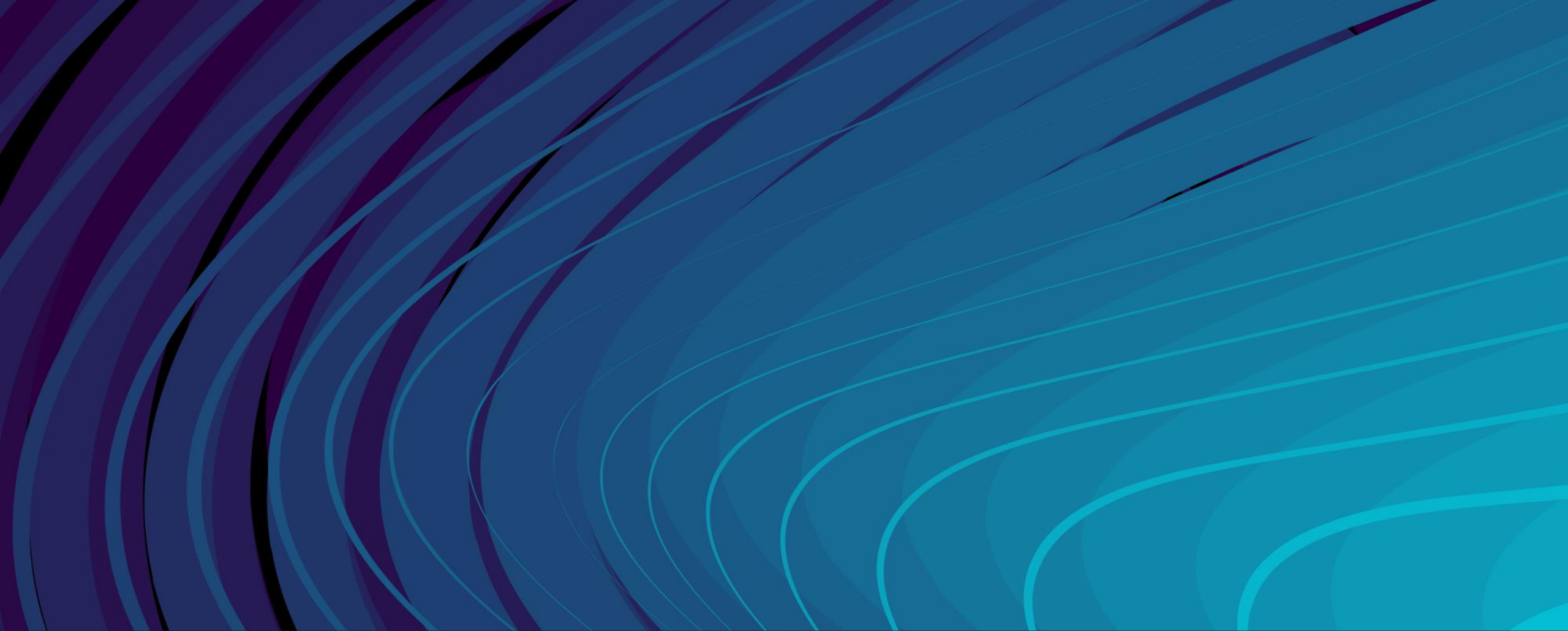




Teams and SharePoint Security Hardening



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 Hardening

- 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.



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.



Data Protection

- Promote a culture of trust and collaboration within Teams and SharePoint through robust security measures, guaranteeing data confidentiality and empowering employees to securely share, collaborate, and access information.

Our eccentric features of **Microsoft teams and SharePoint Security Hardening**

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 for Microsoft Teams and SharePoint Security Hardening



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.



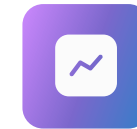
External Sharing Monitoring

- 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.

What we do – Microsoft Teams and SharePoint Security Hardening



Security Infrastructure Implementation

- Deploy monitoring tools and configure access controls to detect and prevent unauthorized mass download and deletion activities, as well as external sharing.
- Implement anti-malware solutions and maintain up-to-date databases to ensure malware detection and prevention in SharePoint.



Policy Development and Enforcement

- Develop procedures for investigating and responding to unauthorized downloads and establish approval workflows for responsible sharing.
- Configure versioning, recycle bin retention policies, and access controls to enforce security policies and prevent mass deletion activities.



Compliance Assurance and Risk Management

- Ensure compliance with regulatory requirements by enabling logging and auditing for tracking external sharing and public access.
- Conduct periodic audits to review files with public access and revoke unnecessary permissions to mitigate security risks and maintain data integrity.

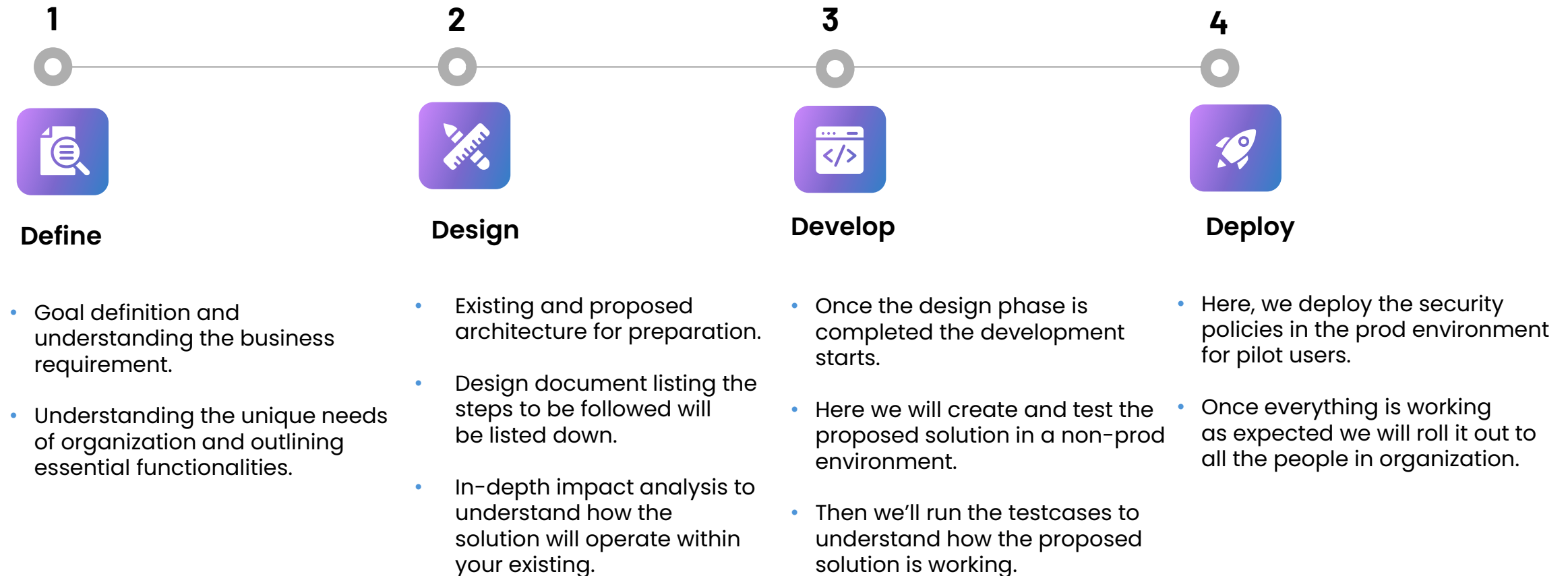


Continuous Monitoring

- Establish automated monitoring processes for continuous assessment of security posture and conduct regular security audits and risk assessments.
- Implement a feedback loop to address security concerns promptly and make necessary improvements to enhance overall security measures.

How we do - Resource efficiency with Azure

Phases - Implementation





Thank You