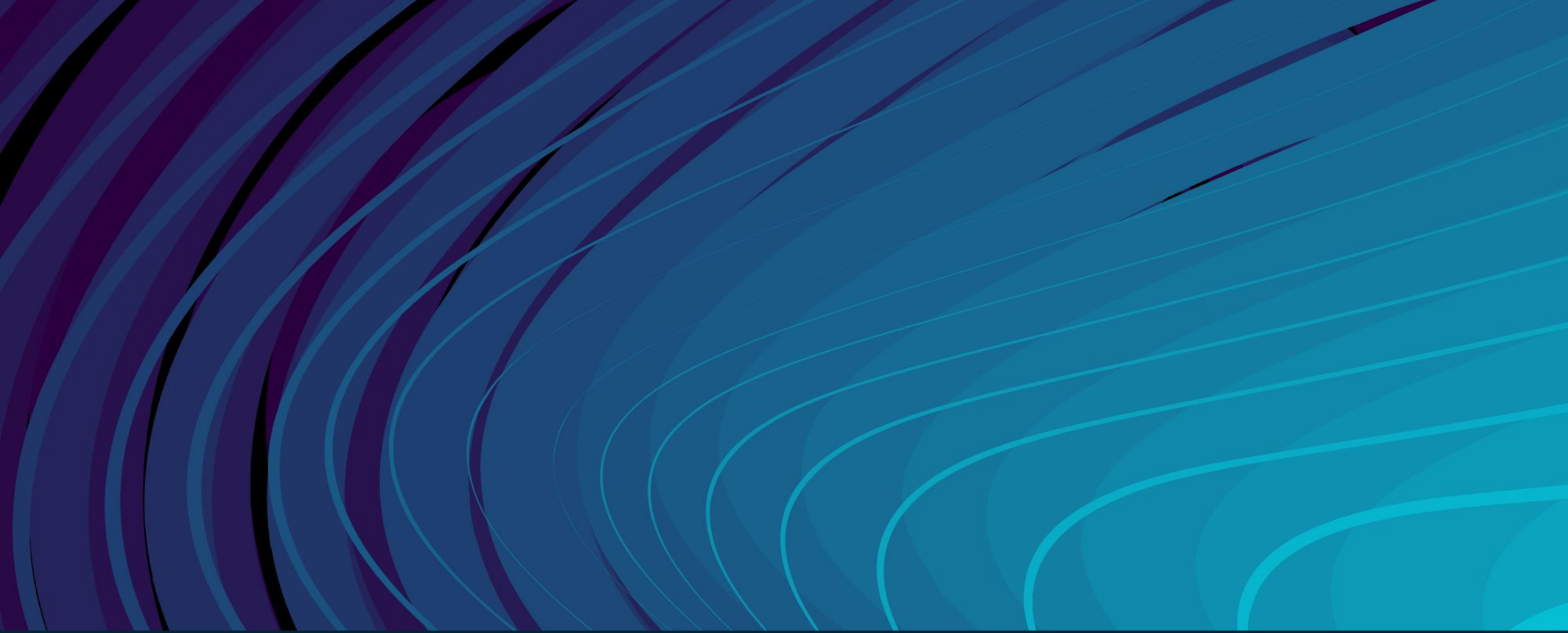




# Teams and SharePoint Security Implementation



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 Teams and SharePoint Security implementation

- Is your organization's digital fortress strong enough to withstand modern cyber threats?
- Thorough Assessment: We conduct a comprehensive assessment of your Teams and SharePoint environment, identifying security gaps in infrastructure, configurations, access controls, and data handling practices.
- Customized Solutions: Receive tailored recommendations addressing critical vulnerabilities, ensuring swift mitigation strategies that align with your organizational objectives.
- Actionable Intelligence: Gain access to detailed reports providing actionable insights, empowering you to make informed decisions that bolster defenses and safeguard your Teams and SharePoint infrastructure.



### Proactive Risk Management

Identify and address potential security threats preemptively, minimizing the risk of data breaches and business disruptions.



### Enhanced protection

Strengthen your digital infrastructure to reduce the risk of unauthorized access, data breaches, and cyber attacks, ensuring the integrity and confidentiality of sensitive information.



### Productivity and Collaboration

Foster a culture of trust and collaboration by ensuring data confidentiality, enabling employees to share, collaborate, and access information securely, leading to increased productivity and innovation..

Our eccentric features of

# Microsoft teams and SharePoint Security implementation

- Find the most recent stats below:
  - According to Cybersecurity Ventures, cybercrime damages are projected to reach \$6 trillion annually by 2021
  - The Ponemon Institute found that the average cost of a data breach is \$3.86 million.
  - Microsoft reported a 250% increase in Teams usage during the COVID-19 pandemic, underscoring the critical need for secure collaboration platforms



## Granular Access Control

Monitor your cloud applications in real-time, detecting and responding to security incidents as they occur to minimize potential damage.



## Secure Integration

Facilitate seamless and secure integration with other enterprise systems and applications using secure APIs and authentication protocols.



## Advanced Threat Detection

Deploy sophisticated mechanisms to detect and respond to security threats in real-time, leveraging AI-driven analytics and behavior-based monitoring.

# Implementation Scope – Microsoft Teams and SharePoint Security Implementation



## Mass Download Activity Monitoring

- Implement monitoring tools for detecting and logging mass download activities.
- Configure alerts for suspicious download patterns.
- Develop procedures for investigating and responding to unauthorized downloads.



## Mass Deletion Activity Prevention

- Configure access controls to limit mass deletion permissions.
- Implement versioning and recycle bin retention policies.
- Establish audit trails for tracking deletion activities.



## Malware Detection and Prevention in SharePoint

- Deploy anti-malware solutions for scanning uploaded files.
- Configure real-time scanning to block malware.
- Maintain up-to-date malware definition databases..



## External communication & Sharing Monitoring

- Enable logging and auditing for tracking external sharing.
- Implement access controls for restricting external sharing.
- Establish approval workflows and user training for responsible sharing.



## Public Access Control

- Review and assess files with public access.
- Implement access controls to restrict public access.
- Conduct periodic audits to revoke unnecessary public access..



## Continuous Monitoring and Improvement

- Establish automated monitoring processes for assessing security posture.
- Conduct regular security audits and risk assessments.
- Implement a feedback loop for addressing security concerns promptly.

# How we do – Microsoft Teams and SharePoint security implementation

## 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, identity 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**