Cloud Access Control as a Service

AMT's hosting service builds on Amazon's Web Services (AWS), which uses the same data center infrastructure on which Amazon runs its own business. Amazon's data center bandwidth requirements vary so dramatically during the year that they decided to meet this need by building and providing secure, reliable data centers as a service in order to ensure excess capacity. Most importantly, at Amazon's scale, they are able to provide a level of reliability, security, and redundancy very few organizations could provide for themselves.

The security of this infrastructure is provided in partnership with application service providers, such as AMT. AMT brings best practices and expertise in our own solution that permit live monitoring, predictive maintenance, performance tuning on the fly, and a level of reliability and availability that is not possible with an on premise solution.

Additionally, this combination eliminates the need for local IT infrastructure, IT labor, servers, etc. Combined with AMT's support for mobile devices, this also eliminates the need for dedicated client workstations on premises, further lowering costs with a BYOD model.

AMT's team of experts provides automated and live monitoring, continuous maintenance, detection and resolution of issues before these issues can impact users.

MORE INFORMATION ABOUT AWS AND AWS SECURITY

aws.amazon.com/what-is-cloud-computing/

aws.amazon.com/security/

d1.awsstatic.com/whitepapers/Security/AWS_Security_White-paper.pdf

Cloud Access Control as a Service

AMT Cloud Service

- All servers and IT infrastructure to support users' mobile devices
- Maintenance of Digital Certificates *(Provides secure, encrypted, authenticated access to the application from end users mobile devices and desktop browser sessions.)*
- Automated and live monitoring (see **Monitored Events**)
- Continuous backups *(hourly)*
- Verification of backups
- Isolation of backups *(Protection from ransomware)*
- Detection of constrained resources *(Most of which can be added without impacting live user sessions.)*
  - Network resources
  - Server resources
  - SQL Server resources
  - Memory resources
  - Disk resources
- Detection of performance bottlenecks *(Providing an opportunity for continuous application improvement from real time observations—something not possible with on premises systems.)*
- Monitoring and detection of many unusual and potentially suspicious activities *(Includes potential malicious user changes, excessive login attempts, and more.)*

Monitored Events

- Active Readers Gone Dark *(Reports readers that have not had an access granted in a week, if they previously had at least one access granted per day for the last four weeks.)*
- Known controller issues *(Detects known issues in controllers, which require resolution.)*
- SQL Server deadlocks detection *(Notification when a deadlock event has occurred.)*
- Deadlock trace activation *(Causes SQL Server to store deadlock data in the SQL error log if a deadlock occurs.)*
- Cards denied that should have access
- Duplicate cards
- Duplicate ID Holder names
- Failed login attempts
- Temporarily disabling of logins *(With too many failed login attempts.)*
- Server resources
- Offline Controllers
- Orphan object alert
- VertX Controller Events Alert *(More than x per hour)*
- VertX Controller Events count *(Current counts)*
- Database backup success/issues
- Disk space
- Load
- Memory
- Memory (paged)
- RDP
- WSB Restore