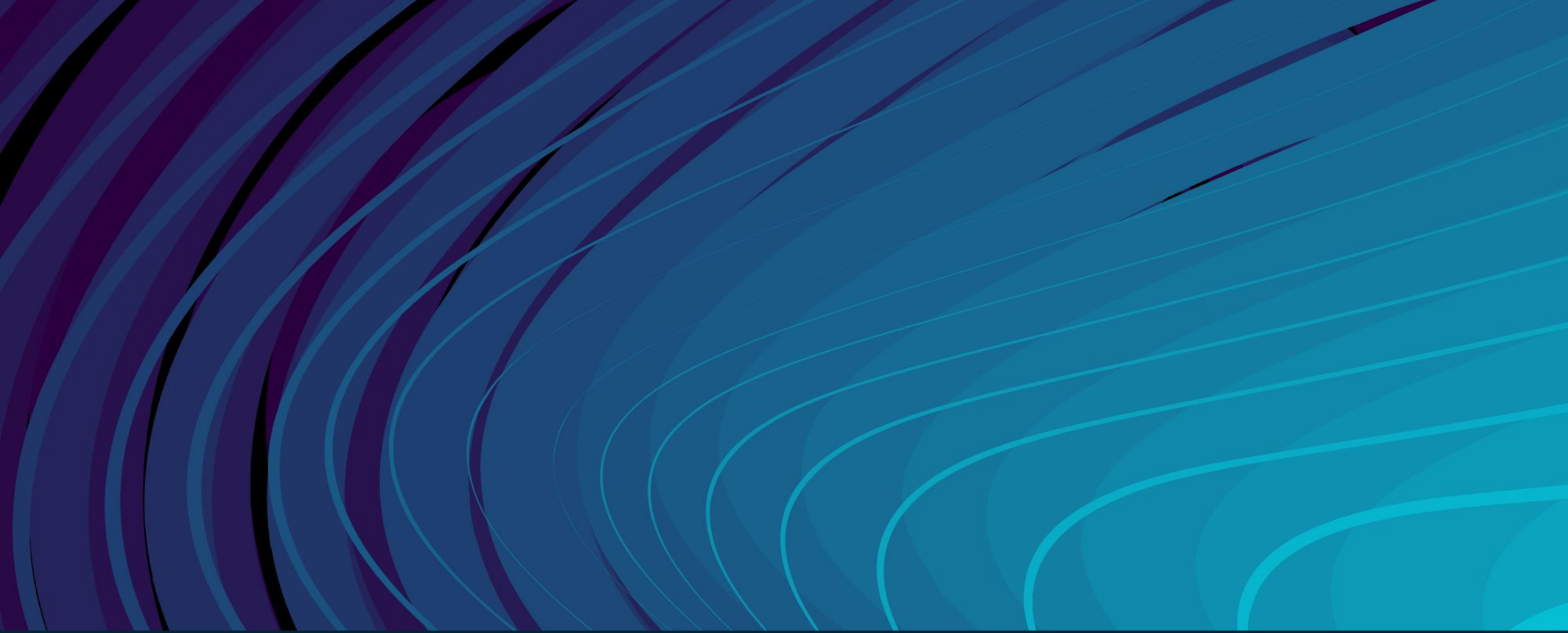




Microsoft Defender for Endpoints and Microsoft Cloud App Security Implementation for Application



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

Microsoft Defender for Endpoints and Microsoft Cloud App Security Implementation for Application

- Is your business equipped to defend against today's evolving cyber.
- Comprehensive Assessment: We meticulously analyze your Microsoft Cloud applications' infrastructure, configurations, access controls, and data handling practices to identify security gaps.
- Personalized Guidance: Get tailored recommendations aligned with your business objectives and security needs. We prioritize critical vulnerabilities for quick mitigation to ensure your security measures match your goals.
- Insightful Reporting: Access detailed reports filled with actionable insights. Our reports empower you to strengthen defenses effectively and make informed decisions to proactively protect your Microsoft Cloud applications.



Zero – Day Protection

Stay protected against zero-day exploits and unknown malware with proactive threat detection mechanisms that analyze behavior patterns and detect anomalies in real-time.



Integrated Incident Response

Seamlessly coordinate incident response efforts with built-in orchestration and automation capabilities. Respond swiftly to security incidents, minimize downtime, and mitigate potential damage to your business



Cloud – Native Security Controls

Leverage native integrations with leading cloud platforms such as Microsoft Azure to enforce granular security controls and protect data at every layer of your cloud environment.

Our eccentric features of Microsoft Defender for Endpoints and Microsoft Cloud App Security Implementation for Application

Find the most recent stats below:

- **73%:** Proportion of cloud breaches due to misconfigured security settings or inadequate access controls (Verizon, 2023).
- **67%:** Increase in cyber-attacks targeting businesses over the past five years, emphasizing the critical need for robust endpoint and cloud security solutions.
- **68%:** Organizations that have experienced a cloud security incident within the last year, underscoring the importance of proactive measures to protect sensitive data.



Integrated Incident Response

Seamlessly coordinate incident response efforts with built-in orchestration and automation capabilities. Respond swiftly to security incidents, minimize downtime, and mitigate potential damage to your business.



Cloud Native Security Controls

Leverage native integrations with leading cloud platforms such as Microsoft Azure to enforce granular security controls and protect data at every layer of your cloud environment.



User and Entity Behavior Analytics

Identify anomalous behavior patterns and insider threats by analyzing user activity and entity interactions. Detect suspicious activities in real-time and take proactive measures to prevent security breaches.

Implementation Scope – Microsoft Defender for Endpoints and Microsoft Cloud App Security Implementation for Application



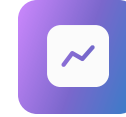
Discovery and Inventory

- Identify all applications within the environment that require MDE and MCAS implementation.
- Create a comprehensive inventory detailing application types, usage, and criticality.



Information (Data) protection

- Define security policies and rules within MDE and MCAS to enforce desired security controls.
- Configure policies for threat detection, data protection, access controls, and compliance management tailored to each application's requirements.



Monitoring and Optimization

- Deploy monitoring mechanisms for continuous performance and security monitoring of MDE and MCAS implementations.
- Collect monitoring data to assess the effectiveness of configurations and policies.



User Behavior Analysis

- Analyzing user activities within Microsoft 365 applications to detect anomalous behavior and potential security threats.



Security Monitoring and Logging

- Monitor user activities and system events in real-time.
- Analyze logs to detect and respond to security incidents effectively.
- Stay informed with immediate alerts and notifications for any suspicious activities detected.



Shadow IT Discovery

- Evaluate risks associated with cloud applications.
- Receive alerts for potentially risky cloud usage.

How we do – Microsoft Defender for Endpoints and Microsoft Cloud App Security Implementation for Application

Phases – Assessment

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, Identity and address the issues faced and ensure the ongoing effectiveness.



Thank You