Syteca

Case Study

Strengthening VDI Security and Insider Threat Visibility for a Government & Telecommunications Sector in the GCC

Customer profile

A highly regulated Government and Telecommunications organization in the GCC managing sensitive citizen data and critical infrastructure.

The organization operates a hybrid Virtual Desktop Infrastructure (VDI) environment across:

- On-premises VDI
- Cloud-hosted VDI on Microsoft Azure

These VDIs are used to access regulated systems and mission-critical applications.

Challenges

The organization required strict control and visibility over user activity within VDI sessions.

Native VDI and OS logs provided limited insight into **what users were actually doing once logged in**. Users could access systems and perform actions that could:

- Data exposure or exfiltration
- Misuse of privileged applications
- Unauthorized system changes

Additional challenges included:

- Limited visibility into user activity
- Difficulty investigating insider incidents
- Lack of audit-ready session evidence
- Hybrid complexity across on-prem and Azure environments
- High-density VDI usage

The solution: Syteca VDI monitoring

Syteca was deployed to provide centralized monitoring, auditing, and real-time detection of all VDI user activity across both on-premises and Azure environments.

Key capabilities implemented

- User login and logout tracking
- Session recording with secure, tamper-proof storage
- URL monitoring and keystroke logging
- Application usage visibility inside VDIs
- Searchable session playback for investigations
- Real-time alerts for high-risk activity

Custom alert policies detected

- Access to restricted applications
- Unauthorized data access attempts
- Suspicious behavior patterns
- Privileged activity outside approved time windows

Optimized VDI deployment & scalability:

To support large-scale hybrid VDI operations, Syteca provided:

- Golden image support for VDI agent deployment
- Automatic license assignment in dynamic VDI environments
- Simplified and fast deployment
- Replica server support for redundancy and high availability
- Grayscale recording to reduce storage consumption
- Integration with Microsoft Power BI for reporting and executive dashboards

Results & business impact

- 100% visibility into user activity within VDI sessions
- Faster insider threat investigations with clear forensic evidence
- Improved compliance with national cybersecurity regulations
- Audit-ready reporting and stronger regulatory confidence
- High availability and storage optimization for scalable growth

Deployment flexibility

- On-premises environments
- Cloud environments
- Availability on the Azure Marketplace
- Air-gapped deployments for high-security and regulated operations

Conclusion

By implementing Syteca VDI Monitoring, the organization achieved comprehensive visibility, stronger insider threat detection, and compliance-ready auditing across hybrid VDI environments.

With intelligent monitoring, scalable deployment, and optimized storage efficiency, Syteca delivered a secure and resilient solution for protecting critical government and telecom operations in the GCC.