Microsoft Cloud Apps Security

Cloud App Security helps organizations address these challenges by acting as a Cloud Access Security Broker (CASB), providing security and compliance monitoring, detecting threats, and enforcing policies to protect data and applications in the cloud.

The implementation includes:

- **Shadow IT Discovery**: Discover and monitor unsanctioned cloud apps being used in the organization by analyzing traffic logs.
- **Risk Scoring**: Assign risk scores to cloud apps based on security, compliance, and usage characteristics to identify high-risk applications.
- **Traffic Analysis**: Monitor and analyze cloud app traffic for deeper insights into usage patterns and potential security risks.
- **Data Protection**: Apply DLP policies to prevent sensitive data from being shared or leaked through cloud applications.
- **Sensitive Information Types**: Pre-configured templates for identifying and protecting common types of sensitive data like PII, financial data, and health information.
- **Cloud App Security Alerts**: Receive alerts when suspicious or abnormal activities are detected, such as unauthorized access attempts or high-risk logins.
- **Automated Remediation**: Automatically take actions such as blocking access, alerting administrators, or applying policies when certain conditions are met.
- **External Sharing Detection**: Identify when sensitive data is shared externally or publicly through cloud apps, and enforce appropriate controls to limit sharing.
- **Microsoft Information Protection:** Use Microsoft Information Protection to label and classify sensitive data, applying security measures such as encryption and rights management.

Email : cloudsales@itx360.com

Phone: +94777270822

The estimated cost mentioned in the offer may vary based on the project's scope and user count. For an exact quote, please contact us.