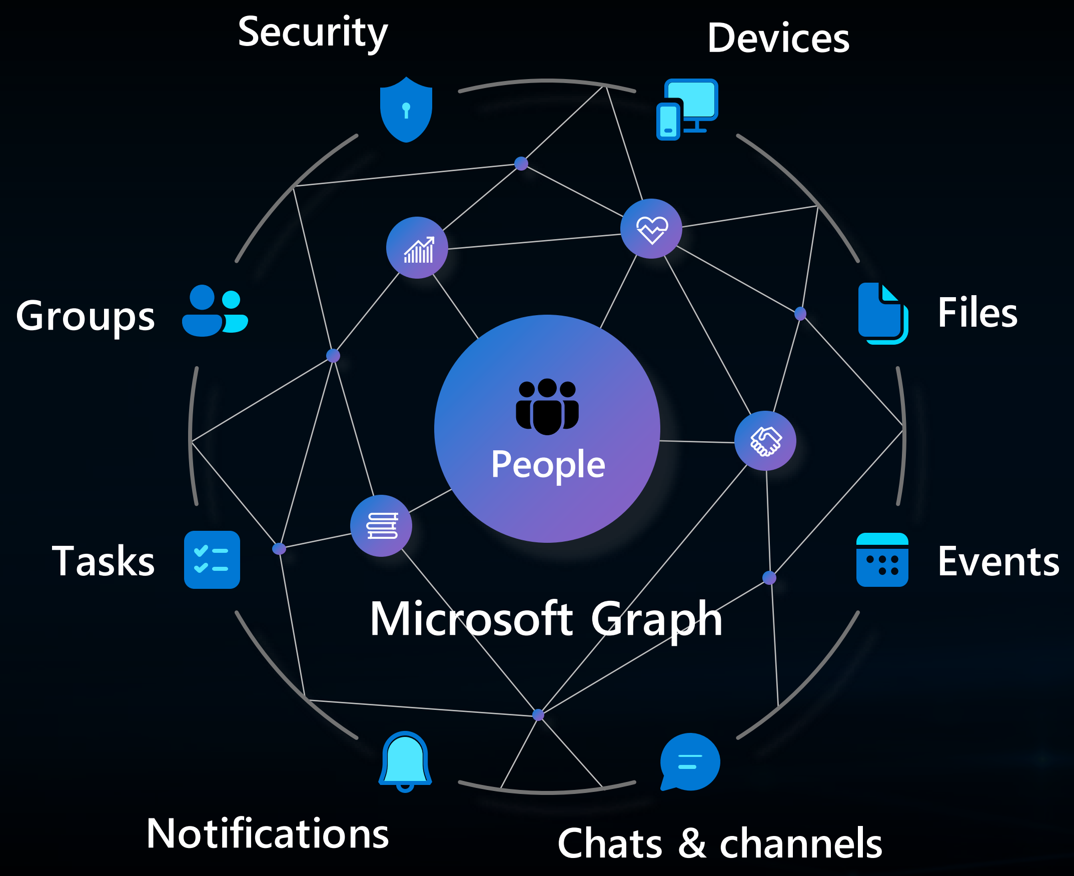
Microsoft

Using Security and Compliance Analytics to Power Business Decisions

Microsoft 365 & Azure Synapse

Collaboration and communication activities generate a massive, rich amount of data in M365



18,000,000,000,000

Microsoft Graph nodes
(emails, users,
files, groups and more)

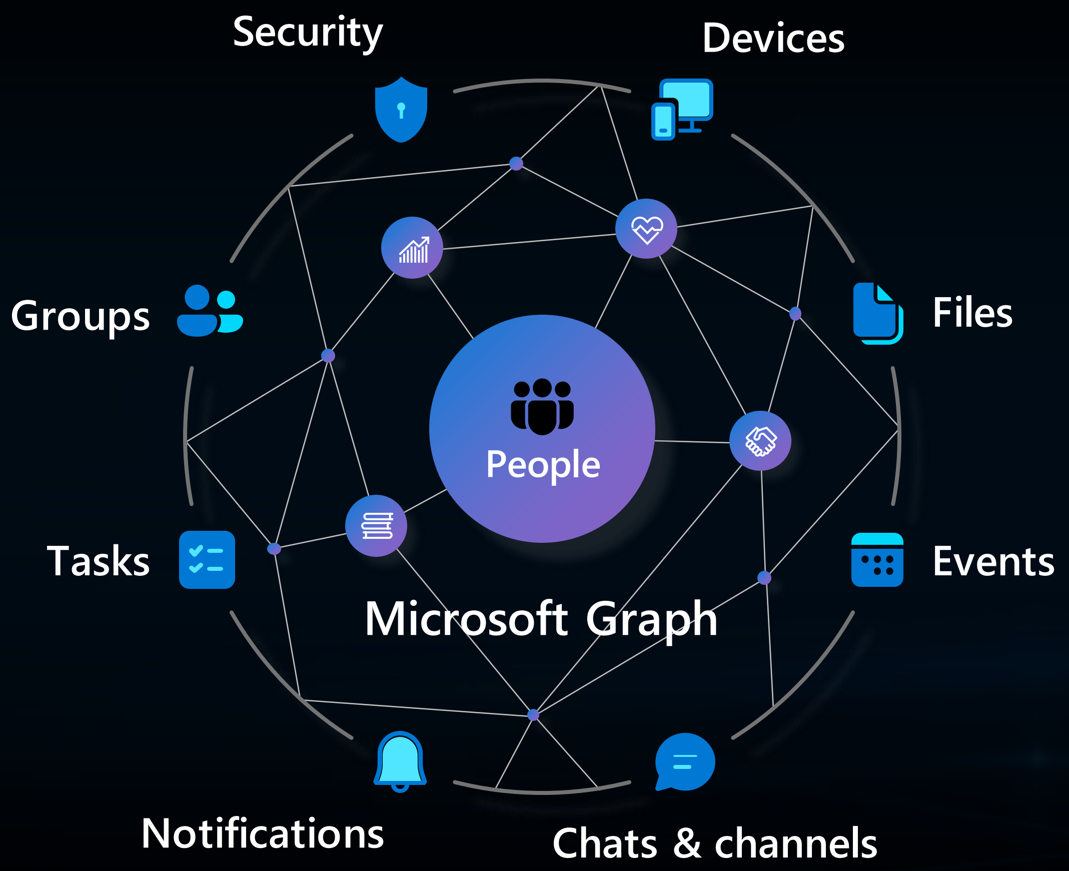
~300 Million

Office365 Users

270 Million

Microsoft Teams users

Collaboration and communication activities generate a massive, rich amount of data in M365



The Opportunity

Secure your business by identifying patterns of information oversharing and fraud in your M365 data

The Opportunity

Secure your business by identifying patterns of information oversharing and fraud in your M365 data

- Uncover false alerts and refocus efforts on genuine threats
- Validate employee intention following questionable activity
- Accelerate investigation of intellectual property theft
- Mitigate regulatory compliance violations

Security & Compliance Analytics Use Cases

Information Oversharing

Validate if sensitive data was mistakenly leaked or if employees intentionally shared confidential information with malicious intent

Fraud Detection

Determine if actions and behaviors between employees violate corporate policies and validate whether there is legitimate risk

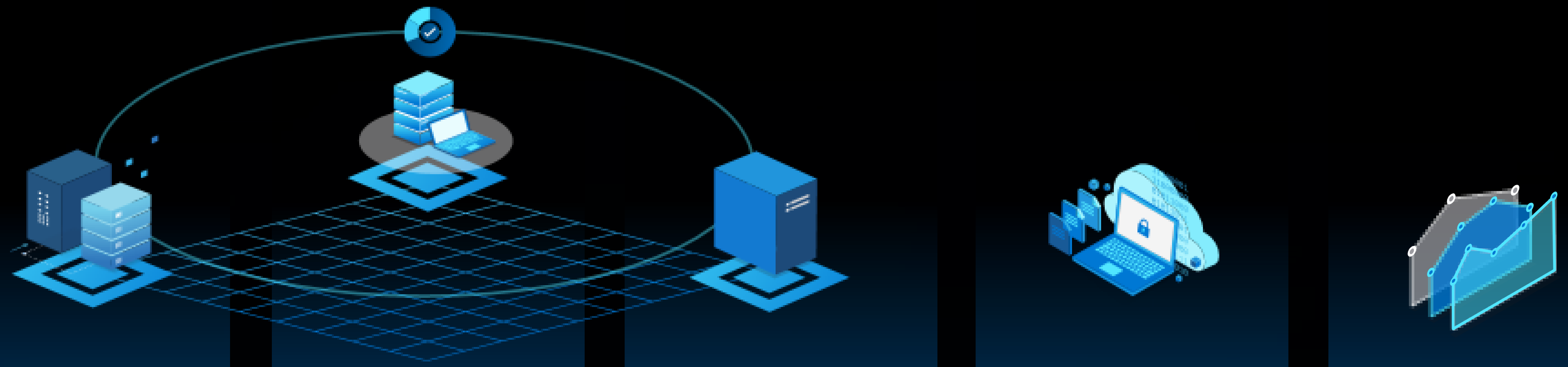
Internal Threat and Anomaly Detection

Detect anomalies in sensitive datasets to protect against internal threats

Security & Compliance Analytics – How it works

Use collaboration data to identify real threats and reduce exposure to risk

- *Outlook*
- *SharePoint*
- *Teams*
- *Viva Insights*
- *Office 365*
- *Azure Active Directory*



1 **Connect** M365 data to Azure Synapse

2 Continuously **collect** and store collaboration data in Azure. **Combine** with other relevant data sources

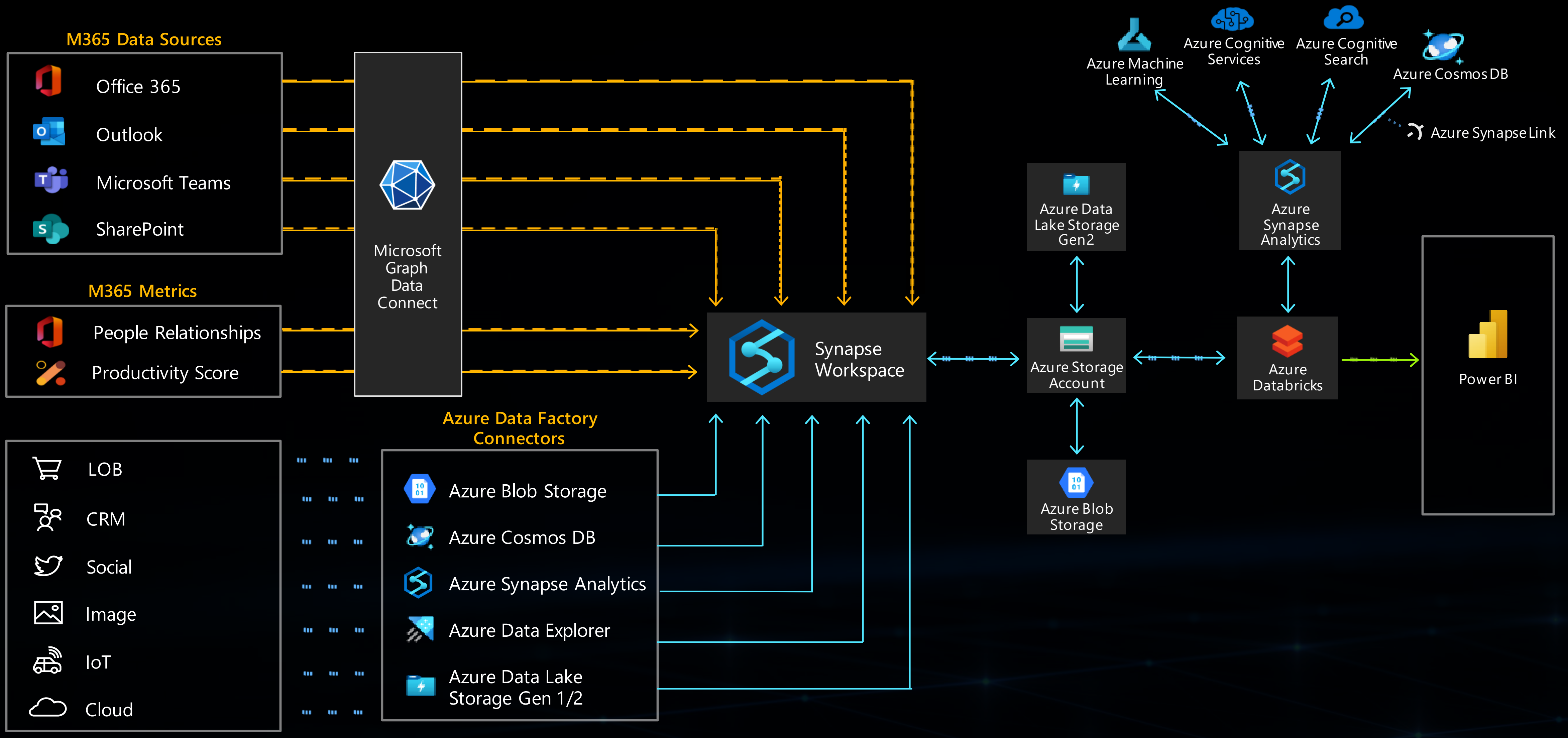
3 Use Azure Synapse to model historical Security & compliance patterns of update threat models

4 Analyze behavioral, collaboration, and data access patterns to detect malicious or noncompliant activity

5 Automate responses and alerts to suspicious behaviors and patterns

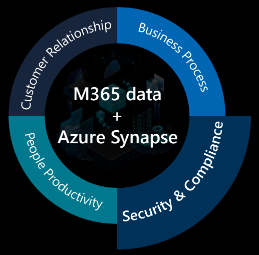
6 Visualize and democratize security and compliance insights with Power BI

M365 Analytics Architecture



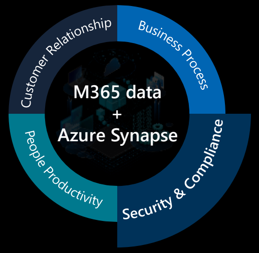
Extend Existing Security & Compliance Insights

Use Cases	Initial Challenge	Initial Solution	Remaining Challenge	M365 Solution
Information Oversharing	Organizations experiencing email data breaches risk exposing confidential data	Data Loss Prevention (DLP) tools mitigate the risk of unauthorized users accessing sensitive data	Many incidents go undetected by static Data Loss Prevention (DLP) tools	Use M365 data to build predictive models to stop data breaches before they happen
Fraud Detection	Inability to detect fraud leads to financial loss, loss of credibility, legal action, and loss of customer trust	Fraud detection software monitors, investigates, and blocks fraudulent activity	Existing fraud detection tools don't leverage the insight available from all the data sources available	Use M365 data to get a complete view of the business and detect fraud faster with greater accuracy using risk scoring models
Internal Threat and Anomaly Detection	Insider threats are difficult to detect and pose serious security risks to an organization	Anomaly detection software identifies data points, events, and observations that deviate from normal behavior and flags for review	Untuned risk models means too much time is spent investigating and ruling out false positives	Use M365 data to generate alerts dashboard by defining risk indicators that match policy conditions. Activities that need investigation go through false alert analysis



Information Oversharing

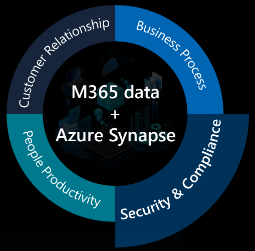
Validate if sensitive data was mistakenly leaked or if employees intentionally shared confidential information with malicious intent



Today's Challenges

- Client and company data is most at risk on email. Organizations experiencing email data breaches risk exposing confidential data
- Inability to predict when a data breach is about to happen and prevent incidents before they happen
- Remote work has dramatically increased the number of emails sent
- Many incidents go undetected by static Data Loss Prevention (DLP) tools. Such tools are often unreliable and difficult to use

Information Oversharing Solution



Understand the behaviors and usage trends to foster positive employee behaviors

Construct an always on, predictive model to act as a safety net to prevent accidental oversharing incidents

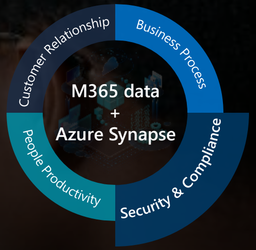
Identify malicious actors and protect confidential data

Set terms to watch for leakage – categorize and assign severity level

BENEFITS

- Build predictive models to stop data breaches before they happen
- Protect confidential client data, maintain constant compliance
- Scale your ML model with the increased volume of email data

Microsoft promotes safer, more secure content management culture through insights from Microsoft Graph Data Connect



BUSINESS CHALLENGE

- The transition from 'classic' attachment sharing (e.g., copies via email or chat) to the use of SharePoint links dramatically increases the **security of sensitive business documents** and helps ensure **legal compliance**
- Anecdotal evidence suggested that Microsoft employees were continuing to share classic documents in collaboration activities, placing the company at **significantly greater risk of unauthorized use**

SOLUTION

- Because Microsoft initially lacked visibility into **SharePoint behaviors and usage trends** which would help influence positive employee behaviors, it sought to fill that gap with **Microsoft Graph Data Connect**
- Data science teams generated robust SharePoint file sharing reports to **understand how content was being shared** across the business

RESULT

- The team at Microsoft revealed the file-sharing behaviors that were prevalent in the organization and used the insights to **develop change management strategies** intended to combat 'classic' attachment sharing
- Product teams are also leveraging these insights to inform the development of **nudges in Outlook** that encourage **safer and more streamlined content management behaviors**

SOLUTION ELEMENTS

Microsoft Graph Data Connect

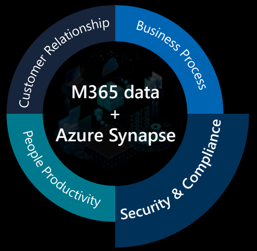
Microsoft 365

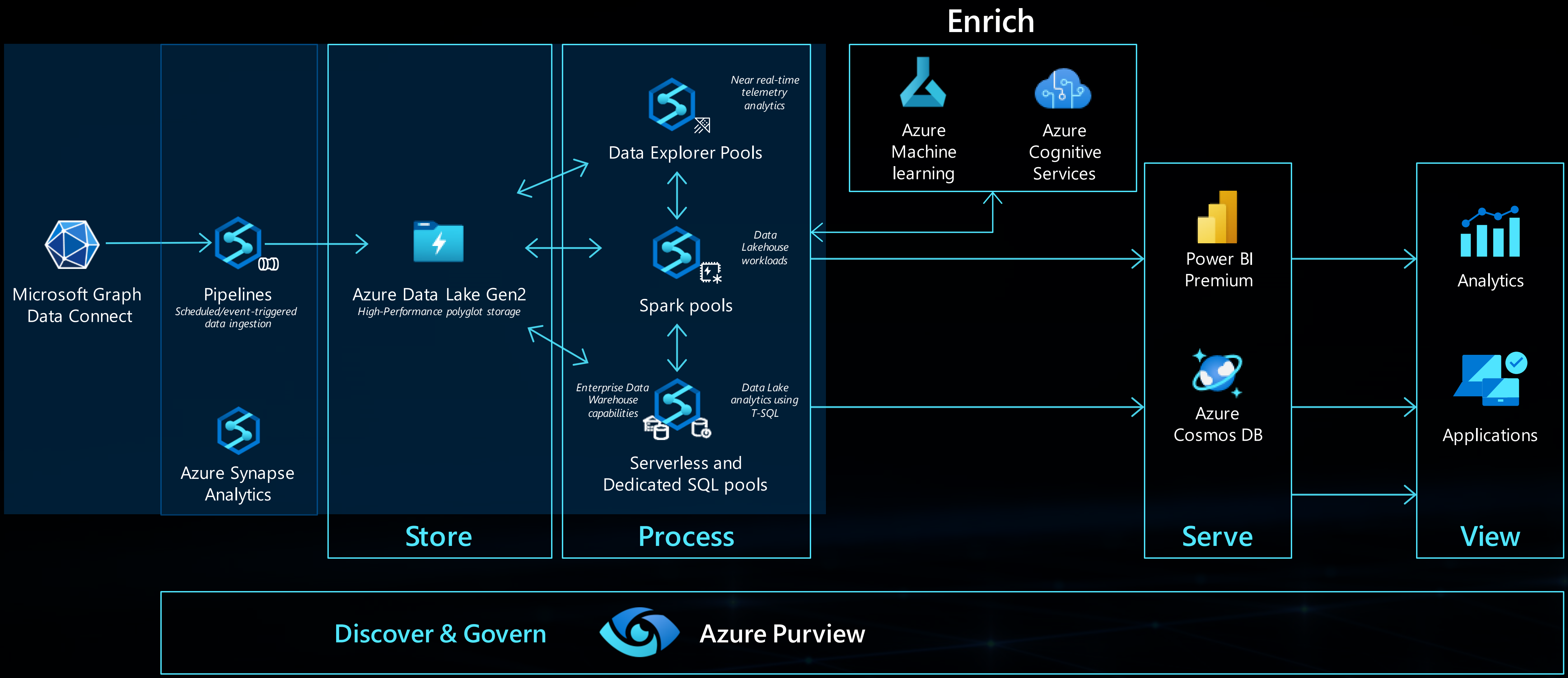
File sharing reports

External data & LOB apps

Azure Synapse

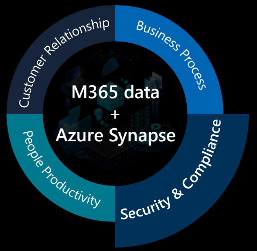
Architecture Overview: Information Oversharing

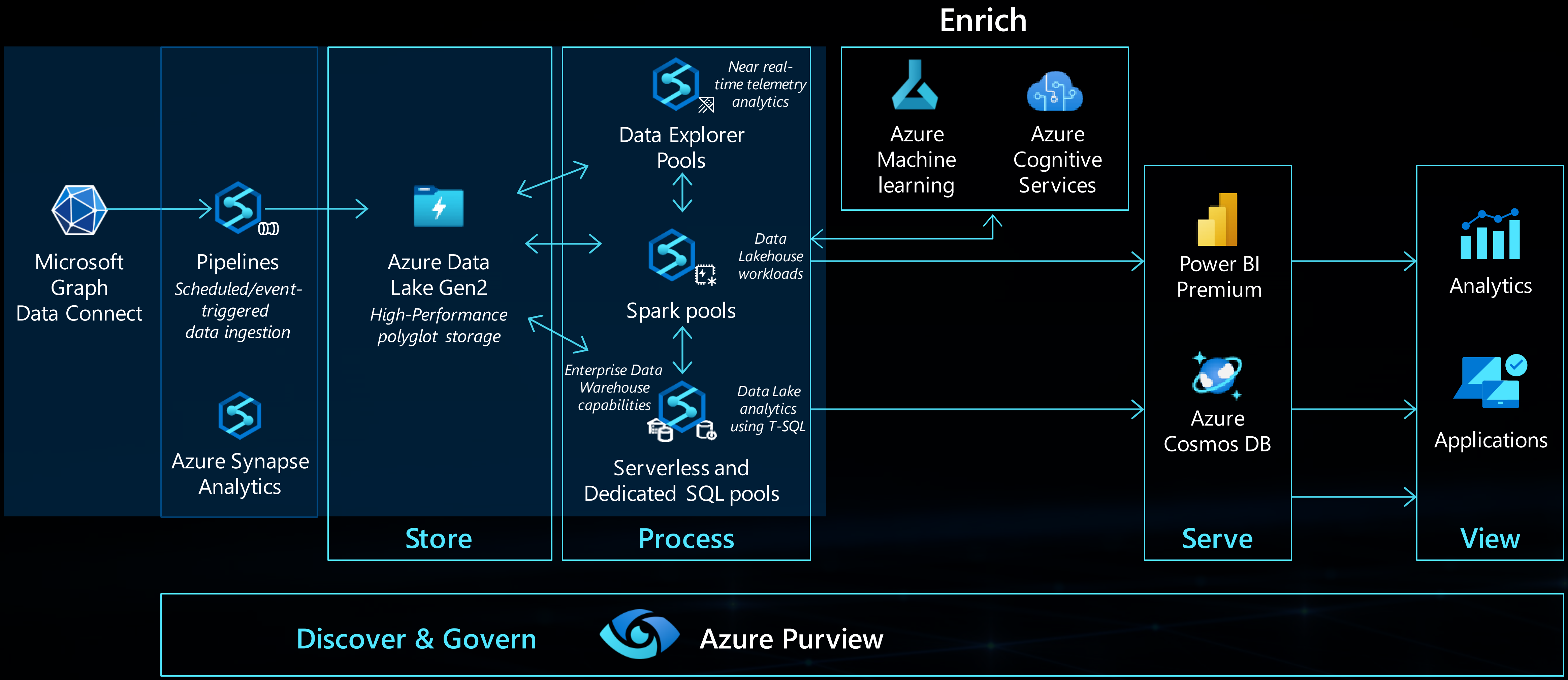


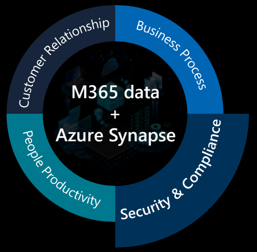


Architecture Overview: Information Oversharing

Learn more:

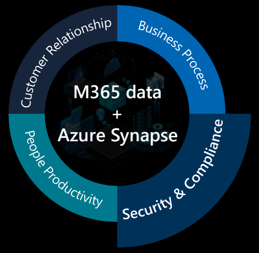






Fraud Detection

Determine if actions and behaviors between employees violate corporate policies and validate whether there is legitimate risk



Customer Relationship

Business Process

M365 data
+
Azure Synapse

People Productivity

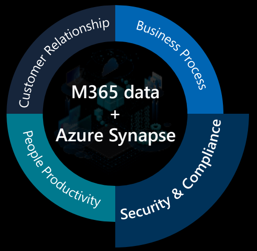
Security & Compliance

Today's Challenges

Reducing the cost and negative customer experience and losses associated with fraud

Existing fraud detection tools may not leverage the insight available from all the data sources available from the bank's specific core banking, customer, telemetry and logs and other data

Fraud Detection Solution



Use big-data analytics + machine learning to model historical patterns of fraud and continuously update threat detection models

Automate responses and alerts to suspicious behaviors and patterns. Visualize and democratize business insights with easy integration of M365 and LOB data with Azure Synapse

Unleash hyper-auto scalability with Azure serverless technologies and Azure Synapse

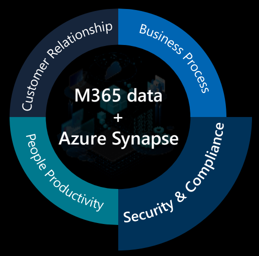
Stay compliant with regional data regulations– keeping key data and apps on-premises, while harnessing cloud technologies to access advanced AI, Analytics, storage and ML

BENEFITS

- **Reduce financial loss** due to fraud with real-time fraud detection tools
- **Uncover hidden insights** within the data such as subtle patterns and suspicious behaviors
- **Detect fraud faster with greater accuracy** in the scoring models

MICROSOFT GRAPH DATA CONNECT – LEAD WITH ANALYTICS

Microsoft enables large processor of debit and credit transactions to better detect and protect against fraud



BUSINESS CHALLENGE

- Need for a unified data platform to better detect and protect against fraud in today's ever-shifting world of commerce

SOLUTION

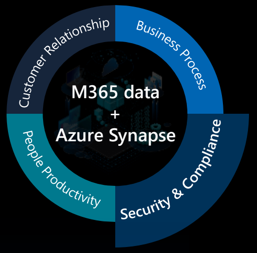
- Rapidly implemented an automated workflow for assessing and prioritizing risk via AI
- As their workflows evolve in sophistication and utility, Azure AI factors increasingly in protecting against fraud

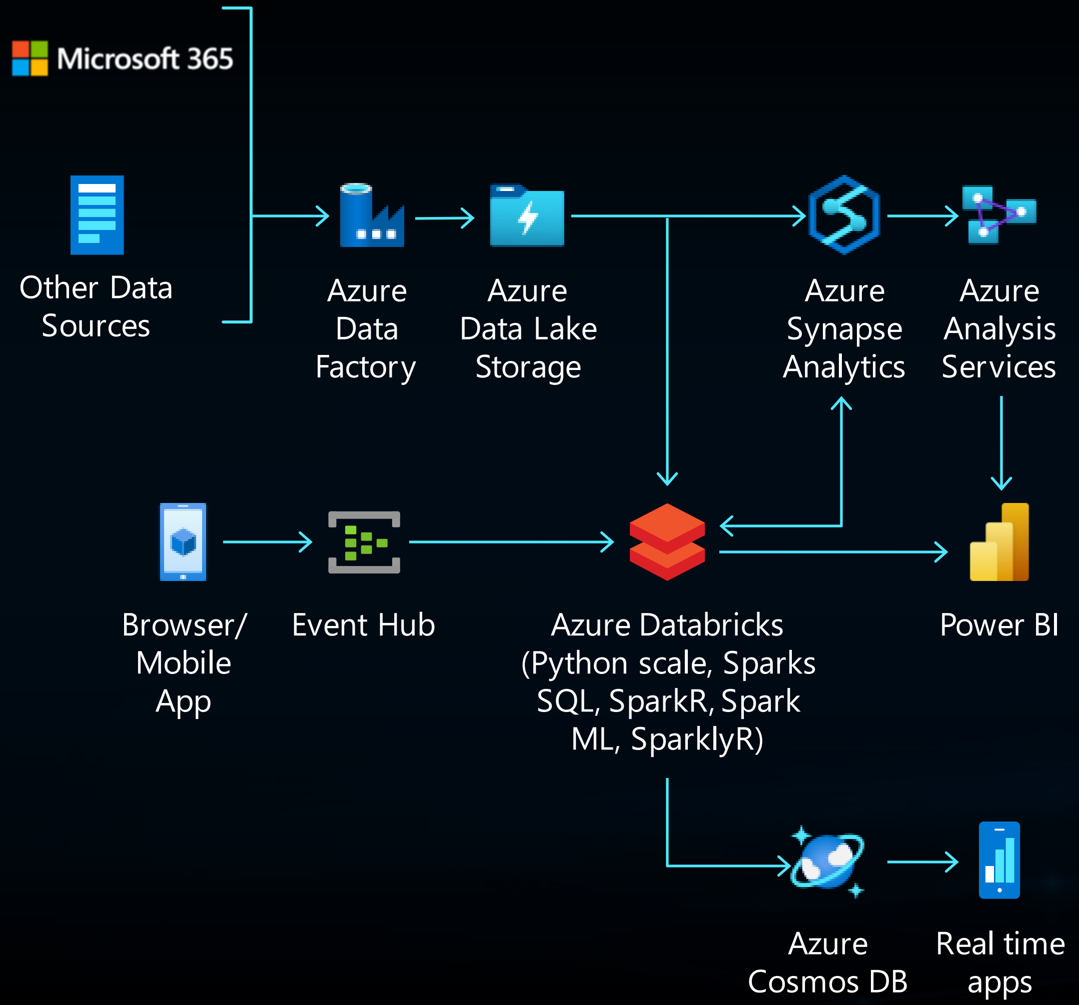
RESULT

- 450% reduction in the time spent identifying potential fraud and an immediate 10 percent reduction in fraud, with potential for that number to increase as it develops and releases new AI-based capabilities

> *Azure offered us the ability to incorporate this solution one step at a time and increase our capacity as we grow. We were able to operate faster immediately and have the flexibility to iterate and refine our approach to AI as new possibilities present themselves*
>
> Director of Data Platforms

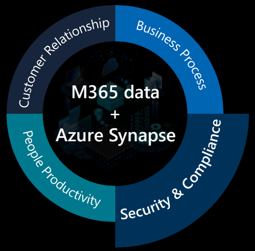
Architecture: Fraud Detection





Technical Hurdles Addressed

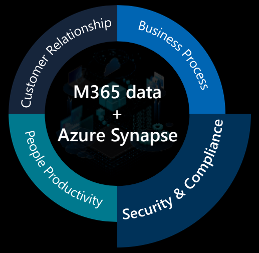
- Challenges with ingestion of huge volumes of real-time data from disparate sources across multiple channels
- Cost effective yet efficient/performant storage for petabyte-scale data sets
- Complex rationalization and normalization of data into a centralized repository
- Easy distribution of data for additional specialized analysis without sacrificing data validation and integrity
- Providing sophisticated data visualization solutions across multiple lines of business and distinct user populations
- Managing near-real time alerting and event handling to enable rapid response (transaction prevention as well as approval



Internal Threat & Anomaly Detection

Detect anomalies in sensitive datasets to protect against internal threats

Today's Challenges



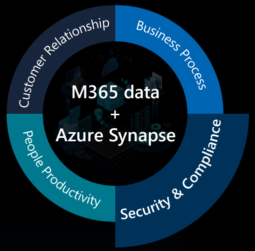
- Whether negligent or malicious, insider threats pose serious security risks to an organization

- 53% of organizations confirmed insider risks against their organization in the previous 12 months

- Insider threats from illegal, inappropriate, unauthorized, or unethical behavior are a major issue for companies and easily go undetected until it is too late

- Too much time is spent investigating and ruling out false positives

Internal Threat & Anomaly Detection Solution



Insider risk management policies are created using pre-defined templates

Alerts are generated by risk indicators are displayed in the Alerts dashboard

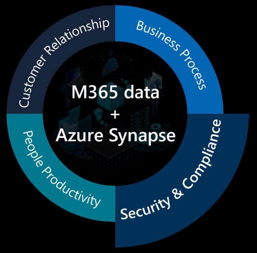
New activities that need investigation go through false alert analysis using M365 data with Azure Synapse

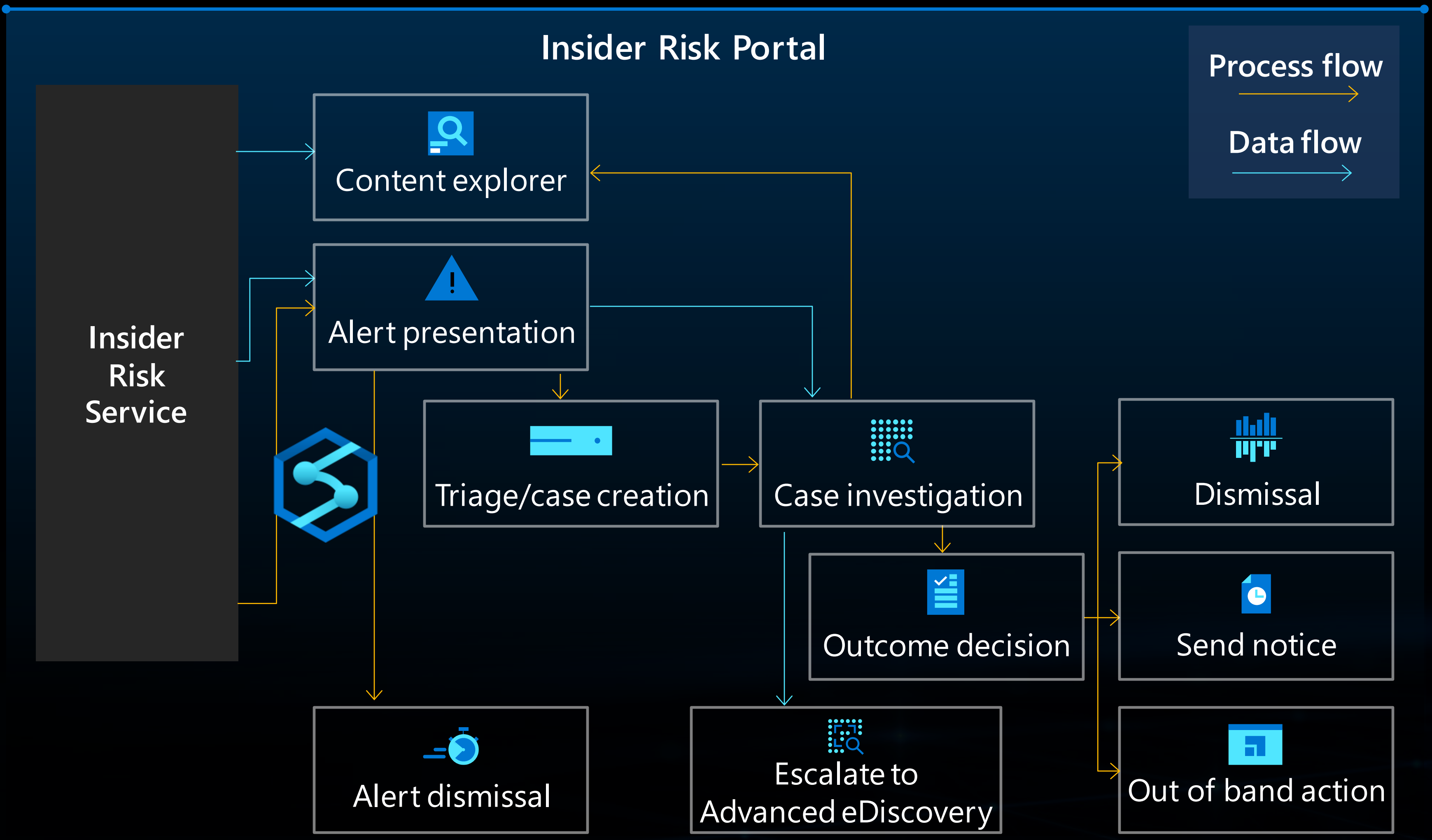
Legitimate alerts are assigned a "needs review" status for reviewers to evaluate and triage

BENEFITS

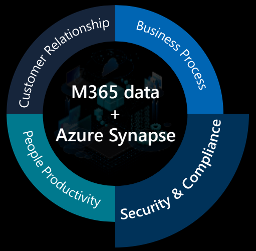
- Reduce operational costs by automating data analysis, and minimizing time spent on false threats
- Enable employees to focus on work that matters and make it easier and quicker to close issues
- Minimize exposure to fraud, litigation, or intellectual property theft

Architecture: Internal Threat & Anomaly Detection





Learn more



Next steps …

- Learn more about how to ingest M365 data in Azure Synapse (Link)
- Align with your business stakeholders for sponsorship, expectations and budget
- Start with business case to develop scenario/use case and supporting solution design

…how Microsoft can help you

- Request MTC Data & AI Architecture Design Session or Rapid Prototype (optional)
- Work with your DAI CSA to do a pilot/ Solution Accelerator (optional)