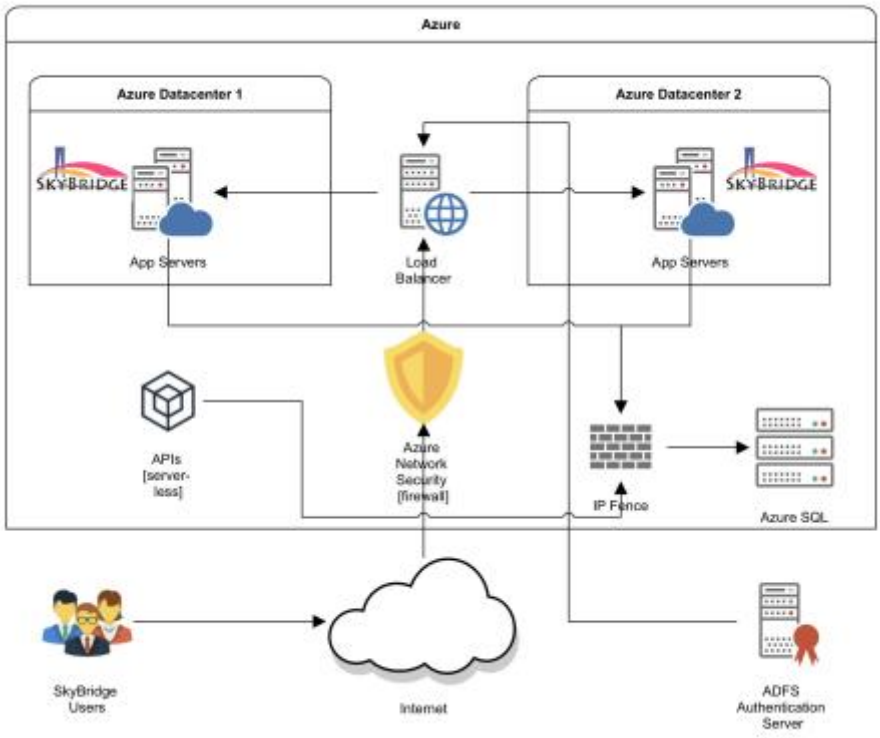
How does SkyBridge improve on LeakDAS?

By making your LDAR data both more accessible and more secure.

SkyBridge takes your LDAR data and puts it into an ultra-secure SQL Server 'lockbox' stored in massive data centers that are managed and protected by Azure, Microsoft's enterprise-class cloud architecture.

The Azure cloud platform is more than 200 products and cloud services designed to help bring new solutions to life—to solve today's challenges and create the future. And it's protected by the most advanced security systems and firewalls in the world.

SkyBridge 2.0 also supports over-the-web authentication to corporate Active Directory accounts and Microsoft-Online accounts



*2 - **SkyBridge 2.0 on the Azure platform***

Does SkyBridge save costs?

You bet it does!

Stop purchasing and upgrading servers, backup storage, network configurations, etc.

No software license fees for Windows Server, SQL Server, CAL licenses, Citrix, e tc.

No responsibility for making or keeping database backups

No IT costs to maintain the system or troubleshoot problems

All backend costs, maintenance, and upgrade fees are included, even software upgrades

What are the SkyBridge advantages?

SkyBridge keeps you connected to your LDAR program in real-time from anywhere.

- Continuous updates and bug fixes happen automatically
- Your LDAR software is always up to date

- You can access your LDAR program data from PCs, laptops, tablets, smartphones, anything that has a web browser
- Technicians can sync from literally anywhere that they have an Internet connection
- The New SkyMobile monitoring app can connect in real-time to your LDAR data making data-loss nearly impossible
- SkyBridge has enhanced GPS support and tracking, along with new location reporting

How do I know it's secure?

The LDAR industry has relied on and trusted InspectionLogic and LeakDAS since the very beginning of The Clean Air Act.

SkyBridge is protected by Azure Security Center, and Azure Defender to secure all resources and data. We further ensure that your data is secure and protected by performing network and website penetration testing and audits for the following:

- Fingerprint webserver software
- Analyze HTTP headers for security misconfiguration
- Check the security of HTTP cookies
- Check the SSL certificate of the server
- Check if the server software is affected by known vulnerabilities
- Analyze robots.txt for interesting URLs
- Check whether a client access file exists, and if it contains a wildcard entry (clientaccesspolicy.xml, crossdomain.xml)
- Discover server configuration problems such as Directory Listing
- Crawl website
- Check for SQL Injection
- Check for Cross-Site Scripting
- Check for Local File Inclusion and Remote File Inclusion
- Check for OS Command Injection
- Check for outdated JavaScript libraries
- Find administrative pages
- Check for sensitive files (archives, backups, certificates, key stores) based on hostname and some common words

- Attempt to find interesting files/functionality
- Check for information disclosure issues
- Network vulnerability scanning
- TCP and UDP port scanning
- Password auditing: length > 50 chars, randomly generated, uppercase, lowercase, numbers and symbols
- Servers have no public IPs and sit behind a firewalled load balancer
- Communication between SQL Server and App server stays on the Azure backbone and does not travel over the public Internet
- All data is encrypted in transmission and at rest with Digicert certificates and mil-spec keys
- No one but you and your agents has access to your data, InspectionLogic support staff need written approval from authorized data owners to do data remediation or access customer data for any reason.