LOGICALIS
Architects of Change

Microsoft

Secure AI

Discover, protect, and govern AI usage with Microsoft Security

The Challenge

Generative AI (GenAI) is being adopted at an unprecedented rate, with organisations actively exploring and implementing it in various capacities. While businesses are enthusiastic about the transformative potential of this technology, it also brings a mix of excitement and concern. The advancements driving innovation and new business opportunities simultaneously introduce significant security and governance risks. Primary concerns among leaders around adopting AI include:

- Potential leakage of sensitive data
- Generation of harmful or biased outputs
- Unclear understanding of upcoming regulations and strategies

Microsoft Partner
Azure Expert MSP
Microsoft

Member of
Microsoft Intelligent Security Association
Microsoft Security
Microsoft Verified Managed XDR Solution

The Solution

The Logicalis' solution, leveraging Microsoft Security's robust suite of tools, provides a comprehensive approach to securing AI applications. From discovery and protection to governance and compliance, these solutions ensure that generative AI technologies can be safely and effectively integrated into the workplace, empowering secure productivity.

Enhanced Detection with Microsoft Defender for Cloud Apps

- **New Detections for Copilot for Microsoft 365**: Alerts on risky activates, such as access from untrusted IP addressed
- **Unified Threat Response**: Integrated with Microsoft Defender for XDR for comprehensive threat investigation and response. Logicalis has Microsoft Global MXDR status.

Access Management and Device Security

- **Microsoft Entra Conditional Access**: Enforces policies for secure access to AI applications, ensuring least privileged access.
- **Microsoft Intune**: Protects Copilot-generated data across managed and unmanaged devices, maintaining data security without requiring device enrolment.

Discovery and Protection with Microsoft Purview

- **AI Hub Dashboard**: Provides insights into AI activity and identifies data security risks.
- **Data Security Controls**: Native inte3gration with Copilot ensures sensitive data is protected throughout its lifecycle, leveraging features like encryption, auto-labelling, and data loss prevention (DLP).

Governance and Compliance

- **Integrated Compliance Controls**: Microsoft Purview offers tools for auditing AI usage, managing data retention, and ensuring compliance with regulatory requirements.
- **Communication Compliance**: Detects and mitigates non-compliant AI usage, preserving data for legal and regulatory purposes.

Securing Third Party AI Applications

- **Discovery and Risk Assessment**: Microsoft Defender for Cloud Apps identifies and assesses risks for over 400 GenAI applications.
- **Conditional Access Policies**: Manage access to third-party AI apps, ensuring security through approvals and regular access reviews.
- **Data Loss Prevention**: Prevents sensitive data from being shared with unsanctioned AI apps, using adaptive DLP policies to mitigate insider risks.

About Logicalis

Logicalis offer lifecycle technology solutions across various vendors technologies to help our customers improve IT efficiency, accelerate innovation, and achieve their desired business outcomes. As a Global certified Microsoft Security Partner and one of only a handful of global firms to receive Microsoft Azure Expert MSP status, and a member of the Microsoft Intelligent Security Association (MISA), we are well-positioned to help you make the most of your technology platforms, including AI, IoT, automation, remote work, and cloud, through supporting professional and managed services.

www.logicalis.com | logicalisinfo@logicalis.com