ShadowManage M365

SRKK Consulting Sdn Bhd

Prerequisites for ShadowManage M365 Service

Technology

Obtain the necessary Microsoft 365 licenses.

People

Ensure skilled personnel to manage and enforce technology.

Process

Implement policies to guide technology usage and compliance.

About Our Managed Service

Worry Free & Fast Response Within (SLA)

Your business up time is our top priority!

Certified Technical Competencies

System support and maintenance by certified support staff and consultants

Certified Partner With Industrial Leaders

Principal-backed support and solution consultancy.

Flexible Support

Priority multi-channel support through email, phone, remote support.

Ticket Management And Tracking

Reliability with our helpdesk system to efficiently track support process and monitor service standards

Maximize Digitalization Adoption

Provide information on program functionality, use case scenarios, and proactive technology updates

SRKK

ShadowManage M365

Simplified Onboarding

Access your customers tenants to quickly and easily configure settings, create users and assign licenses

Proactive Account Management

Take your customer relationships to the next level with AI-powered insights & recommendations

Tenant Configuration

Gain insight into configuration across all your tenants

Monitoring and Alerts

Monitor and manage customers centrally to easily identify gaps in end-customer configuration, target improvements, and drive adoption

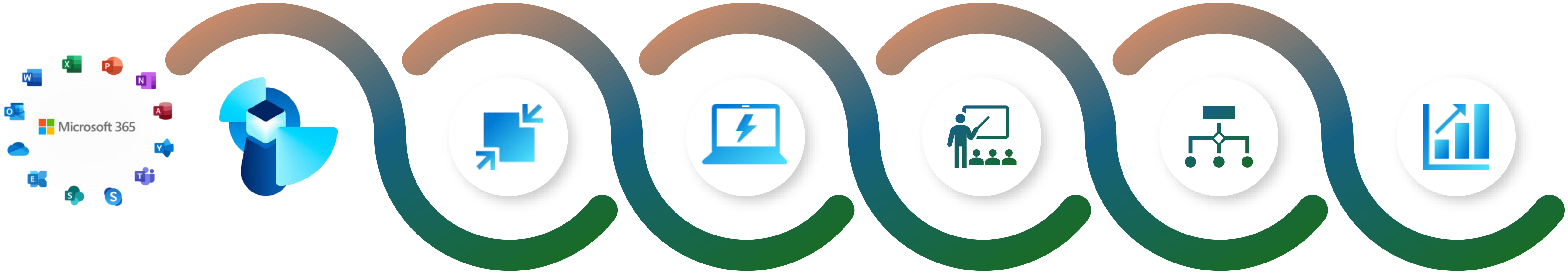
User, Device & Data Protection

Ensure your customers stay protected across devices, data, and users

Hassle-free. Simple. Secure.

SRKK

Enabling end-to-end success utilization of M365



Purchase Readiness

Possess the necessary licensing and exhibit readiness to implement a robust productivity and security solution.

Technical Readiness

Assess the customer's level of preparedness and compliance with governance requirements, and identify recommended configurations for implementation.

Targeted Assignment

Identify the best set of users and pilot to get started with and test features and policies.

Evaluation

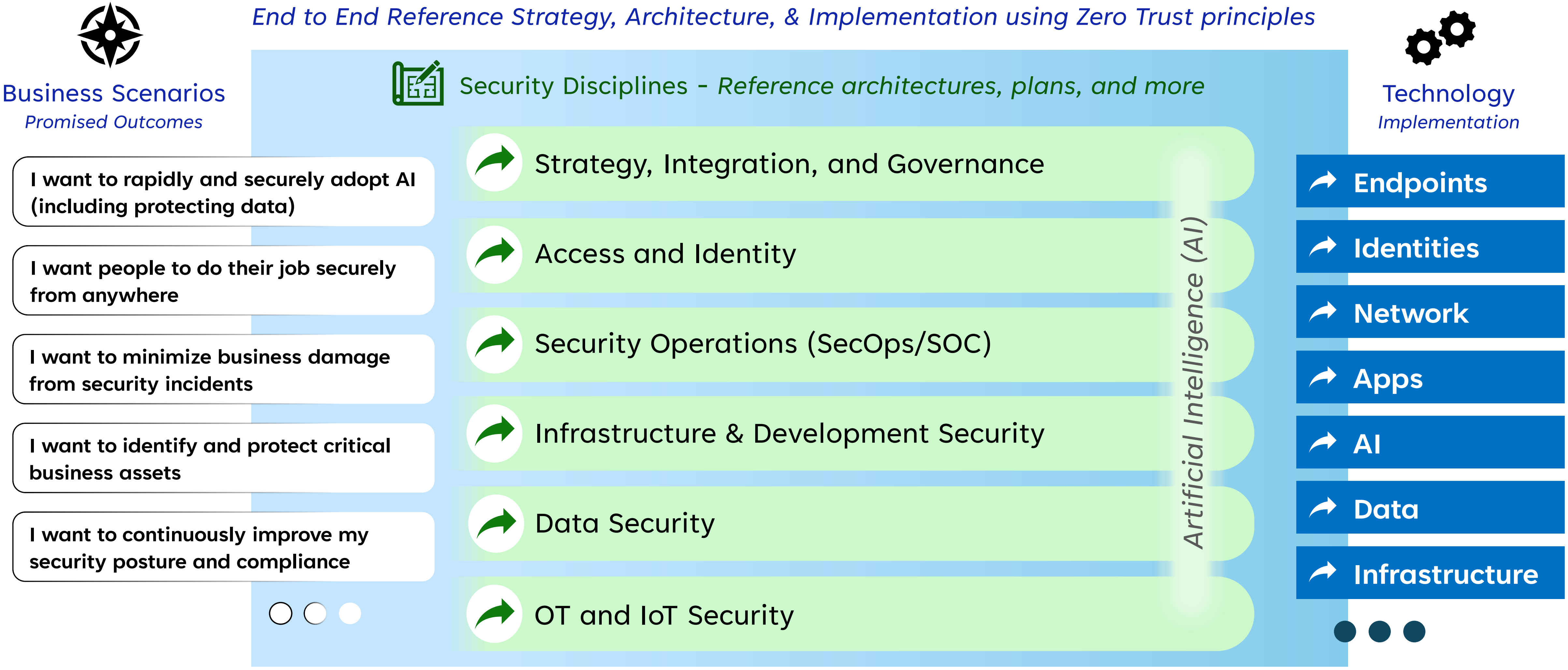
Track and measure user engagement and leverage resources and content to accelerate adoption and fine tuning.

Exploration Expansion

Identify customers who are prepared to elevate their current security and productivity posture to a more advanced level.

SRKK Adopt Security Adoption Framework (SAF)

Zero Trust security modernization aligned to business goals and risks



End to End Reference Strategy, Architecture, & Implementation using Zero Trust principles

Business Scenarios

Promised Outcomes

- **I want to rapidly and securely adopt AI (including protecting data)**
- **I want people to do their job securely from anywhere**
- **I want to minimize business damage from security incidents**
- **I want to identify and protect critical business assets**
- **I want to continuously improve my security posture and compliance**

○ ○ ○

Security Disciplines - *Reference architectures, plans, and more*

- Strategy, Integration, and Governance
- Access and Identity
- Security Operations (SecOps/SOC)
- Infrastructure & Development Security
- Data Security
- OT and IoT Security

Artificial Intelligence (AI)

Technology

Implementation

- **Endpoints**
- **Identities**
- **Network**
- **Apps**
- **AI**
- **Data**
- **Infrastructure**

● ● ●

Security Modernization with Zero Trust Principles

Security Strategy and Program

Business Enablement

Align security to the organization’s mission, priorities, risks, and processes

Assume Breach (Assume Compromise)

Assume attackers can and will successfully attack anything (identity, network, device, app, infrastructure, etc.) and plan accordingly

Verify Explicitly

Protect assets against attacker control by explicitly validating that all trust and security decisions use all relevant available information and telemetry.

Use least privilege access

Limit access of a potentially compromised asset, typically with just-in-time and just-enough-access (JIT/JEA) and risk-based polices like adaptive access control.

Zero Trust Architecture

- Access and Identity
- Infrastructure & Development Security
- IoT and OT Security
- Modern Security Operations (SecOps/SOC)
- Data Security

*Anything outside of Microsoft 365 modern workspace do not cover by ShadowManage365