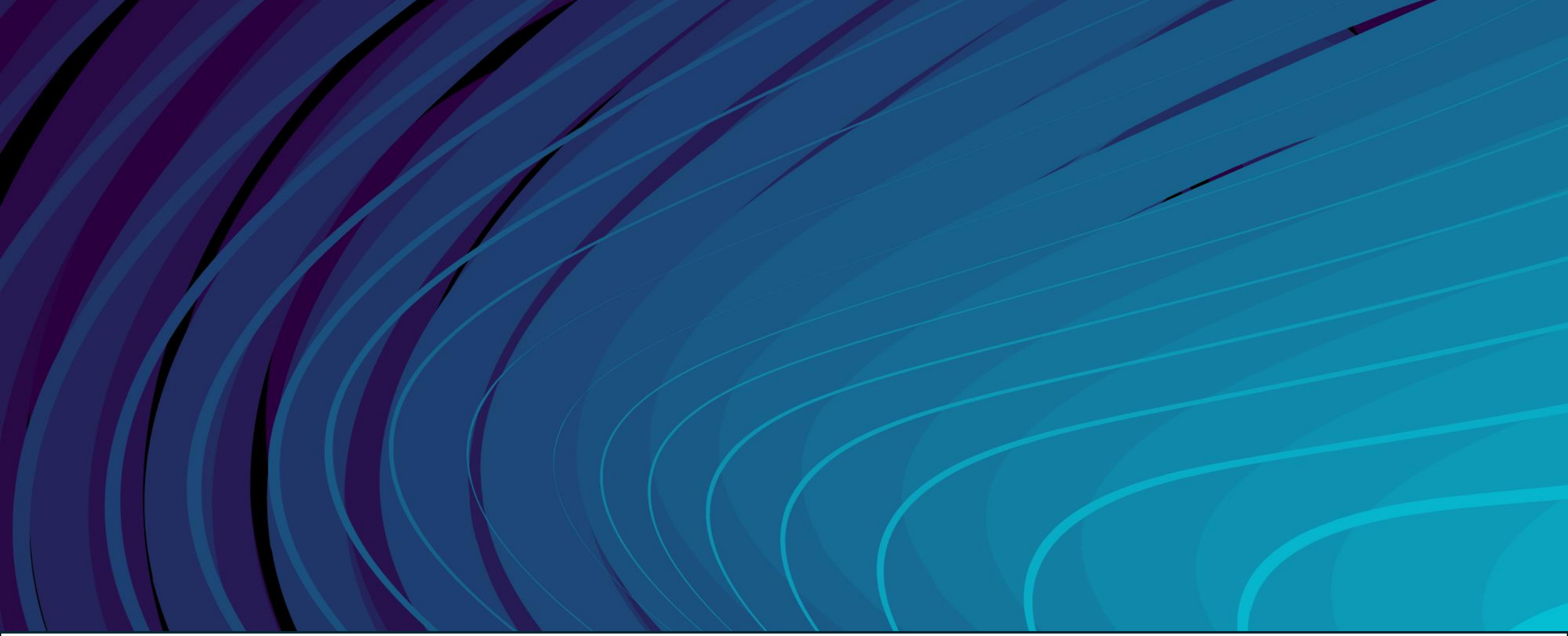
AVASOFT
SHAPING NEXT GEN

Device Monitoring with Microsoft Defender for Endpoint



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

Device Monitoring with Microsoft Defender for Endpoint

- Considering migrating your devices from on-premises to the cloud?
- Our specialized Device Migration Vulnerability Assessment ensures a secure transition while fortifying your cloud environment against emerging threats.
- Our assessment meticulously examines every step of your device migration journey, uncovering potential vulnerabilities that could compromise data security.
- Minimize disruptions and ensure a seamless transition with enhanced security measures

Enhanced Security

- Stay proactive against evolving cyber threats with real-time monitoring and response capabilities.
- Ensuring you stay ahead of potential security breaches by leveraging Microsoft Defender for Endpoint .

Cloud Based EDR Solutions

- Utilize cloud-based EDR solutions to detect and respond effectively to evolving threats.
- Access advanced real-time capabilities for swift threat detection and response.
- Ensure robust endpoint security, safeguarding against emerging cyber threats with comprehensive measures.

Automated Incidence and Response

- Overcome the challenge of promptly identifying and responding to security incidents with automated incident and response solutions.
- Streamline the process to ensure swift detection and mitigation of threats.
- Enhance your organization's overall security posture with efficient incident management and response capabilities.

Our eccentric features of

Device Monitoring with Micrsoft Defender for Endpoint

Find the most recent stats below:

- **68%** of organizations have experienced a security incident that went undetected for over a month
- **50%** of breaches involve the use of stolen credentials.
- The average time to identify and contain a data breach is **280 days.**

Centralized Log Repository

- Consolidate logs from diverse sources such as servers, applications, networks, and cloud services into a centralized repository for easy access and analysis.

Real-Time Monitoring

- Monitor logs in real-time to detect anomalies, suspicious activities, and performance deviations, enabling proactive intervention and threat mitigation.

Customized Dashboards and reports

- Create custom dashboards and reports tailored to your organization's specific needs and requirements to see the overall status of devices from various Microsoft software. Get reports for incidents alerts.

Implementation Scope - Device Monitoring with Microsoft Defender for Endpoint

Inventory

- Gain insight into organization's technology assets for informed decisions.
- Determine prerequisites for implementation.

Assessment

- Identify areas for improvement and innovation.
- Monitor activities and domains for security.

Framing Security Policies

- Use inventory and assessment as foundation.
- Formulate policies based on findings.

Continuous Monitoring

- Monitor logs for issues or abnormalities.
- Utilize predictive analytics for efficient monitoring.

Post-implementation Support Service

- Access expert assistance for IT issues.
- Ensure optimal performance and reliability.

How we do - Device Monitoring with Microsoft Defender for Endpoint

Phases - Implementation

1

Define

- Goal definition and understanding the business requirement.
- Understanding the unique needs of organization and outlining essential functionalities.

2

Design

- Existing and proposed architecture for preparation.
- Design document listing the steps to be followed will be listed down.
- In-depth impact analysis to understand how the solution will operate within your existing.

3

Development

- Once the design phase is completed the development starts.
- Here we will create and test the proposed solution in a non-prod environment.
- Then we'll run the testcases to understand how the proposed solution is working.

4

Deployment

- Here, we deploy the security policies in the prod environment for pilot users.
- Once everything is working as expected we will roll it out to all the people in organization.

Benefits - Device Monitoring with Microsoft Defender for Endpoint

- Stay proactive against evolving cyber threats with real-time monitoring and response capabilities, ensuring you stay ahead of potential security breaches by leveraging Microsoft Defender for Endpoint.
- With cloud-based EDR solutions, businesses can overcome the challenge of detecting and responding to evolving cybersecurity threats across their endpoints. Gain access to advanced threat detection and response capabilities, ensuring real-time protection and enhanced security for your organization.
- With automated incident and response solutions, organizations can overcome the challenge of promptly identifying and responding to security incidents. Streamline the process to ensure swift detection and mitigation of threats, enhancing your organization's overall security posture.
- Manage security policies and configurations centrally from a single console for enhanced efficiency & seamlessly

  integrate with other Microsoft security solutions for a cohesive defense strategy.

AVASOFT
SHAPING NEXT GEN

Thank You