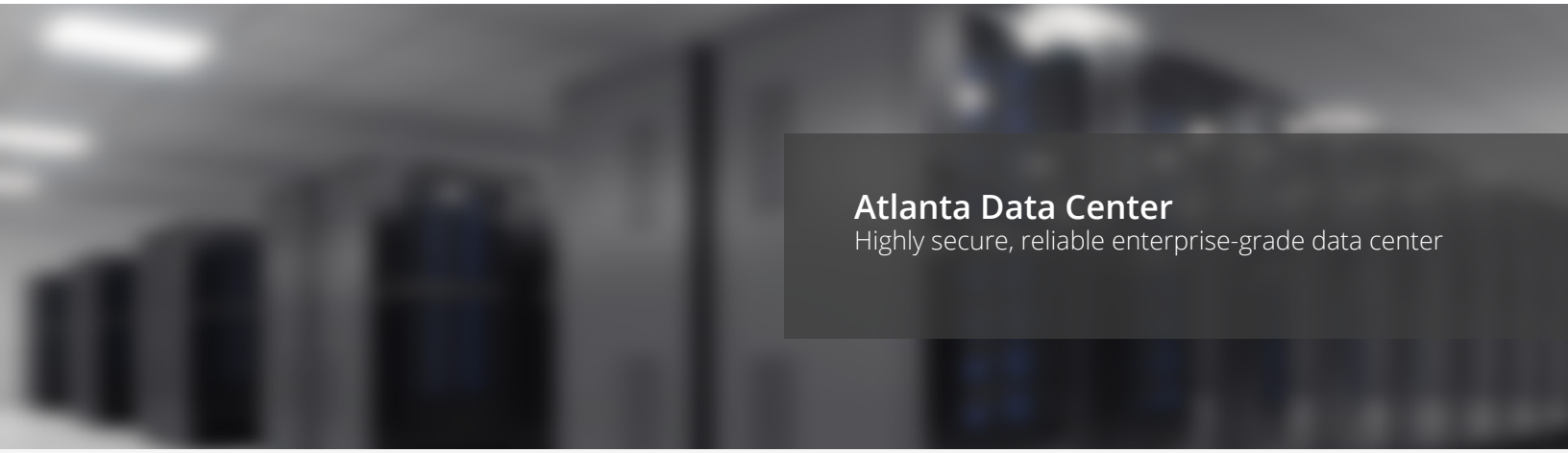
lume



Physical Security Controls

Based on ISO 27001 Standards and Controls

- The data center is physically segregated and requires special access privileges.
- Each floor is outfitted with several strategic man traps throughout the data center.
- Access to raised floor areas are restricted and secured via man traps with sensors and biometrics.
- All cabinets and cages are locked.
- Any and all equipment that is brought into and/or out of the facility is documented via serial numbers.
- In addition to security guards and facility coordinators, a combination of key card access, pin and/or biometric restrictions and building lobby security limit access to facilities.
- Physical access control reviews of data center access are performed periodically by the Operations Manager or appropriate designee.
- Surveillance cameras are located at strategic locations within the data center as a deterrent to unauthorized access.
- Only authorized users can request changes to data center user access listings.
- Visitors and contractors are required to sign in and are escorted by authorized personnel when accessing the facility.
- Semi-annually, access lists are emailed to customers to confirm the users listed as authorized to access the facility.
- Key card request forms for new hires are completed and approved by the Operations Manager.
- Physical access for terminated personnel is revoked immediately.
- Customers granted unescorted badge access must be approved by a data center supervisor or designee.