URVARA CLOUD SECURITY CASE STUDY

The Problem: A healthcare company with 300 employees migrated to AWS but had major security gaps:

- 3 AWS accounts with inconsistent security settings
- 1,200+ publicly accessible S3 buckets (containing patient data)
- No centralized monitoring
- Failed healthcare data compliance audit based on their origin country
- Potential fine + risk of losing healthcare clients

Our Solution:

- Cloud Security Posture Management (CSPM) deployed
- Multi-account security standardization
- Automated compliance monitoring (HIPAA)
- Data encryption enforced across all storage
- Constant cloud threat monitoring

Results after 6 months:

- All 1,200 S3 buckets secured
- Passed healthcare data compliance audit
- Detected and stopped multiple unauthorized access attempts
- 60% reduction in cloud security incidents
- Saved $75k in compliance fines
- Annual cloud cost optimization + avoided regulatory penalties

Notes: Companies move to cloud for speed but often misconfigure security. Most cloud breaches are due to misconfiguration, not cloud provider failures. Automated monitoring catches what manual checks miss. With URVARA's Cloud Security solutions have your cloud services at their most optimal and secure form.