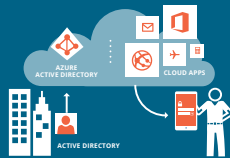


# Compliant Cloud Computing

## CLOUD SECURITY + PRIVACY + COMPLIANCE

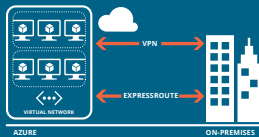
The Lumen21 Compliant Cloud Solution leverages either the Microsoft Azure Cloud or the Amazon AWS Cloud infrastructure today. The Lumen21 Compliant Cloud Computing Solution is HIPAA compliant and its validated by HITRUST (Health Information Trust Alliance) common security framework (CSF). HITRUST CSF is a certifiable framework that is used by health care organizations that create, access, store or exchange personal health and financial information. The HITRUST CSF framework encompasses Federal HIPAA/HITECH, PCI, COBIT and NIST Frameworks. Additionally, the Lumen21 Compliant Cloud Computing also maps to NIST SP 800-144, NIST SP 500-299 standards and complies and exceeds the Cloud Security Alliance (CSA) Framework.



### IDENTITY AND ACCESS

Lumen21 offers enterprise-level cloud identity governance that enables clients to manage its users access:

- Help prevent unauthorized access to servers via Multi-Factor Authentication
- Change and Configuration Management of the entire Compliant Cloud Infrastructure



### NETWORK SECURITY

Lumen21 Private Cloud virtual machines and data are isolated from undesirable traffic and users. Clients accesses them through encrypted or private connections:

- Unlimited firewall Zones at each tier and partitioned networks to help protect against unwanted traffic
- All virtual machines remote desktop session can only be access via multi-factor authentication
- All traffic is over Azure ExpressRoute, AWS DirectConnect, or Point to Point VPN between Client and Microsoft Azure or AWS Datacenter
- Intrusion Detection and Intrusion Prevention Systems as part of the environment



### DATA PROTECTION

Data protection is Lumen21's highest priority. Technology safeguards, such as encryption, and operational processes about data destruction to keep your data yours only:

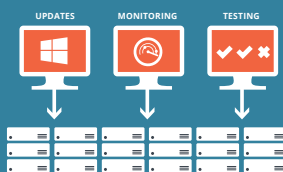
- Encryption is used to help secure data in transit between datacenters and client sites, as well as between and at Microsoft datacenters
- Key Management for all Encrypted Storage and VMs will be managed by Lumen21 and Client
- Contractual agreement with the Cloud Infrastructure provider to follow strict industry standards that call for overwriting storage resources before reuse, as well as physically disposing of decommissioned hardware
- Backup snapshots available for 14 days with ongoing backup retention for any data for seven years on encrypted storage



### DATA PRIVACY

Lumen21 is committed to safeguarding the privacy of the Client's data, and the Client controls where data resides and who can access it

- All data will reside within the US Boundaries as per HIPAA BAA Agreement
- All data is stored on encrypted storage with key management between Lumen21 and Client only. Cloud infrastructure vendors does not have access to the encrypted keys.
- Lumen21 is registered with Department of Commerce under the U.S. Safe Harbor Regulations and Framework



### THREAT DEFENSE

- Integrated unified threat management (UTM)
- Log Management and Review
- Threat Management
- Firewall Management
- Multi-Factor Authentication for any Administrative Access
- Continuous monitoring and analysis of traffic reveal anomalies and threats—forensic tools dissect attacks
- Web Application Firewall (WAF)
- IP Reputation Services
- Monthly Vulnerability Scanning and Management
- Quarterly penetration testing of applications
- Annual Risk Assessment Report
- Secure Portal Access
- Dedicated Secure Encrypted Connection into Client's Environment

Microsoft Azure and Amazon AWS are all certified below as listed:



### COMPLIANCE AND CERTIFICATIONS

Lumen21 is certified below as listed:

- SOC 1
- SOC 2
- PCI DSS
- HIPAA
- US Safe Harbor
- ISO 27001\*

(\*in progress)