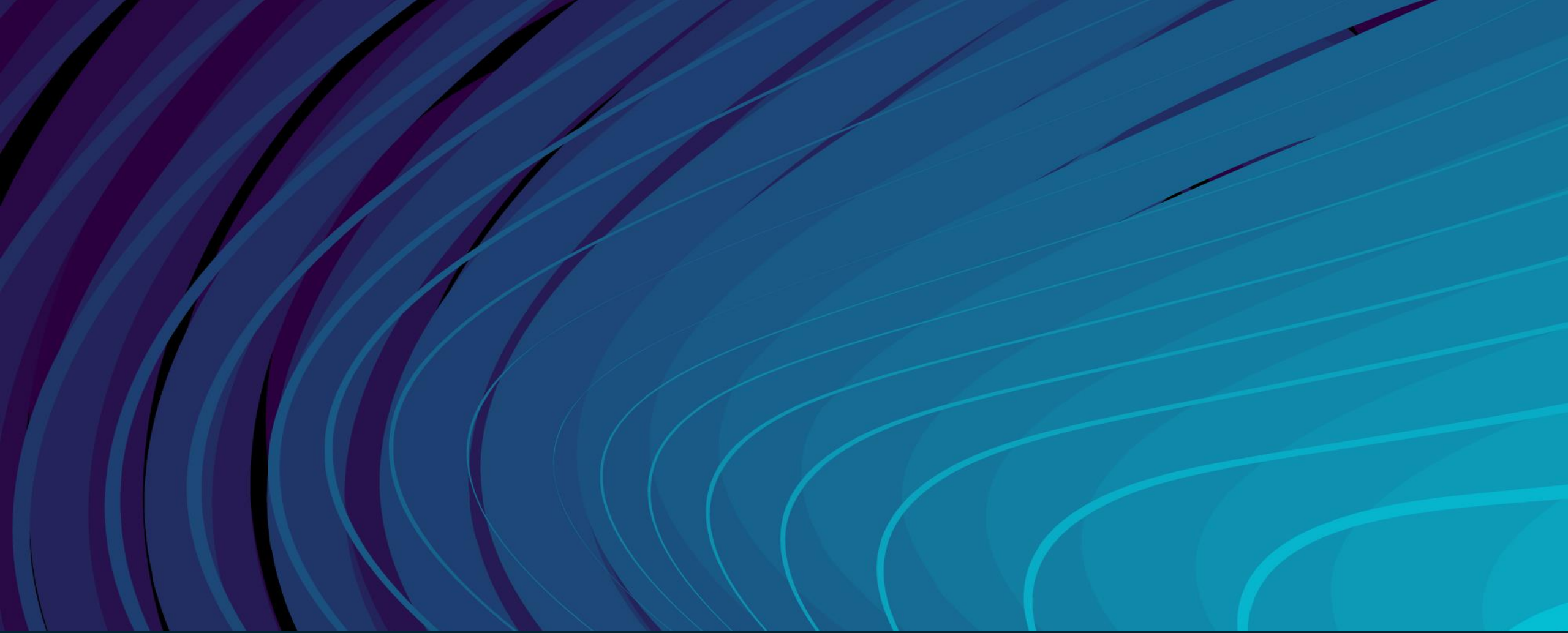




Data Access Control with Microsoft Cloud App Security



15-year proven track record of delivering end-to-end digital transformation, harnessing data insights, and enhancing ROI for global clients.

Who We Are

AVASOFT is a leading digital transformation strategy company that offers enterprises a holistic, product-centric approach to digital transformation by combining strategic planning with a proprietary AI-powered implementation methodology.

With over 15+ years of experience and a team of more than 1,000 technologists, we are committed to harnessing bleeding-edge technologies to provide all our clients with maximum ROI from their technology platforms.

1,500+

Team members
world-wide

Locations

Ireland | USA | Canada | India

What you get with this

Data Access Control with Microsoft Cloud App Security

Your data shielded against today's ever-evolving cyber threats?

Thorough Evaluation:

- Comprehensive assessment of data access controls in Microsoft Cloud apps.
- Evaluation covers infrastructure, configurations, access controls, and data handling practices.

Tailored Recommendations:

- Personalized guidance on critical vulnerabilities for quick mitigation.
- Recommendations aligned with business goals to ensure effective security measures.



Enhanced Data Security

With Microsoft Cloud App Security (MCAS), regain control over your data access. Prevent unauthorized access attempts and protect your sensitive information from external threats.



Real – Time Monitoring

Gain real-time visibility into data access activities across your cloud applications. Detect and respond to suspicious behavior promptly, mitigating the risk of data breaches and insider threats.



Threat Intelligence

Access advanced threat intelligence and analytics to identify and respond to potential security threats promptly, minimizing the impact of cyber attacks.

Our eccentric features of

Data Access Control with Microsoft Cloud App Security

Find the most recent stats below:

- According to the 2021 Cost of a Data Breach Report by IBM, the average cost of a data breach is \$4.24 million
- Research from McAfee indicates that insider threats account for approximately 43% of data breaches, making proactive data access control essential.



Activity Monitoring

Monitor user activities, file movements, and data access events in real-time to detect and respond to security incidents promptly.



Shadow IT Discovery

Identify and manage unsanctioned cloud applications used within your organization, mitigating the risk of data leakage and compliance violations.



Access Control Management:

Implement granular access controls to ensure that only authorized users have access to your cloud applications, reducing the risk of unauthorized access and data breaches.

Implementation Scope - Data Access control with Microsoft Cloud App Security



Data Loss Prevention (DLP) Policies

- Data Loss Prevention (DLP) Policies to prevent unauthorized sharing or transmission of sensitive data



Policy Enforcement

- Granular control over access permissions to safeguard sensitive data.
- Role-based access controls (RBAC) enable precise allocation of privileges.
- Policy violation alerts prompt immediate action to rectify breaches and reinforce security measures.



Shadow IT Discovery

- Identification and assessment of unauthorized cloud applications and services.
- Comprehensive visibility into the extent of shadow IT usage within the organization.



Conditional Access Policy

- Enforce access controls based on conditions such as user identity, device health, location, and application sensitivity. For example, require multi-factor authentication (MFA) for accessing sensitive data from unmanaged devices.



Security Monitoring and Logging

- Track user activities and system events.
- Analyze logs for security incidents.
- Receive real-time alerts and notifications for suspicious activities.



Anomaly Detection Policies

- Configure policies to detect abnormal user behavior, login attempts, or data access patterns that deviate from typical usage, triggering alerts for further investigation and remediation.

How we do – Data Access Control with Microsoft Cloud App Security

Phases - Implementation

1



Define

- AVASOFT defines goals and business requirements for robust cyber defense.
- We focus on understanding your needs and essential response functionalities.

2



Design

- **Solution Architecture** : We define the Proposed security architecture for the organization
- **Customization** : Configure features and policies based on your specific needs and security posture

3



Development

- **Secure Testing Environment** : Create a replica of your application environment for controlled testing and deployment
- **MCAS Configuration** : Implement the customized security plan within the testing environment
- **Rigorous Testing** : Perform thorough testing to validate functionality, identify potential issues and customize performance

4



Deployment

- **Pilot Rollout** : Implement MCAS for small group of pilot users from the organization
- **Continuous Monitoring**: Monitoring the performance, identify and address the issues faced and ensure the ongoing effectiveness.



Thank You