Threat Protection

Helping clients mitigate and protect against cyber threats in their cloud

April 2022

Threat Protection

A suite of tools that enable visibility into immediate threats across email, identity and data

Do you know how many phishing attacks your organization has received? If employees are using the right password protocol? Whether personal data is being exposed? In short, is your organization's cloud environment as secure as you think it is?

If your organisation has workloads on Azure or M365 you can benefit from an integrated set of threat protection solutions that provide a holistic view of security and advance their Zero Trust strategy:

Microsoft Defender for Endpoint - delivers endpoint security for Windows, macOS, Linux, Android, iOS, and network devices and helps to rapidly stop attacks, scale your security resources, and evolve your defences. It's delivered at cloud scale, with built-in AI that reasons over the industry's broadest threat intelligence. It enables discovery of all endpoints and even network devices, such as routers, in your environment. It offers vulnerability management, endpoint protection, endpoint detection and response (EDR), mobile threat defence, and managed hunting all in a single, unified platform.

Microsoft Defender for Identity - formerly Azure Advanced Threat Protection, also known as Azure ATP), Microsoft Defender for Identity is a cloud-based security solution that leverages your on-premises Active Directory signals to identify, detect, and investigate advanced threats, compromised identities, and malicious insider actions directed at your organization.

REPLY
CLUSTER
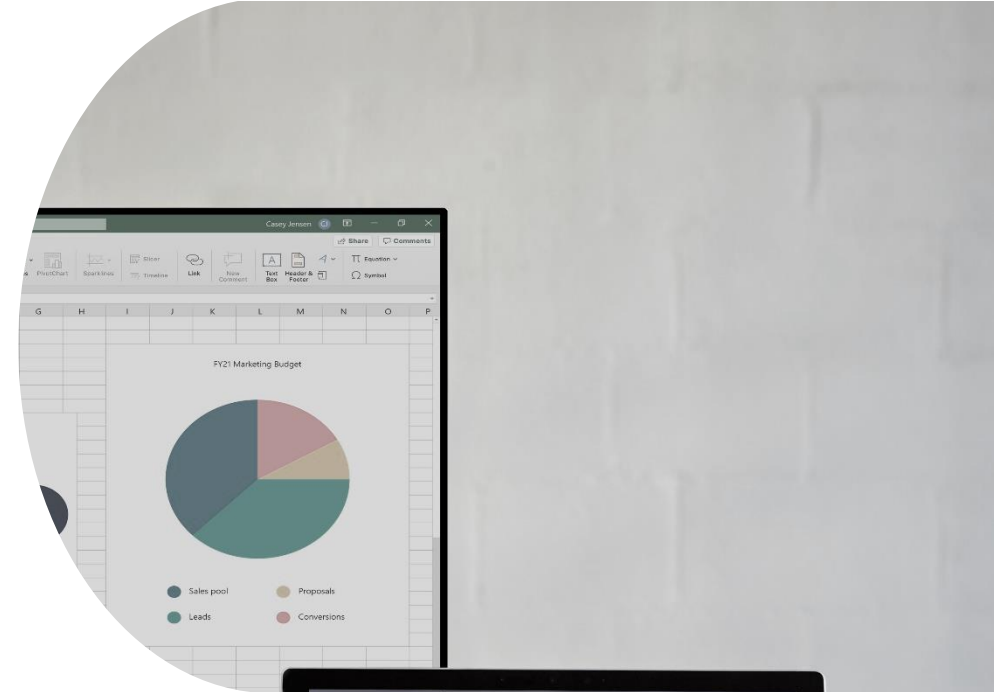
Threat Protection Workshop - **Overview**

REPLY CLUSTER

Strengthen your organisation 's approach to cyber security and accelerate your journey to Zero Trust

Designed as a three-day engagement, in this workshop we will partner with you to strengthen your organization's approach to cybersecurity. We'll help you better understand how to prioritize and mitigate potential attacks, with:

- Deep analysis of cyberattack threats that are found targeting your organization
- Actionable recommendations to help immediately mitigate the identified threats
- A detailed assessment of your IT and security priorities and initiatives, direct from cybersecurity pros
- An inside look at Microsoft's holistic approach to security, and how it relates to your organization
- Demonstrations of integrated security, including the latest tools and methods
- Long-term recommendations about your security strategy, with key initiatives and tactical next steps

Workshop Highlights

Review your security goals and objectives

Showcase security scenarios with product demos

Identify real threats in your cloud environment with Threat Check

Develop joint plans and next steps

Map identified threats to specific solution recommendations

Microsoft Gold Partner | Azure Expert MSP | Cloud Adoption Framework | Cloud Centre of Excellence

Threat Protection Workshop - Why attend

Learn how to put next-generation Microsoft security tools to work for you

Given the volume and complexity of identities, data, applications, devices, and infrastructure, it's essential to learn how secure your organization is right now, and how to mitigate and protect against threats moving forward. By attending this workshop, you can:

Identify current, ongoing security threats in your cloud environment

Walk away with actionable next steps based on your specific needs and objectives
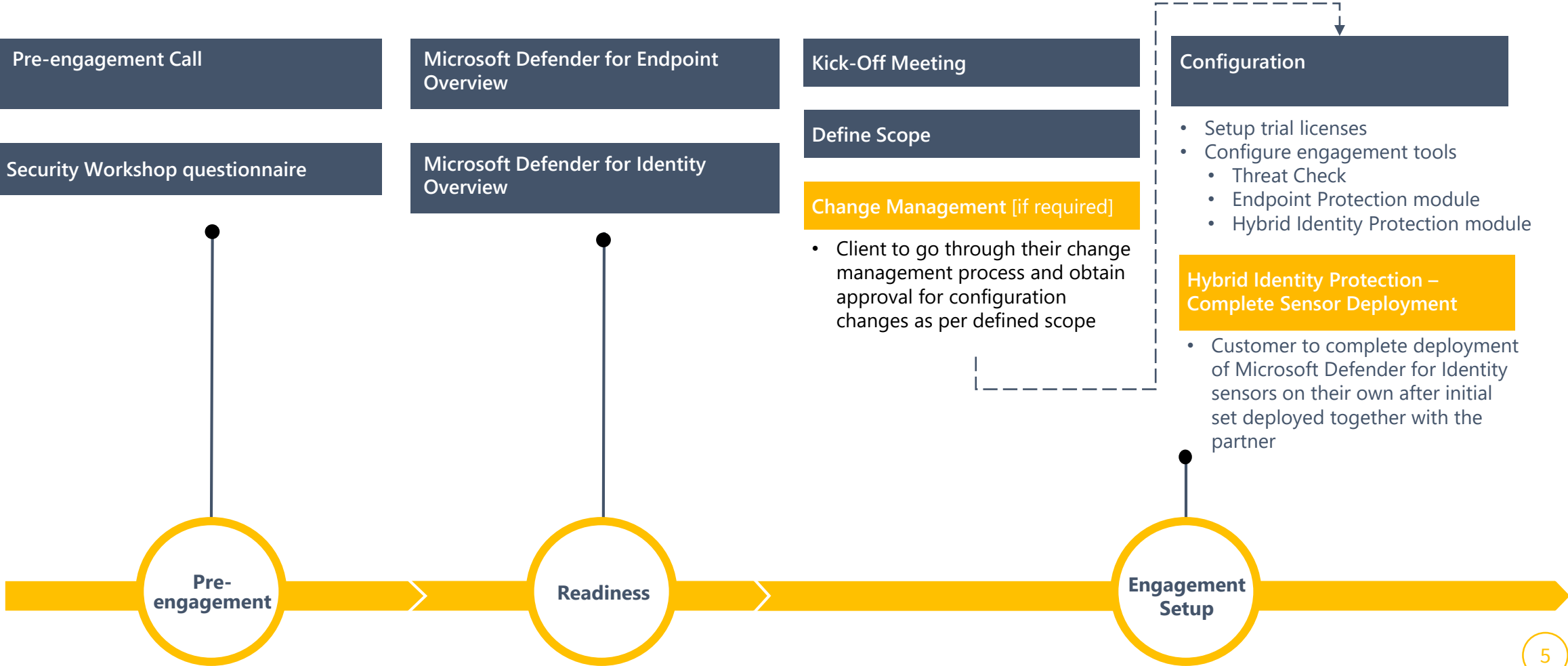
Document your security strategy for the benefit of key stakeholders

Better understand how to accelerate your security journey using the latest tools
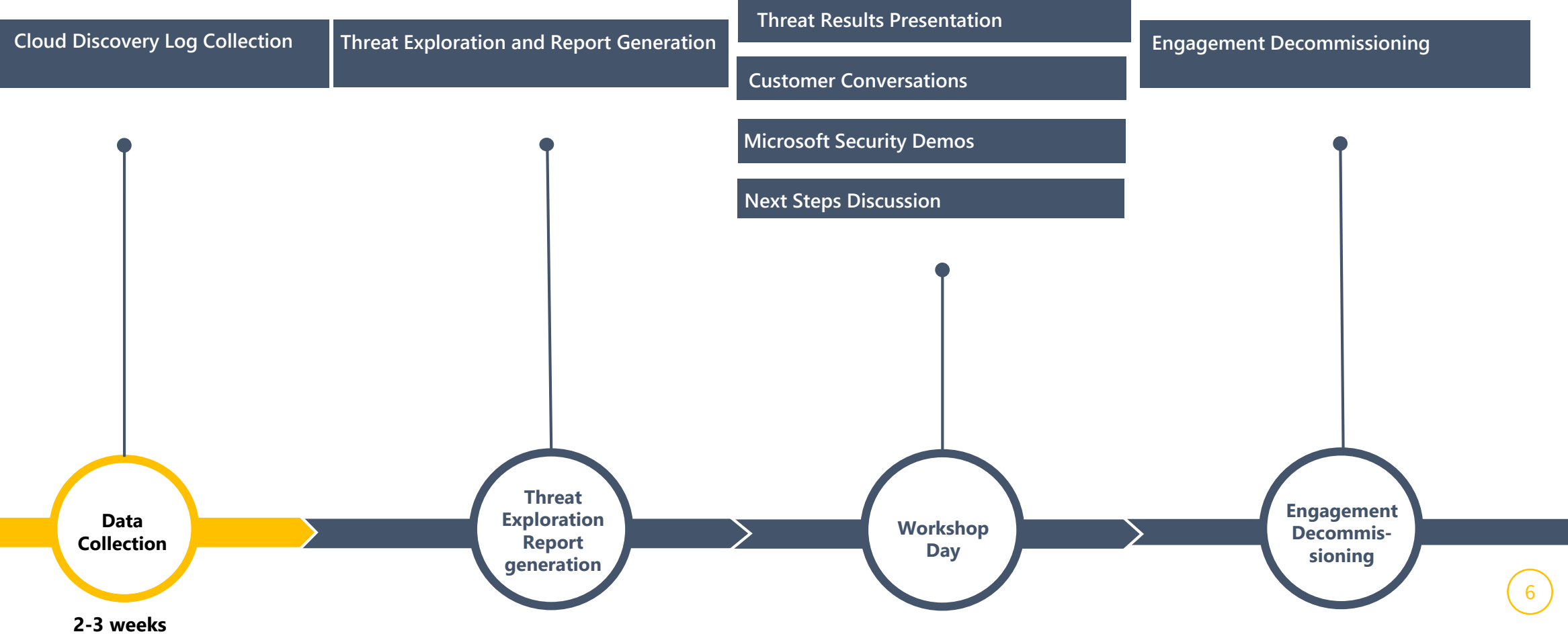
Threat Protection Workshop - Scope & Structure

A structured approach based on Microsoft best on practises and a well-defined methodology

Pre-engagement Call

Security Workshop questionnaire

Microsoft Defender for Endpoint Overview

Microsoft Defender for Identity Overview

Kick-Off Meeting

Define Scope

Change Management [if required]

- Client to go through their change management process and obtain approval for configuration changes as per defined scope

Configuration

- Setup trial licenses
- Configure engagement tools
  - Threat Check
  - Endpoint Protection module
  - Hybrid Identity Protection module

Hybrid Identity Protection – Complete Sensor Deployment

- Customer to complete deployment of Microsoft Defender for Identity sensors on their own after initial set deployed together with the partner

Pre-engagement

Readiness

Engagement Setup

Threat Protection Workshop - Scope & Structure

A structured approach based on Microsoft best on practises and a well-defined methodology

Cloud Discovery Log Collection

Threat Exploration and Report Generation

Threat Results Presentation

Customer Conversations

Microsoft Security Demos

Next Steps Discussion

Engagement Decommissioning

Data Collection

Threat Exploration Report generation

Workshop Day

Engagement Decommis-sioning

2-3 weeks

The Cluster Advantage

Cluster Reply is a multi-award winning technology consultancy specialising in Azure

Credentials

- **Microsoft Gold Competencies** – Gold competency is awarded to companies that have demonstrated the top level of expertise on a particular technology or service area. We hold 14 Microsoft Gold competencies, including **Gold Windows and Devices**, **Gold Datacentre, Gold Security** and **Gold Cloud Platform**.

- **Azure Expert MSP** – this accreditation assures clients that they are connecting with one of Microsoft's most capable and high-fidelity Azure Managed Service Providers. Whether you are working on mission-critical apps, entire datacentre footprints, or hybrid environments, Cluster Reply have proven their capabilities to be able to help you

Technical Expertise & Experience

Our architects and engineers have extensive experience in:
- Formulating security strategies and roadmaps helping organisations deliver flexible, secure and productive user experiences
- Deploying end configuring threat protection solutions such as Azure Sentinel, Microsoft 365 Defender and Azure Defender
- Assessing and optimising large-scale and complex Azure and M365 environments covering multiple tenants, across different geographies
- Designing and implementing cloud security technologies including AAD, Azure ADDS, Azure Sentinel, Microsoft 365 Defender and Azure Defender Certificate Authorities etc.

Making the most of cloud

Contact:

Christos Myrsakis
c.myrsakis@reply.com
+44 (0) 7880921202