MS SENTINEL ACCELERATOR & MANAGED SERVICE

Agriculture

100+ years in market

15,000 tons output/ month
Export to 70+ countries

Customer Overview

A fully fledged supplier of nutritional products which operates globally, with a strong presence in Asia. It leverages strategic investments in local resources and livestock management, which helps empower independent farmers and improve livestock productivity.

Customer pain points and needs

- Challenges in maintaining consistent security configurations across Azure and on-premise systems, limiting their ability to detect and respond to threats in real time.
- The company sought enhanced threat visibility, streamlined incident response, and automated security operations to reduce manual effort and effectively manage risks across their complex infrastructure.

Approach

- Implemented MS Sentinel
- Sentinel-as-Code with Azure DevOps
- Provided ongoing administration services

Value and impact

Automation with **Sentinel-as-Code** and **Azure DevOps**

Time to **DEPLOY** and **CONFIGURE** security infrastructure decreased **80%**

Real-time visibility across **multi-cloud environment**

Time to **DETECT** threats and **RESPONSE** decreased **50%**

Lesson learned

Implementing Sentinel-as-Code proved to be a highly effective strategy, allowing for rapid, consistent deployment.
>> This approach can be replicated across other industries where compliance and security are paramount.

UPLIFTING MULTI-CLOUD SECURITY POSTURE

Analytics Technology

220% Churn Reduction

350% ROI rate

Customer Overview

A leader in conversation intelligence technology, providing AI-driven analytics that empower organizations to gain valuable insights from customer interactions across voice, chat, and email channels.

Customer pain points and needs

- Complexity in data protection and compliance due to differing encryption and access requirements across platforms Azure and AWS.
- Gathering audit-ready evidence is resource-intensive, requiring ongoing monitoring and reporting to meet compliance across both cloud environments.

Approach

- Assess security gaps for both Azure and AWS using Microsoft Defender for Cloud.
- Use Microsoft Sentinel for real-time insights and threat detection.
- Configure Azure AD as the identity provider for AWS SSO, and used Azure Privileged Identity Management (PIM).
- Integrate native security features (Azure Firewall, Network Watcher, Key Vault, Bastion, etc.) to establish a fully monitored infrastructure.

Value and impact

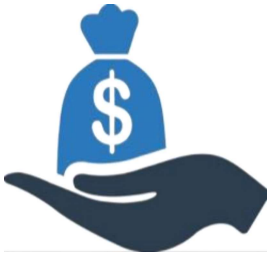
Unsecured resources

– 250%

Secure multi-cloud environments

+ 270%

Security Score



X4 revenue in the next quarter

Lesson learned

FPT developed a scalable practice for strengthening multi-cloud security posture using Microsoft Defender for Cloud, creating a solution that can be readily applied to future customers.

ENTRA ID – CONDITIONAL ACCESS POLICIES-AS-CODE (CAP-AS-CODE)

Power Energy | $30.0B market cap | $30,9B revenue 2023

Customer Overview

A leading company in the Energy sector, with more than 125 years on the market with various business segments across Europe, America, UK and especially German

Customer pain points and needs

- Challenges in securing access to their critical cloud resources across a distributed workforce.
- Lack of automation (managing CAP) results in slower deployment times and increased operational overhead.

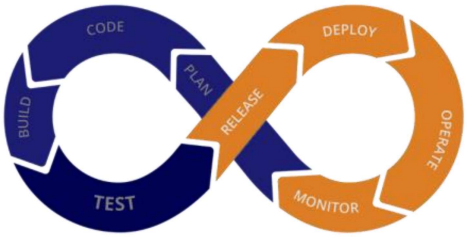
Approach

- **Design and Implement CAP-as-Code**: use Azure Active Directory and Azure DevOps, allowing for the automated deployment and management of CAPs.
- **Customization for Industry Needs:** The CAPs were tailored to meet the specific security and compliance requirements of the Energy sector, including restrictions based on location, device compliance, and risk levels

Value and impact

Enhanced Security Compliance

Operational Excellence



Lesson learned

Implementing Conditional Access Policies as Code provided significant benefits in terms of security and operational efficiency. This approach can be replicated in other sectors where secure, dynamic access control is critical, offering a scalable solution to meet evolving security challenges.

STRENGTHENING IAM ACROSS MULTI-CLOUD ENVIRONMENTS

Analytics Technology | 220% Churn Reduction | 350% ROI rate

Customer Overview

A leader in conversation intelligence technology, providing AI-driven analytics that empower organizations to gain valuable insights from customer interactions across voice, chat, and email channels.

Customer pain points and needs

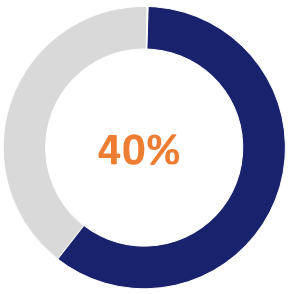
- Managing security across a multi-cloud environment with Microsoft Azure and AWS
- Challenges in implementing a Zero Trust model, particularly around seamless identity verification and access management for both internal and external users.
- Struggles with visibility into security events and integrating new security measures with existing infrastructure across their distributed systems.

Approach

- Use Entra ID AD as IdP for AWS SSO. Implement and leverage Azure PIM to manage and perform weekly reviews on privileged accounts.
- Integrate MFA and SSPR (Combined Registration) to enhance security and reduce IT support costs.
- Leverage Azure AD Conditional Access to implement dynamic, context-based access controls.

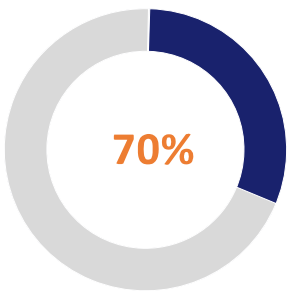
Value and impact

Automated Identity management workflows using Identity Governance



Administrative overhead

Overall improvement in security



Unauthorized access attempts

Lesson learned

FPT's use of Azure AD, Identity Governance, and Conditional Access to implement a Zero Trust approach proved crucial for ensuring secure identity management.

IMPLEMENTING AZURE LANDING ZONE WITH ROBUST IAM INTEGRATION

Analytics Technology | 220% Churn Reduction | 350% ROI rate

Customer Overview

The customer is a global tech leader recognized as the Largest IT Services Company in Fortune 500 SEA and Gartner's Top 50 IT Services Companies in Asia

Customer pain points and needs

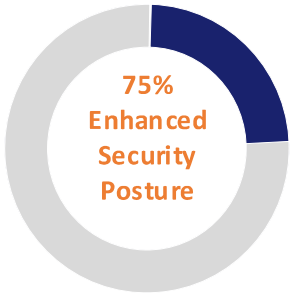
- Challenges in establishing a secure, scalable Azure Landing Zone to support its cloud adoption journey, solving concerns around scalability, security, and regulatory compliance.
- Need robust access control and governance to ensure a safe cloud environment, with differentiated access levels for regular users, developers, and administrators.

Approach

- Implement account tiering to segment user personas into three categories: User, Developer, and Admin, allowing for differentiated access control
- Implement Azure PIM to manage and secure elevated privileges for administrators. Privileged Access Workstations (PAW) were deployed for administrators for further security enhancement

Value and impact

Account tiering, PIM, PAW, and Conditional Access



Identity-related security incidents decreased **75%**

Automated IM workflows and JIT access

Time to manage user permissions and access requests decreased **50%**

Lesson learned

Implementing account tiering with specialized controls for administrators, such as PAW and JIT, proved essential in enhancing security for privileged access. This strategy is crucial for organizations moving to the cloud and seeking a Zero Trust approach.

To learn more about FPT Software, please visit our website at **www.fpt-software.com/service/cyber-security**