AccountabilIT
Security Amplified, Cloud Simplified

# Shadow AI **Exposed:** Zero Trust & Shadow AI Threats

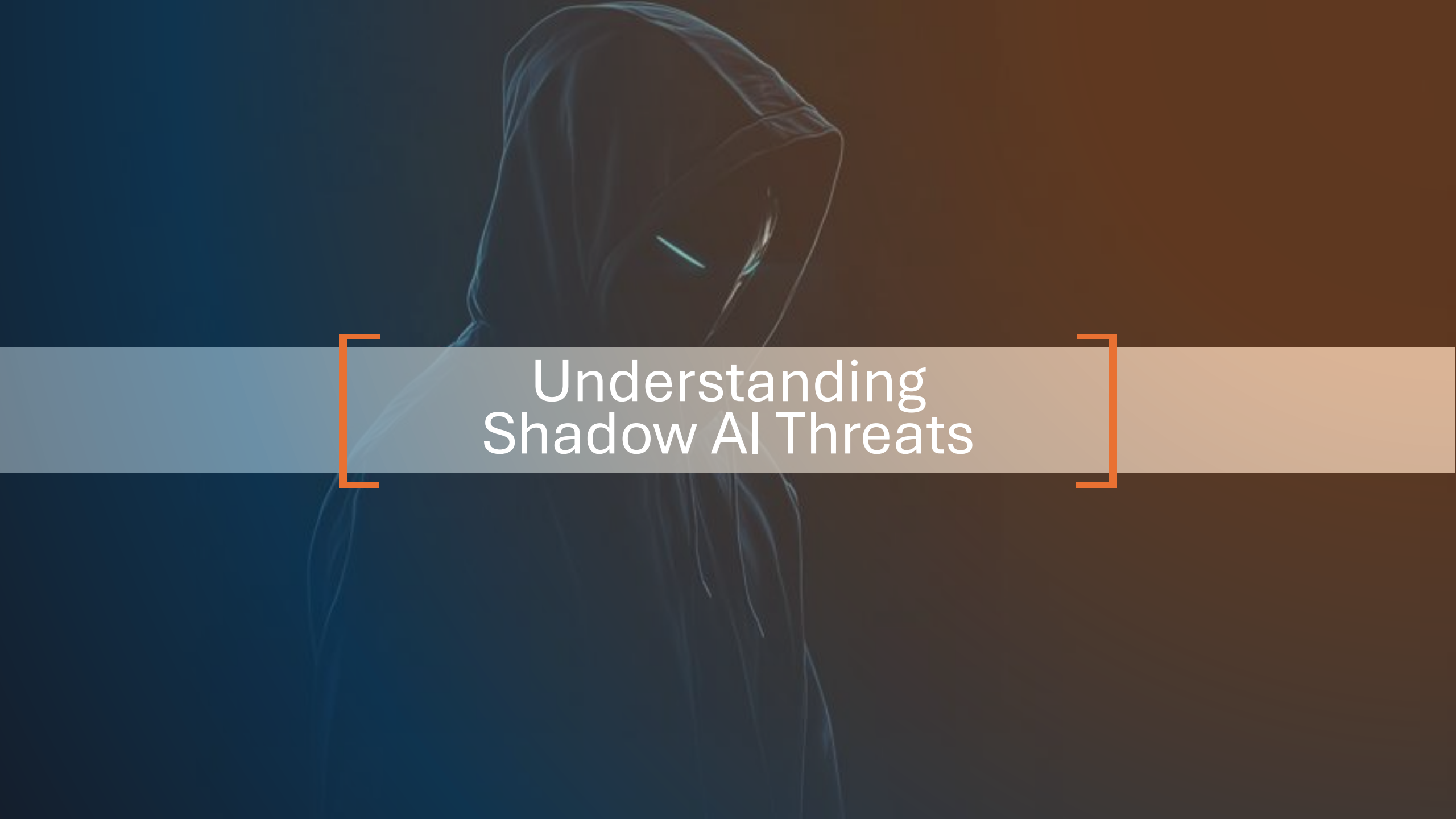
## Combating Shadow AI with Microsoft Security Solutions and Zero Trust Methodologies

MARCH 5TH, 2025

AccountabilIT
Security Amplified, Cloud Simplified

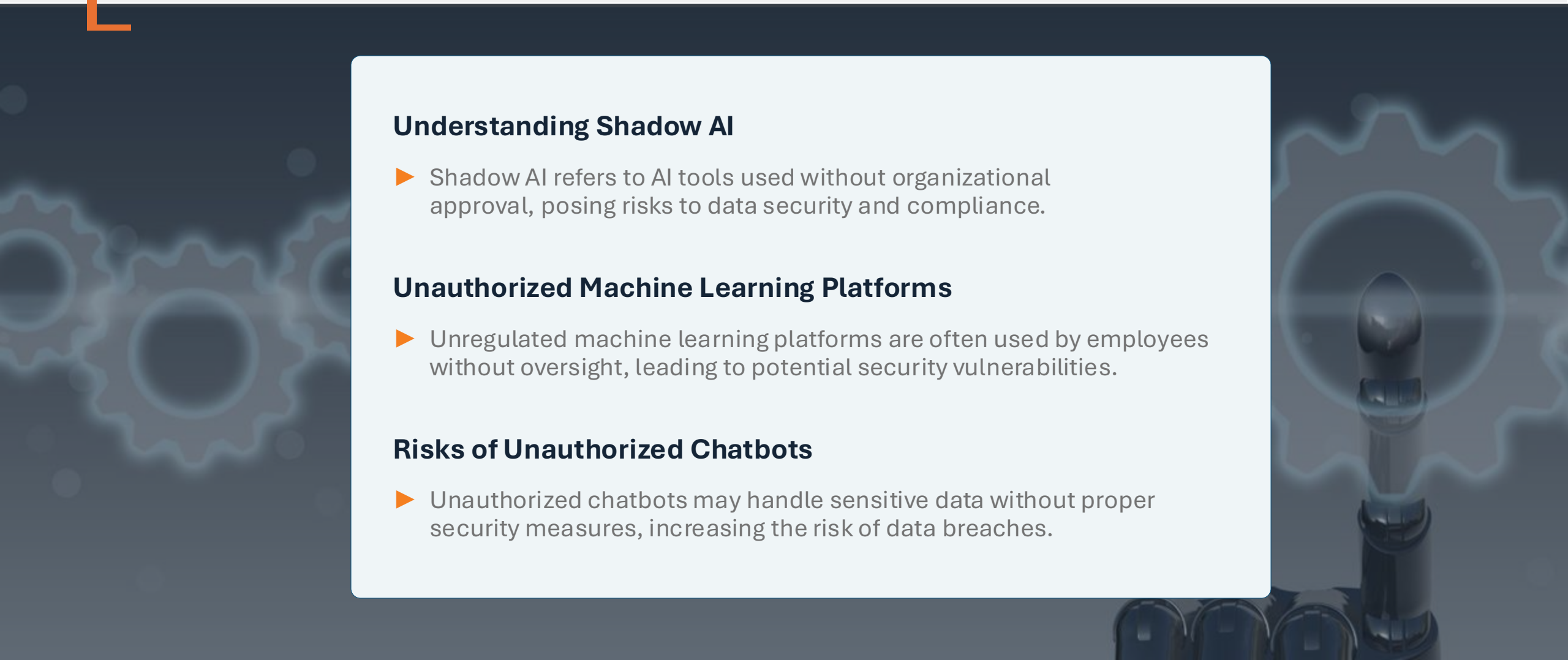
# TOPICS TO BE COVERED

- Understanding Shadow AI Threats
- Introduction to Zero Trust Methodologies
- Leveraging Microsoft Purview for Threat Detection
- Utilizing Intune for Endpoint Protection
- Integrating Microsoft Purview & Intune for Comprehensive Security



# Understanding Shadow AI Threats

# Definition and Examples of Shadow AI



## Understanding Shadow AI

- Shadow AI refers to AI tools used without organizational approval, posing risks to data security and compliance.

## Unauthorized Machine Learning Platforms

- Unregulated machine learning platforms are often used by employees without oversight, leading to potential security vulnerabilities.

## Risks of Unauthorized Chatbots

- Unauthorized chatbots may handle sensitive data without proper security measures, increasing the risk of data breaches.

AccountabilIT
Security Amplified, Cloud Simplified

# Risks Associated with Shadow AI

## Data Breaches

Shadow AI can lead to significant data breaches, exposing sensitive information and compromising organizational security.

## Compliance Violations

Organizations using shadow AI risk violating compliance regulations, which can result in hefty fines and legal challenges.

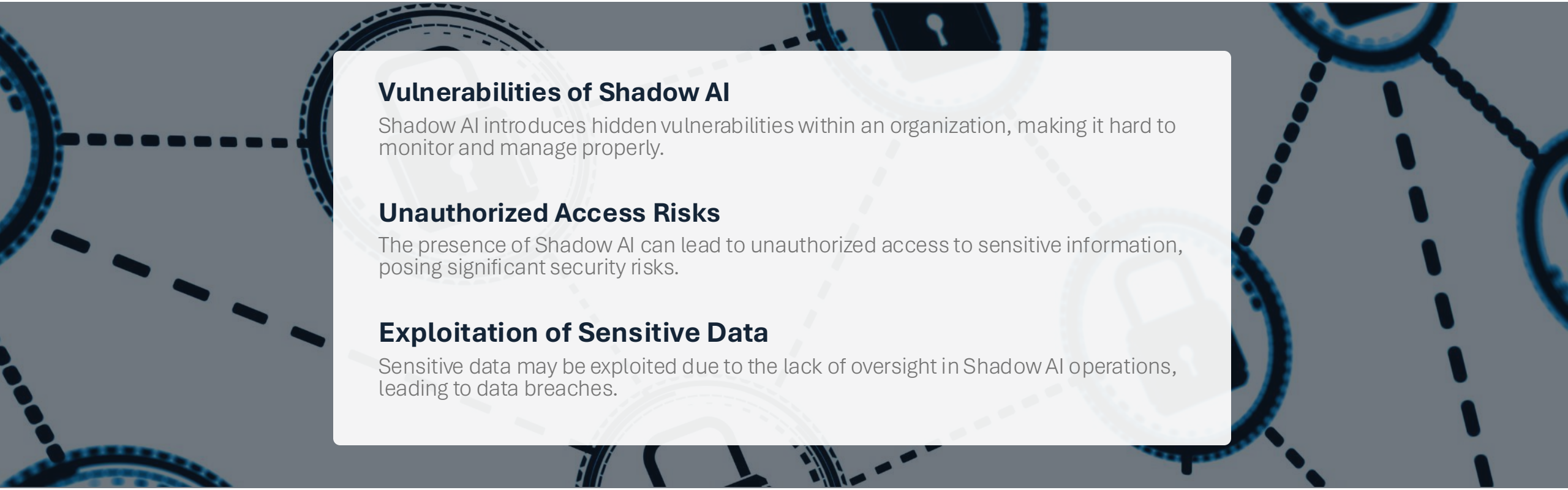
## Malicious AI Usage

The potential for malicious AI usage can pose threats to organizations, leading to misuse of AI technologies for harmful purposes.

## Reputational Damage

Reputational damage can occur if organizations fail to manage shadow AI risks, impacting public trust and stakeholder confidence.

# Impact on Organizational Security



### Vulnerabilities of Shadow AI

Shadow AI introduces hidden vulnerabilities within an organization, making it hard to monitor and manage properly.

### Unauthorized Access Risks

The presence of Shadow AI can lead to unauthorized access to sensitive information, posing significant security risks.

### Exploitation of Sensitive Data

Sensitive data may be exploited due to the lack of oversight in Shadow AI operations, leading to data breaches.

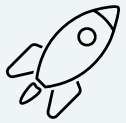
# A Perfect Storm

### Significant Investment Drives Quick Feature Development

Companies, both large and small, are racing to release and enhance their products with AI functionalities.

### Regulatory Agencies are Starting to Respond

Government bodies are beginning to update compliance and legal frameworks to address the rapid increase in AI usage.



### Rapid Growth of New AI Applications

Every day, new AI-driven applications are launched in the market, each carrying its own set of risks.

### Users and Threat Actors are Eager and Ambitious

Individuals at various levels are investigating new AI-enabled opportunities, creating a conducive environment for Threat Actors to breach systems.

INTRODUCTION TO

# Zero Trust Methodologies

# Principles of Zero Trust Security

## Never Trust, Always Verify

The Zero Trust model emphasizes verifying all users and devices before granting access to resources, reducing potential threats.

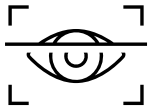
## Least Privilege Access

Implementing least privilege access ensures users have only the permissions necessary for their roles, minimizing risk exposure.

## Continuous Monitoring

Continuous monitoring is crucial in the Zero Trust model to detect and respond to threats in real-time.

# Key Components of Zero Trust Architecture

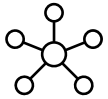


## Identity Verification

Identity verification ensures that only authorized users can access sensitive information and systems, enhancing overall security.

## Device Health Checks

Regular device health checks ensure that only compliant and secure devices can connect to the network, minimizing vulnerabilities.



## Network Segmentation

Network segmentation divides the network into smaller segments to limit the spread of potential breaches and enhance security.

## Data Encryption

Data encryption protects sensitive information during transmission and storage, ensuring privacy and integrity against unauthorized access.

## Data Classification

Data classification enables intelligent decision making based on its classification level.

AccountabilIT
Security Amplified, Cloud Simplified

# Benefits of Implementing Zero Trust

## Enhanced Security

Zero Trust enhances security by minimizing attack surfaces and protecting sensitive data from potential breaches.

## Regulatory Compliance

Implementing Zero Trust helps organizations meet compliance requirements, safeguarding sensitive data and enhancing overall trust with stakeholders.

## Improved Data Protection

With Zero Trust, organizations can implement stricter access controls, ensuring that only authorized users have access to sensitive information.

## Culture of Security

Individuals at various levels are investigating new AI-enabled opportunities, creating a conducive environment for Threat Actors to breach systems.

# Calculate Risk

**ALE = ARO * SLE**

**SLE = AV * EF**

**ALE: Annualized Loss Expectancy**
**ARO: Anualized Rate of Occurrence**
**SLE: Single Loss Expectancy**
**AV: Asset Value**
**EF: Exposure Factor**

# Leveraging M365 Purview

## FOR THREAT DETECTION

AccountabilIT
Customer Driven IT Services

# Overview of M365 Purview Capabilities

## Data Classification

M365 Purview offers robust data classification tools that help organizations categorize and manage sensitive information efficiently.

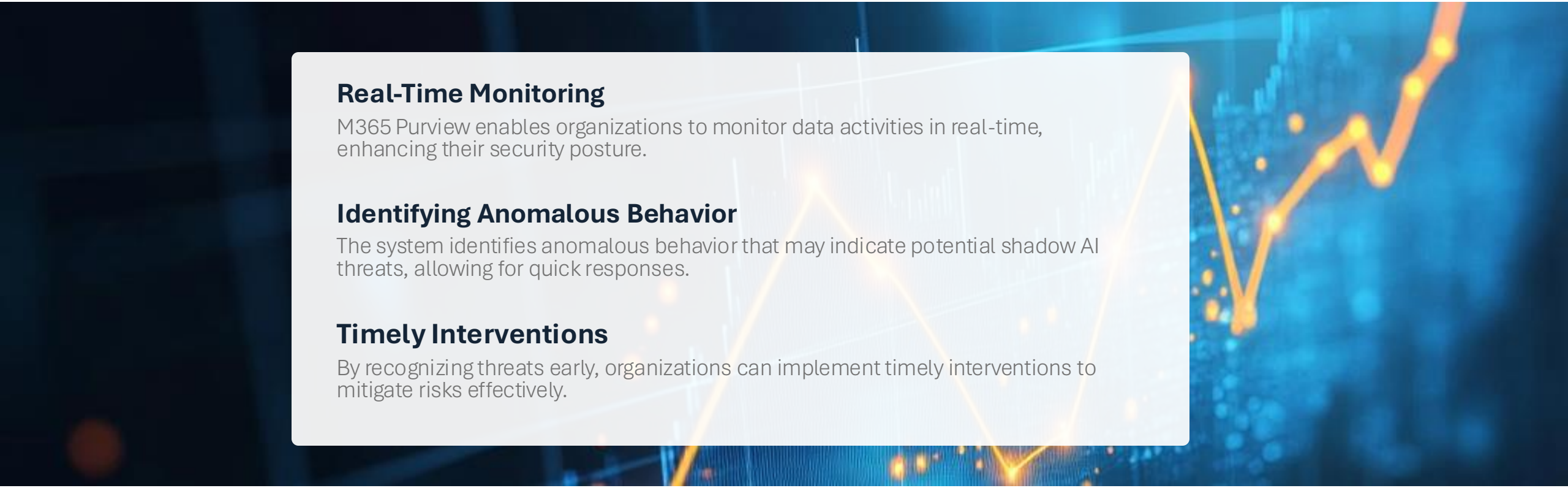
## Labeling Mechanism

The labeling feature allows users to apply security and compliance labels to data, enhancing data protection and ensuring regulatory compliance.

## Activity Monitoring

M365 Purview enables organizations to monitor data activity and access, ensuring that data governance policies are followed effectively.

# Monitoring and Analyzing Data Activities



### Real-Time Monitoring

M365 Purview enables organizations to monitor data activities in real-time, enhancing their security posture.

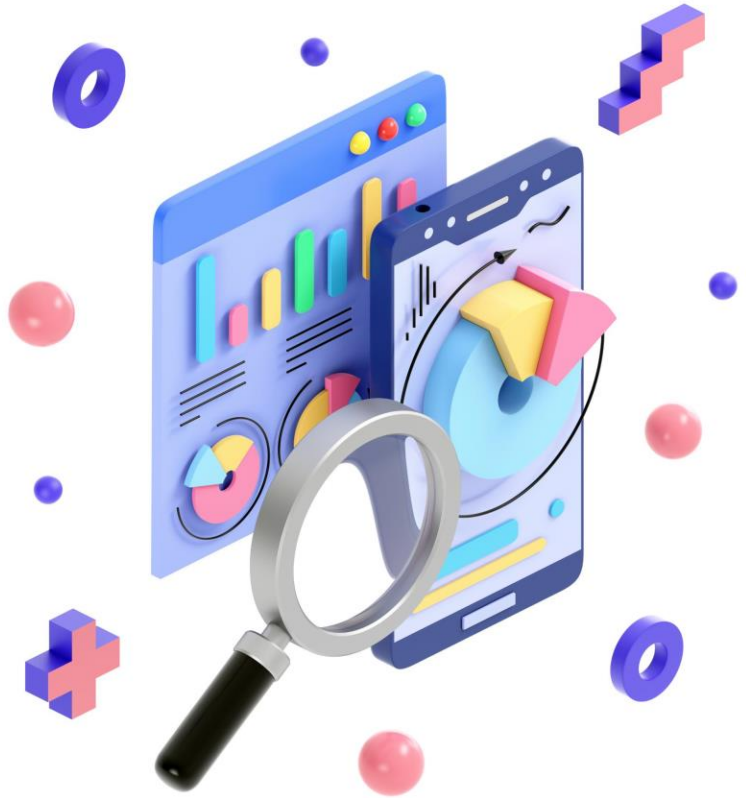
### Identifying Anomalous Behavior

The system identifies anomalous behavior that may indicate potential shadow AI threats, allowing for quick responses.

### Timely Interventions

By recognizing threats early, organizations can implement timely interventions to mitigate risks effectively.

# Identifying and Mitigating Shadow AI Threats



## Advanced Analytics Tools

Microsoft Purview utilizes advanced analytics tools to detect and identify potential shadow AI threats within organizations.

## Risk Mitigation Strategies

Organizations can implement effective risk mitigation strategies with Microsoft Purview to manage shadow AI threats proactively.

## Security Measures Implementation

Microsoft Purview facilitates the implementation of appropriate security measures to protect against shadow AI risks and vulnerabilities.

## Data Classification

Microsoft Purview facilitates the data classification and discovery process, enabling improved decision making over time.

# Reduce Risk with Microsoft Intune

Intune, a powerful ally

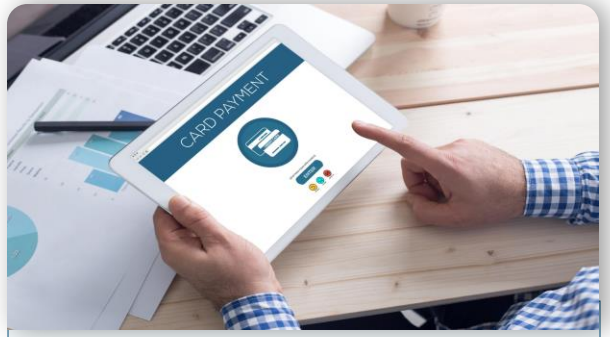
# Introduction to Intune Features

## Mobile Device Management

Intune enables organizations to manage mobile devices securely, ensuring compliance with corporate policies.

## Application Management

With Intune, IT administrators can manage applications on devices, controlling access and deployment effectively.



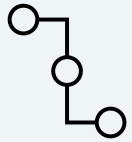

## Policy Enforcement

Intune's policy enforcement features help maintain security across all endpoints, ensuring devices meet compliance standards.

# Deploying Zero Trust Policies via Intune

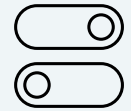
## Zero Trust Security Framework

Zero Trust is a security model that requires strict identity verification for every person and device trying to access resources.



## Endpoint Management with Intune

Intune allows organizations to manage devices and apps, ensuring compliance with security policies across all endpoints.



## Access Control Policies

Implementing access control policies ensures that only authorized users and devices can access sensitive data and applications.

AccountabilIT
Security Amplified, Cloud Simplified

# Ensuring Compliance and Enforcement

## Compliance with Security Policies

Intune aids organizations in adhering to security policies, ensuring that all devices meet required standards.

## Automated Compliance Checks

Automated checks provided by Intune help streamline the compliance process, reducing manual effort and errors.

## Minimizing Security Breaches

By enforcing compliance, Intune minimizes the risk of security breaches, protecting organizational data and resources.

# Integrating M365 Purview and Intune

## FOR COMPREHENSIVE SECURITY

# Combining Data Governance and Endpoint Management

### Synergistic Security Approach

Integrating Microsoft Purview and Intune creates a unified security strategy for organizations.

### Effective Data Management

Organizations can manage data efficiently while ensuring compliance and security across their endpoints.

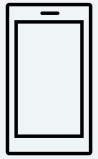
### Endpoint Security

Securing endpoints is crucial for protecting sensitive data and maintaining organizational integrity.

# Case Studies of Integrated Security Approaches

### Integration of Microsoft Purview

M365 Purview provides powerful tools for data protection and compliance, enhancing security within organizations.



### Role of Intune

Intune plays a critical role in managing mobile devices securely, ensuring that organizational data remains protected.

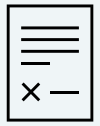
### Mitigating Shadow AI Threats

Integrating these solutions helps organizations effectively mitigate potential threats posed by shadow AI technologies.

# Best Practices for Seamless Integration

### Regular Audits

Conducting regular audits ensures compliance and identifies areas for improvement in the integration process.



### Alignment of Security Policies

Aligning security policies across platforms ensures a cohesive security posture and minimizes risks during integration.

### Continuous Training

Providing continuous training for staff helps maintain up-to-date knowledge on Microsoft Purview and Intune functionalities and best practices.

### Alignment of Compliance Policies

Aligning compliance policies empowers security teams to be proactive in defense of critical assets within the datasphere.

# What's Next?

## Apply for a *Low-Cost* Data Security Assessment

As a valued attendee of our Microsoft Purview webinar, you have the exclusive opportunity to apply for a comprehensive data security assessment. This assessment will help you:

- **Identify Vulnerabilities:** Uncover potential weaknesses in your data security infrastructure.
- **Enhance Protection:** Receive tailored recommendations to strengthen your data protection measures.
- **Ensure Compliance:** Align your data security practices with industry standards and regulations.
- **Optimize Resources:** Make informed decisions to efficiently allocate your security resources.

AccountabilIT
Security Amplified, Cloud Simplified

# CONCLUSION

## Zero Trust Methodologies

Implementing Zero Trust methodologies is crucial for security, ensuring that all access requests are verified.

## Microsoft Purview Integration

Leveraging M365 Purview helps organizations manage data security and compliance, enhancing overall protection.

## Intune for Device Management

Intune plays a vital role in managing devices securely and ensuring organizational data remains protected.