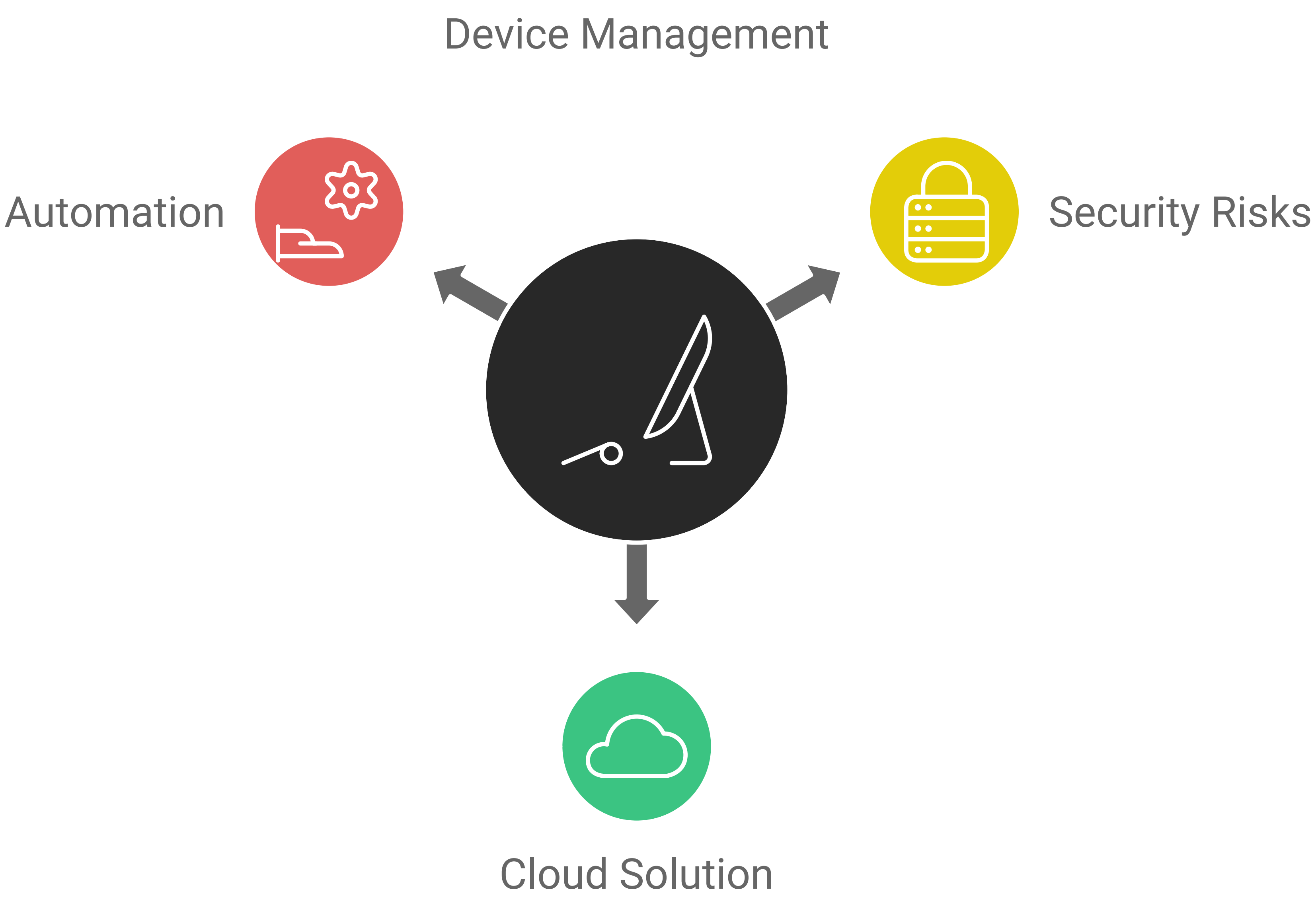
Aakash Rahsi

Cloud Security & Automation Case Study: Microsoft Intune Deployment for Enterprise

1. Introduction

Background

Our client, a prominent enterprise in the financial services industry, was managing a distributed workforce that spanned multiple regions. With the rise in remote work, device management became increasingly complex. Employees used a mix of company-owned and personal devices to access sensitive data, including financial records and customer information. This fragmented setup exposed the company to significant security risks, such as unauthorized access, data leaks, and compliance violations. Existing manual processes for security updates and device management were proving inefficient and error-prone.
In response, the client sought a scalable, cloud-based solution to centralize device management, enhance security controls, and automate compliance policies across the organization. Microsoft Intune was selected as the platform of choice for its seamless integration with existing systems like Azure Active Directory and Microsoft 365.



Project Overview

The primary objectives of this project were:

- **Security Enhancements:** Implement stricter endpoint security and compliance checks across the organization, ensuring that only compliant and secure devices could access sensitive data.
- **Automation:** Streamline the deployment of applications, security patches, and compliance policies to reduce the need for manual intervention, thus minimizing human error.
- **Unified Device Management:** Centralize the management of all devices (Windows, macOS, iOS, Android) through a single platform that integrates with Azure Active Directory (Azure AD) for better control and visibility.

The deployment aimed to cover 5,000+ devices and manage diverse operating systems with comprehensive security, compliance, and automation.

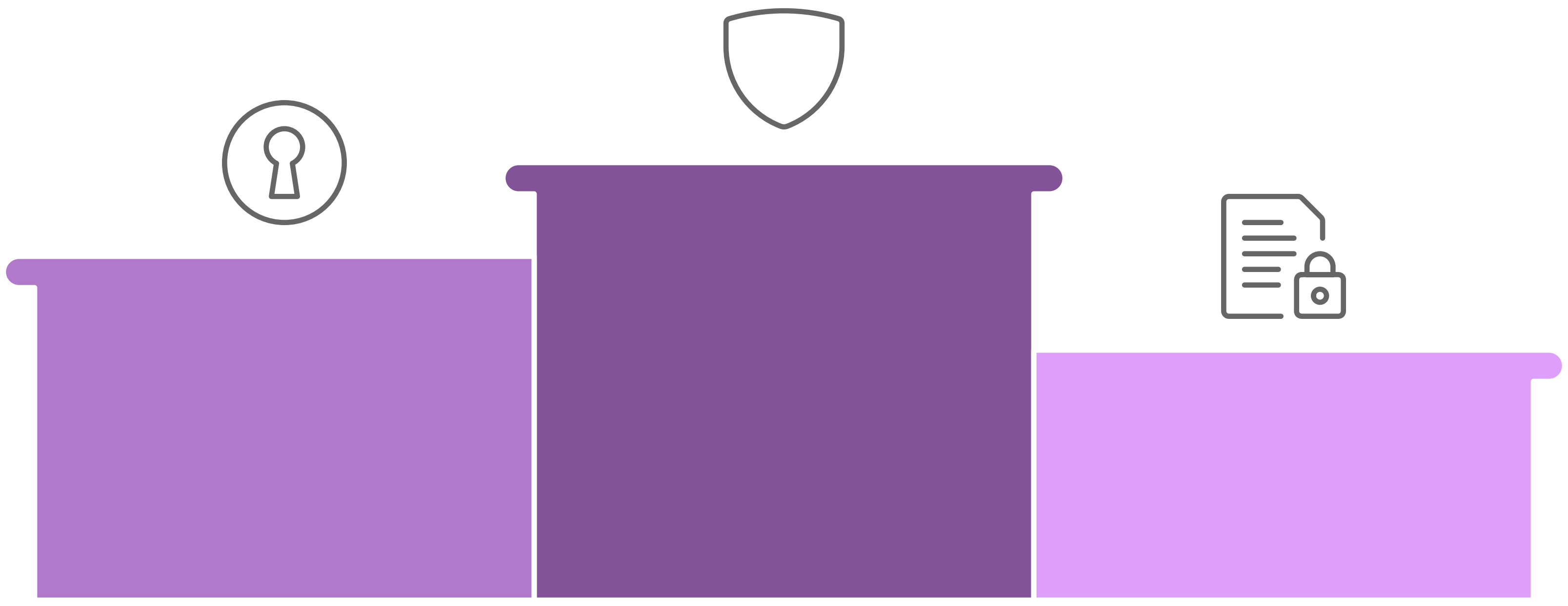
2. Project Goals and Objectives

Security Goals

The project’s primary security objectives were focused on ensuring the confidentiality, integrity, and availability of data by deploying policies that enforced strict compliance rules and conditional access policies. Key goals included:

1. **Strengthen endpoint security** through the deployment of security baselines.
2. **Mitigate risks of unauthorized access** by implementing Azure AD Conditional Access policies that would only grant access to compliant, managed devices.
3. **Encrypt sensitive data** on all endpoints using BitLocker for Windows and FileVault for macOS.

Key Security Objectives in Microsoft Intune Deployment



Automation Objectives

Automation was critical in ensuring that all devices received regular updates without requiring manual intervention. The following automation goals were identified:

1. **Automate patch deployment** to ensure all devices remain up-to-date with the latest security patches and updates.
2. **Automate device enrollment** and provisioning, minimizing the need for manual configuration and reducing the time needed to bring devices into the corporate environment.
3. **Automate compliance reporting** to track which devices met security standards and alert the IT team in case of compliance violations.

Management Aims

With a large number of devices in the organization, centralizing device management was essential for efficient operations. The management goals were:

1. **Create a unified endpoint management platform** to manage Windows, iOS, macOS, and Android devices under a single system.
2. **Enable remote device wiping** and lock functionality to protect sensitive corporate data if devices were lost or stolen.
3. **Establish user and device-based policies** that could be dynamically assigned based on role and device type using Azure AD groups.

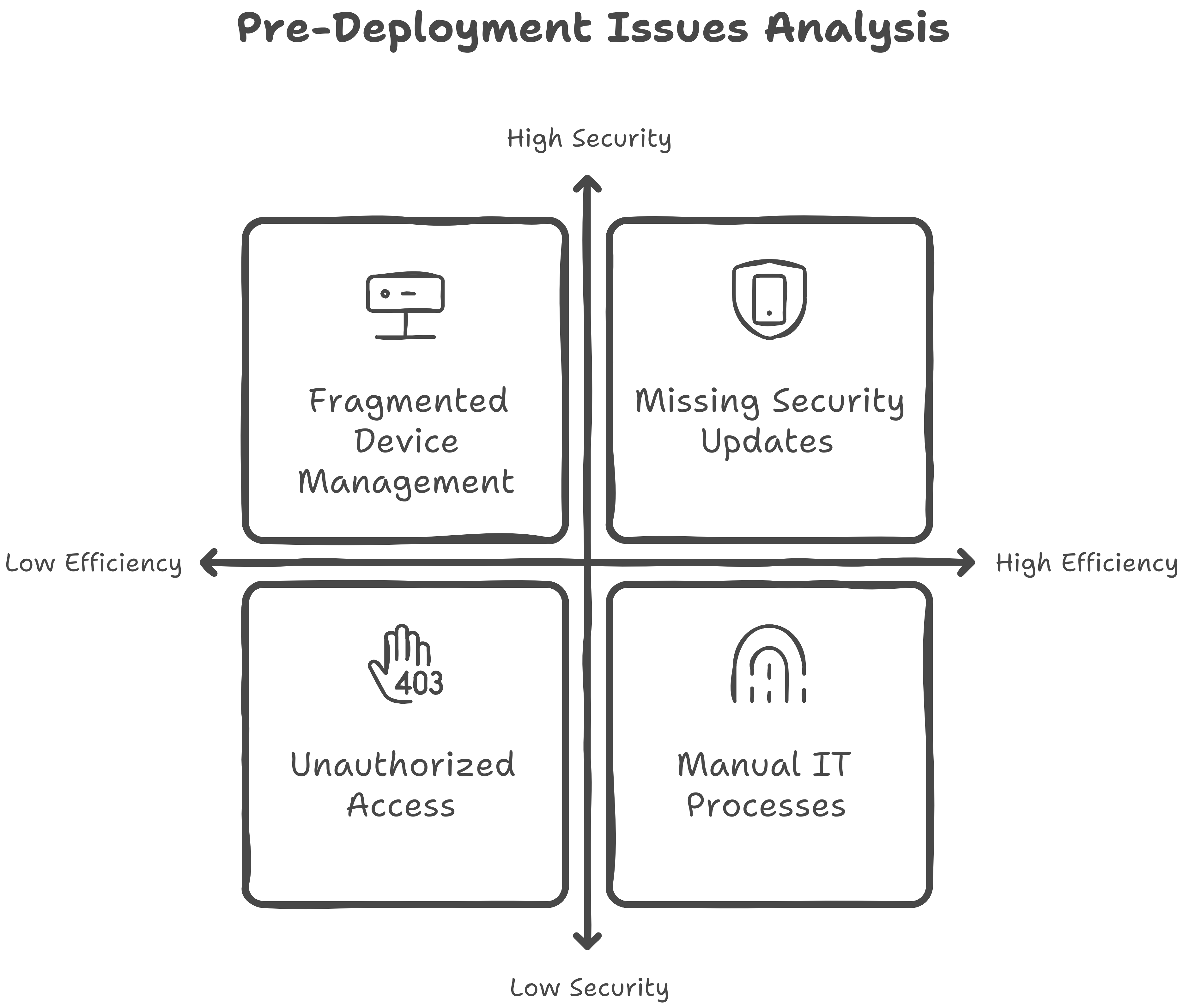
3. Pre-Deployment Analysis

Assessment of Existing Infrastructure

Before deploying Microsoft Intune, we conducted a detailed analysis of the existing infrastructure, which included:

1. **Device Inventory:** The client was using a mix of on-premises tools like SCCM (System Center Configuration Manager) to manage Windows devices, while other devices (macOS, iOS, Android) were unmanaged. This created a fragmented view of the devices accessing corporate data.
2. **Security Gaps:** Devices were missing security updates, and there was no centralized mechanism for enforcing security policies such as encryption or multi-factor authentication (MFA).

3. **User Access Control:** Most devices lacked multi-factor authentication, and unauthorized devices were able to access the company network, posing security threats.
4. **IT Challenges:** The IT team was managing device configuration and security manually, which was both time-consuming and prone to errors.



Requirement Analysis

Based on the assessment, the following requirements were identified:

1. **Integration with Azure Active Directory** to enforce Conditional Access policies and MFA.
2. **Unified management across all operating systems** to ensure consistent security policies across the organization.
3. **Self-service device enrollment** to allow users to securely enroll their own devices without burdening the IT team.
4. **Automation of compliance checks** to alert administrators when a device fell out of compliance.

4. Solution Design

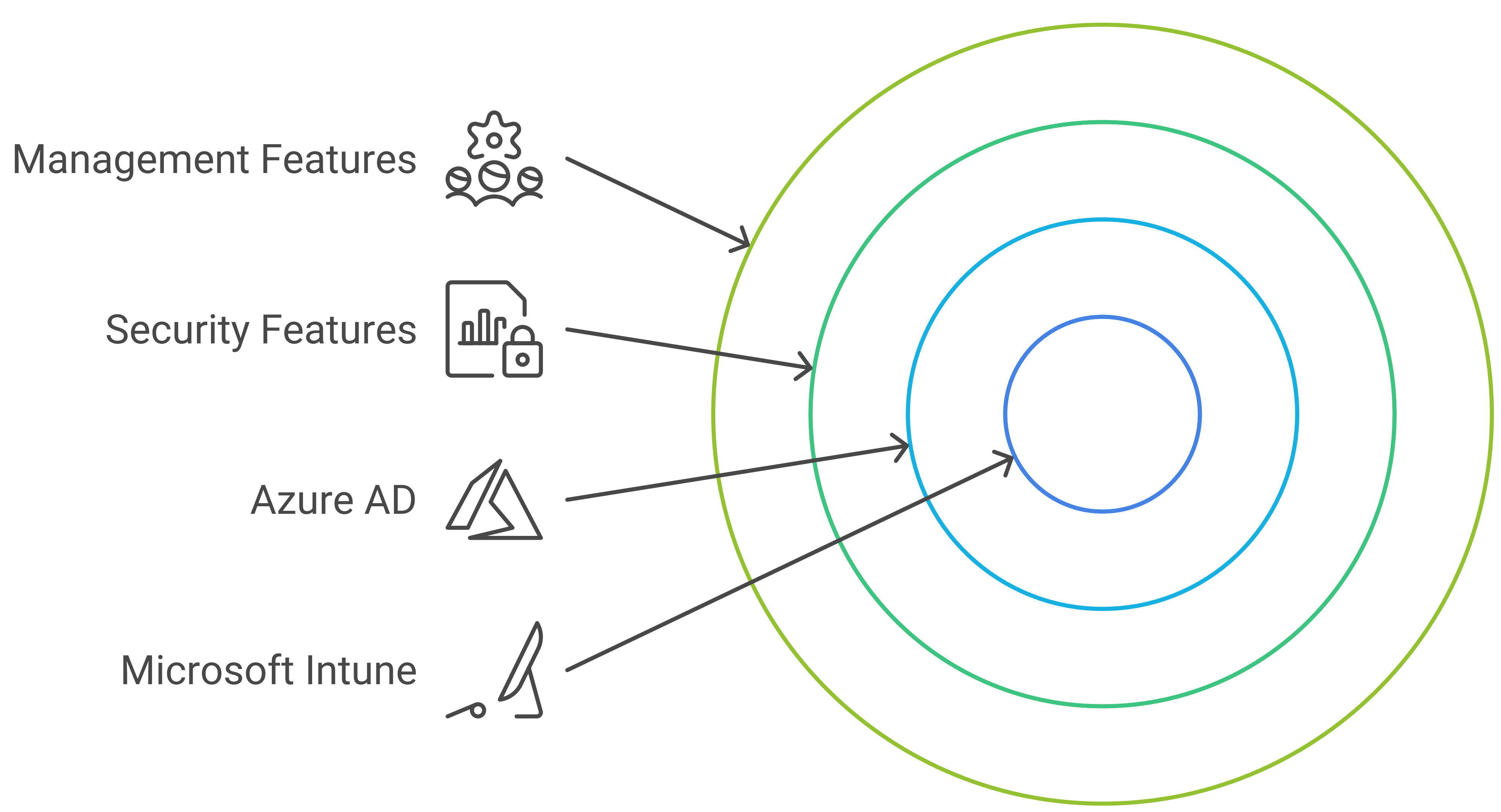
Architecture

The proposed architecture integrated Microsoft Intune as a part of the Microsoft Endpoint Manager suite. The core components of the architecture included:

- **Intune for MDM and MAM:** Microsoft Intune would handle both Mobile Device Management (MDM) and Mobile Application Management (MAM), ensuring security and management across both corporate and BYOD devices.
- **Azure Active Directory (Azure AD):** Azure AD Conditional Access was used to ensure only compliant devices could access corporate data.
- **Azure Information Protection (AIP):** For data protection and encryption, ensuring sensitive data could be automatically classified and protected.

Figure 1: Architecture of Microsoft Intune and its integration with Azure AD.

Microsoft Intune Architecture



Security Configuration

The security configuration focused on deploying security baselines across all devices. The primary security features included:

- **Device Compliance Policies:** Devices had to meet certain criteria (e.g., encrypted storage, password protection, and antivirus enabled) to access corporate data.
- **Conditional Access:** Using Azure AD, we created policies to block non-compliant devices from accessing corporate applications and sensitive data.
- **Data Protection Policies:** Mobile Application Management (MAM) policies restricted the sharing of corporate data with unmanaged apps.

5. Implementation Strategy

Phase 1: Planning and Pilot Testing

The project began with a detailed planning phase, where a small pilot group of users was selected to test the Intune deployment.

- **User Group:** The pilot included employees from various departments, using different devices (Windows, macOS, Android, iOS) to ensure that all configurations worked seamlessly across the board.
- **Testing Scope:** During this phase, we tested compliance policies, device enrollment, security baselines, and Conditional Access.
- **Feedback:** Based on feedback, we made necessary adjustments, particularly in the areas of user training and policy fine-tuning.

Phase 2: Full Deployment

With the pilot's success, the deployment was scaled across the organization in phases, department by department. We ensured minimal disruption to daily operations by rolling out during non-peak hours.

- **Automated Device Enrollment:** Users enrolled their devices via a secure, self-service portal, reducing the burden on IT staff.
- **Security Baselines:** Policies were applied automatically to ensure compliance and security of each device.
- **Monitoring:** Intune's built-in reporting tools provided real-time monitoring of compliance status and security incidents.

Phase 3: Post-Deployment Optimization

Post-deployment, we continued optimizing the environment by adding automation for patch management and leveraging Intune's analytics to refine policies.

- **Patch Management:** Devices were automatically patched to ensure they were always up to date.
- **Regular Compliance Audits:** Automated reports were used to audit device compliance on a regular basis, with any non-compliant devices flagged for remediation.

6. Security Enhancements

Policy Implementation

Several key security policies were implemented to secure the enterprise:

- **Password and PIN Requirements:** All devices were required to have complex passwords or PINs, reducing the risk of unauthorized access.
- **Encryption:** BitLocker was enforced on all Windows devices, and FileVault was required for macOS devices, ensuring data encryption at rest.
- **Antivirus and Firewall:** Compliance policies required that all devices have active antivirus software and firewalls enabled before they could access corporate resources.

Passwords & PINs

Encryption

Antivirus & Firewall

Access Controls

We implemented Conditional Access policies based on device compliance. These policies ensured that:

- Only compliant and managed devices could access corporate applications like Microsoft Teams, SharePoint, and Outlook.
- Multi-factor authentication (MFA) was required for users accessing the network from outside the corporate perimeter.

7. Automation Features

Automated Deployments

- **Application Deployment:** Corporate apps were pushed to devices based on user role and device type. This included Office 365, internal apps, and security tools like antivirus software.
- **Security Patch Automation:** Devices received automatic security patches and updates, ensuring they were always up to date with the latest security fixes.

Dynamic Management

Dynamic Azure AD groups were created to automatically assign policies and applications based on user attributes. For instance:

- **Device Type Management:** Policies were dynamically assigned based on the type of device (e.g., mobile vs. desktop) and its compliance status.
- **Role-Based Management:** Users in specific roles (e.g., finance or HR) automatically received applications and policies tailored to their specific needs.

8. Device Management

Device Enrollment

- **Company-Owned Devices:** For company-owned devices, IT enrolled them during the provisioning process, ensuring that they were pre-configured with the necessary apps and policies.

- **BYOD Devices:** Users were able to enroll their own devices securely via a self-service portal. Devices were automatically configured with the required security settings and policies.

Monitoring and Reporting

- **Compliance Monitoring:** Intune's real-time compliance reporting allowed the IT team to monitor the status of every device, ensuring that only compliant devices were accessing corporate resources.
- **Security Alerts:** Automated alerts were triggered whenever a device fell out of compliance (e.g., missing a critical update), allowing IT to take immediate action.

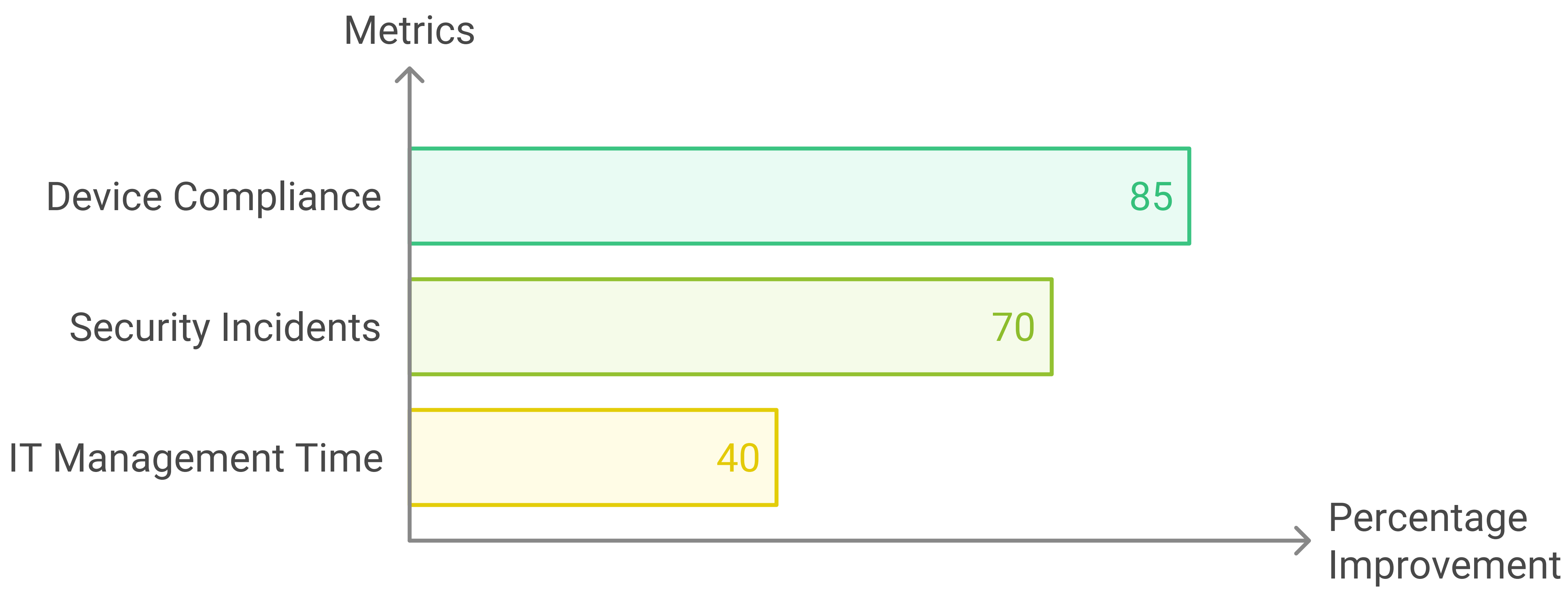
9. Results and Evaluation

Before and After Analysis

- **Before:** The organization struggled with inconsistent device management, poor visibility into device compliance, and frequent security incidents due to unmanaged devices.
- **After:** Post-deployment, device compliance improved by over 85%, and the number of security incidents related to unmanaged devices dropped by 70%. This led to an overall increase in data security and a more streamlined IT operation.

Key Performance Indicators (KPIs)

- **85% increase in device compliance** within the first three months.
- **70% reduction in security incidents** involving unmanaged devices.
- **40% decrease in the time IT spent managing devices**, thanks to automation.



Impact of Microsoft Intune Deployment

10. Lessons Learned

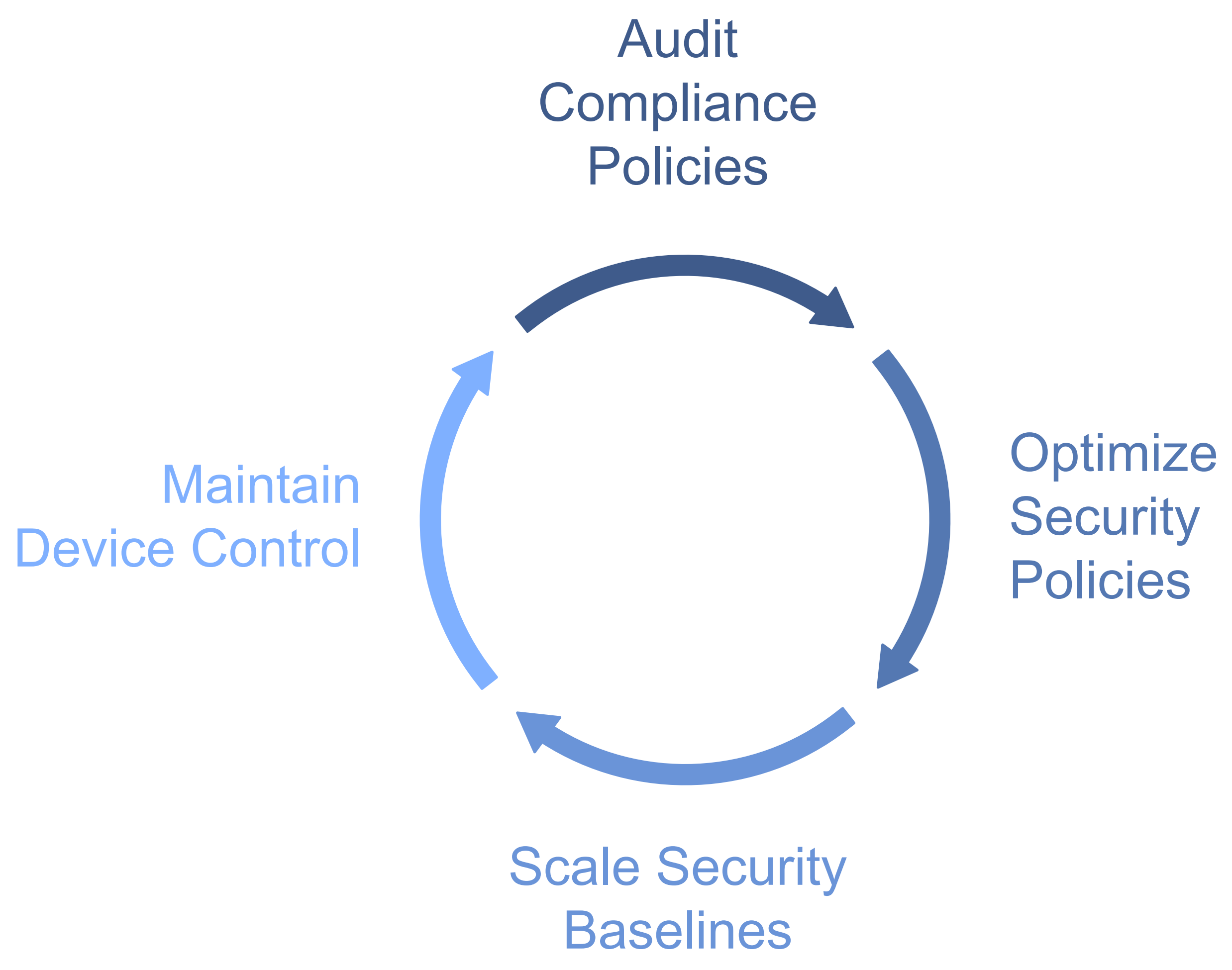
Insights

- **User Training is Crucial:** End-user training proved vital in ensuring a smooth enrollment process. Providing comprehensive training resources allowed users to enroll and manage their devices effectively.
- **Automation Saves Time:** Automating security updates and compliance checks reduced the time IT spent on manual tasks and significantly improved security across the board.

Recommendations for Future Projects

- **Continuous Policy Optimization:** Regularly audit and optimize compliance and security policies to stay ahead of emerging threats.
- **Scale Security Baselines:** As the number of devices grows, continue to adjust security baselines to maintain control over compliance.

Continuous Security Improvement Cycle



11. Appendices

Technical Specifications

- **Device Compliance Policies:**
  - Password complexity: Minimum of 8 characters with uppercase, lowercase, and numeric characters.
  - Encryption: BitLocker and FileVault enforced on Windows and macOS, respectively.
  - Antivirus: Windows Defender for Windows, with third-party solutions for macOS.
- **Conditional Access Policies:**
  - MFA required for all external network access.
  - Access restricted to compliant devices.
- **Dynamic Group Configuration:** Groups were set up in Azure AD to automatically apply specific policies based on user attributes such as department and device type.

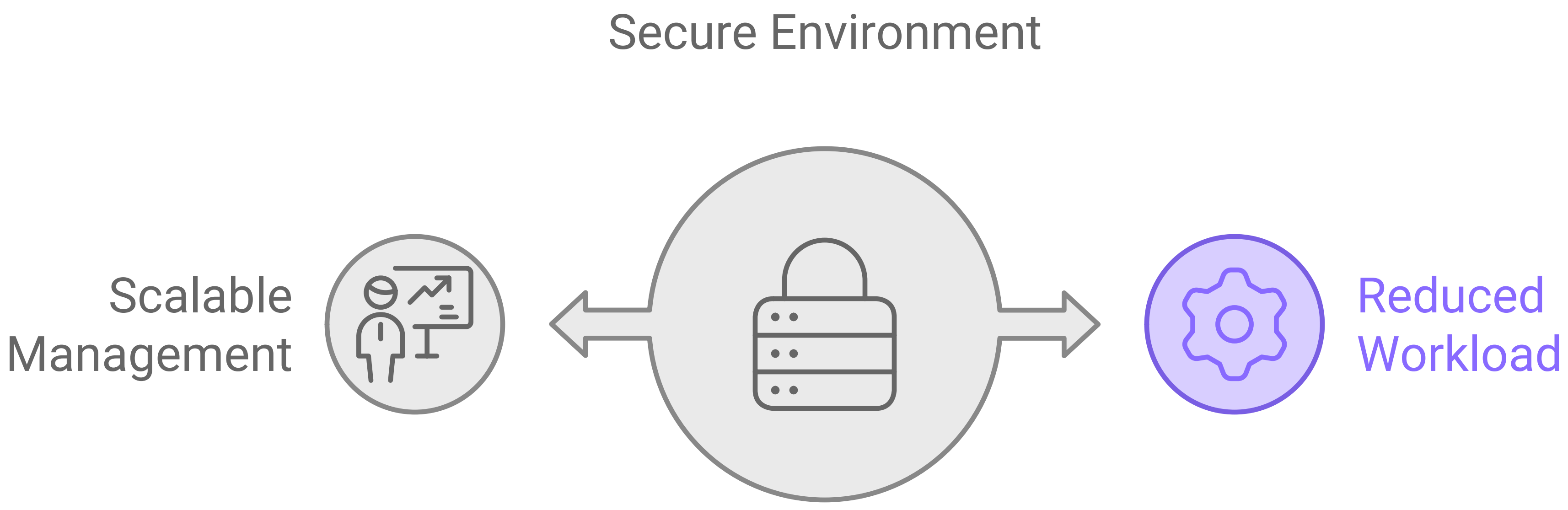
Screenshots and Diagrams

- **Diagram 1:** Intune integration with Azure AD for compliance and Conditional Access.
- **Screenshot 1:** Example of Intune compliance report dashboard.
- **Screenshot 2:** Conditional Access policy configuration.

12. Conclusion

Summary of Achievements

The deployment of Microsoft Intune resulted in a fully managed and secure environment, significantly reducing the risk of data breaches and unauthorized access. The IT team now benefits from a streamlined management process, reducing manual workload and improving operational efficiency. This project has set a solid foundation for scaling device management and security as the organization grows.



Future Considerations

- **Expand Automation:** Explore further automation opportunities in areas like user onboarding and device retirement.
- **Strengthen Security Baselines:** Continuously update security policies as new threats emerge and devices evolve.

13. References

- Microsoft Intune Documentation: https://docs.microsoft.com/en-us/mem/intune/
- Azure Active Directory Conditional Access: https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/
- Best Practices for Endpoint Security: https://www.microsoft.com/security/blog/

Aakash Rahsi