AUTHENTX™
CLOUD

AuthentX Cloud Can Eliminate Antiquated Hardware

Part of the assessment process for FedRAMP involves the elimination of redundant or outdated hardware. By the time the assessment is through, agencies should expect to phase out capital expenditures on non-critical infrastructure.

These expenditures can move to more necessary budgets, or go toward cost reduction.

AuthentX Cloud Can Improve Visibility into Security

Vulnerabilities will be exposed and analyzed, and the process will create transparency with Cloud Service Providers (CSPs).

The FedRAMP program provides the flexibility and adaptability to evaluate security threats on an ongoing basis.

AuthentX Cloud Improves Communications Systems

FedRAMP increases communication capabilities across the board. Governments can use FedRAMP to get security information to the right people at the right time.

Added Security

- FedRAMP HIGH
- Multi-Factor Access Required

Convenient

- Accessible via most browsers
- Quick Onboarding for New Customers

Cost Effective

- Reduced Equipment Costs
- Reduced O&M Costs
- Reduced Security Authorization Cost
- Reduced Infrastructure/Hosting Cost

Federal Compliance

- HSPD-12, FIPS 201, Related NIST Guidance
- CIO & OMB Cloud Initiatives

Continuous Monitoring

- 57 items monitored continuously
- Annual assessments
- Monthly scanning, auditing, POA&M

Enhanced Infrastructure

- Three US Based and hosted data centers Transparency
- Third Party Governance & Security Assessments
- Rigorous Continuous MonitoringRequirements
- FedRAMP guidance and requirements

AuthentX Cloud Supports Government Mandates

These mandates reduce budgetary risks.

Mandates Include: FISMA, NIST SP 800-53, OMB A-130, 2019 Federal Cloud Computing Strategy “Cloud Smart”, Data Center Optimization Initiative (DCOI) M-19-19, Improving ICAM OMB M-19-17, HSPD-12, FIPS 201, SP800 PIV related series-e.g. 800-63, 800-157, CIO Council PIV-I.