Enhancing Data Security with Microsoft Purview and ML

A study of the importance of tailored solutions in data security and the benefits of leveraging advanced technological tools for organizational data protection.

OVERVIEW

Oakwood worked with a nonprofit organization that's dedicated to serving the Catholic Church through the delivery of professional services with a focus on integrity, ethical practices, and a commitment to the highest standards of performance.

Their mission revolves around providing high-quality, value-centered services that are designed to support and enhance the operational effectiveness of Catholic institutions. They offer a comprehensive suite of services including but not limited to health benefits, retirement plans, property/casualty insurance, and information technology solutions.

This client faced significant challenges in safeguarding Personally Identifiable Information (PII) and Protected Health Information (PHI) during their migration to Microsoft 365. The transition from the outdated Lotus Notes to Microsoft's Cloud platform aimed to capitalize on cloud-based applications, collaboration tools, and advanced security features. However, the efficient identification and secure handling of sensitive data, crucial to meet regulatory compliance and prevent risks like financial penalties, legal issues, and reputational damage, remained a primary concern.

CHALLENGE

The core challenge for them was the accurate identification and classification of PII and PHI in their digital communications and data storage. This was particularly vital in outbound data, where ensuring encryption was mandatory. Their existing systems struggled to recognize various formats of sensitive data, notably U.S. Social Security Numbers (SSNs) presented in unconventional formats like "123.45.6789" or "123/45/6789". The failure of Microsoft's default sensitive information types to detect these variations resulted in potential risks of data misclassification and unsecured data transmission.

SUMMARY

Business Challenge:
the accurate identification and classification of PII and PHI in their digital communications and data storage.

Solution:
Oakwood Systems Group enhanced the client's data security in Microsoft 365 by implementing an advanced data classification system with Microsoft Purview. This system accurately identified and encrypted sensitive information, including a custom format for U.S. Social Security Numbers. The solution ensured compliance with data protection regulations and reinforced their commitment to data security.

Benefits:
The partnership between the client and Oakwood Systems Group resulted in a successful, robust data security system, ensuring effective classification and protection of sensitive information and reinforcing compliance and trust.

SOLUTION

In response, Oakwood Systems Group partnered with the client to deploy a comprehensive data security solution. Utilizing Microsoft Purview's AI and machine learning capabilities, Oakwood introduced a sophisticated data classification system within their digital environment. This system included:

- **Custom Sensitive Information Type**: Oakwood created a custom information type to identify SSNs in various formats. By employing Regular Expressions, the system could accurately recognize and categorize SSNs, overcoming the limitations of Microsoft's default settings.
- **Enhanced Data Classification**: Beyond PII and PHI, this system also classified additional sensitive data, adapting to the diverse and dynamic data environment. This customization ensured comprehensive coverage and minimized the risk of misclassification.
- **Data Loss Prevention Policy**: To secure the transmission of sensitive data, a data loss prevention (DLP) policy was implemented, ensuring encryption of classified data before external sharing.

OUTCOME

The collaborative efforts of Oakwood and their client led to the successful deployment of a robust and precise DLP solution. Regular monitoring and testing ensured the effectiveness of the data classification system, significantly reducing the risks associated with data mismanagement. This not only ensured compliance with regulations but also fortified the trust and reputation of the organization in managing sensitive information. The case exemplifies the importance of tailored solutions in data security and the benefits of leveraging advanced technological tools for organizational data protection.