Threat Check Workshop

Overview

Introduction

Overview: Onsite workshop to explore your security landscape, address your most pressing security goals and challenge, review high-level current threats and provide recommendations.

Outcomes:

- Understanding of current threats
- Threat Check findings report – your current active threats
- Proposed next steps and recommendations

Who should attend?

- CISCO/ Information Security role
- CIO/ IT Director
- IT Operations/Data Protection

A technical review into security strategy, tailored to your organisation

What we'll do during the workshop

Focus on learning about your priorities, initiatives and key influences on your security strategy.

Discover threats to your environment across email, identity, and data.

Learn about Microsoft's approach to security with an immersive experience.

Plan next steps on how we can work together.

Deliverables

Have initial **security strategy** documentation for your stakeholders.

Better understand, prioritize, and mitigate **potential threats**.

Accelerate your security journey with **Microsoft**.

Have defined **next steps** based on your needs and objectives.

What's included?

Discovery Session

Microsoft Security Overview

Threat Check

Microsoft 365 E5 Trial

Recommendations and Next Steps

Workshop Timeline

STAGE 1: CALL

Pre-engagement call

Goals:

- Introductions
- Define engagement scope
- Identify right stakeholders
- Engagement scheduling
- Align expectations & next steps

STAGE 2: THREAT CHECK

Threat Check Kick-Off

Goals:

- Kick-off meeting
  - Goals and deliverables
  - Engagement tools
  - Expectations and next steps

Technical Setup

Goals:

- Set-up Threat Check license
- Configuration

STAGE 3: WORKSHOP

Discovery Session

- Introductions
- Discuss challenges, opportunities and priorities

Microsoft Security Overview

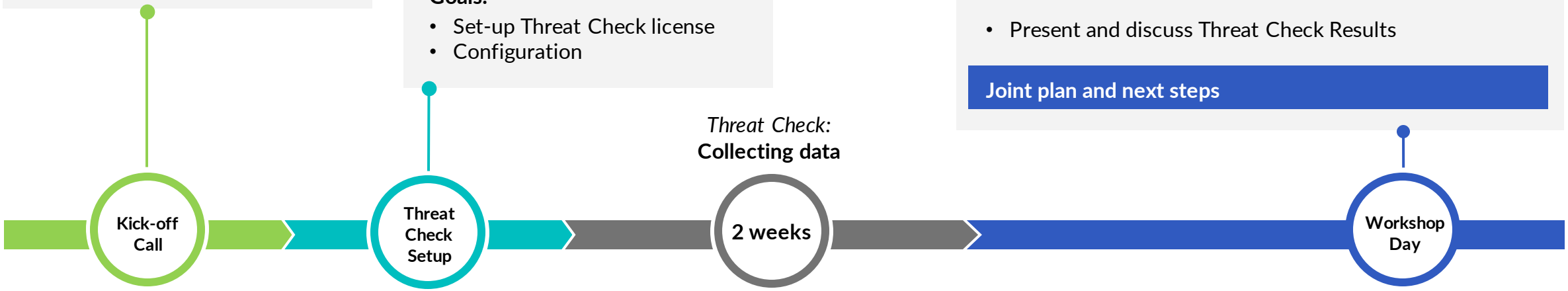
- Explore Microsoft 365 capabilities, discuss various technologies and features

Lunch

Threat Check findings

- Present and discuss Threat Check Results

Joint plan and next steps



Your Responsibilities

Access to key attendees

- Attendance of selected members of security or infrastructure teams is required for the workshop.

Provide stakeholder/sponsor oversight

- A stakeholder/sponsor is required to oversee and own the process from the customer side.

Trial setup and read-only access

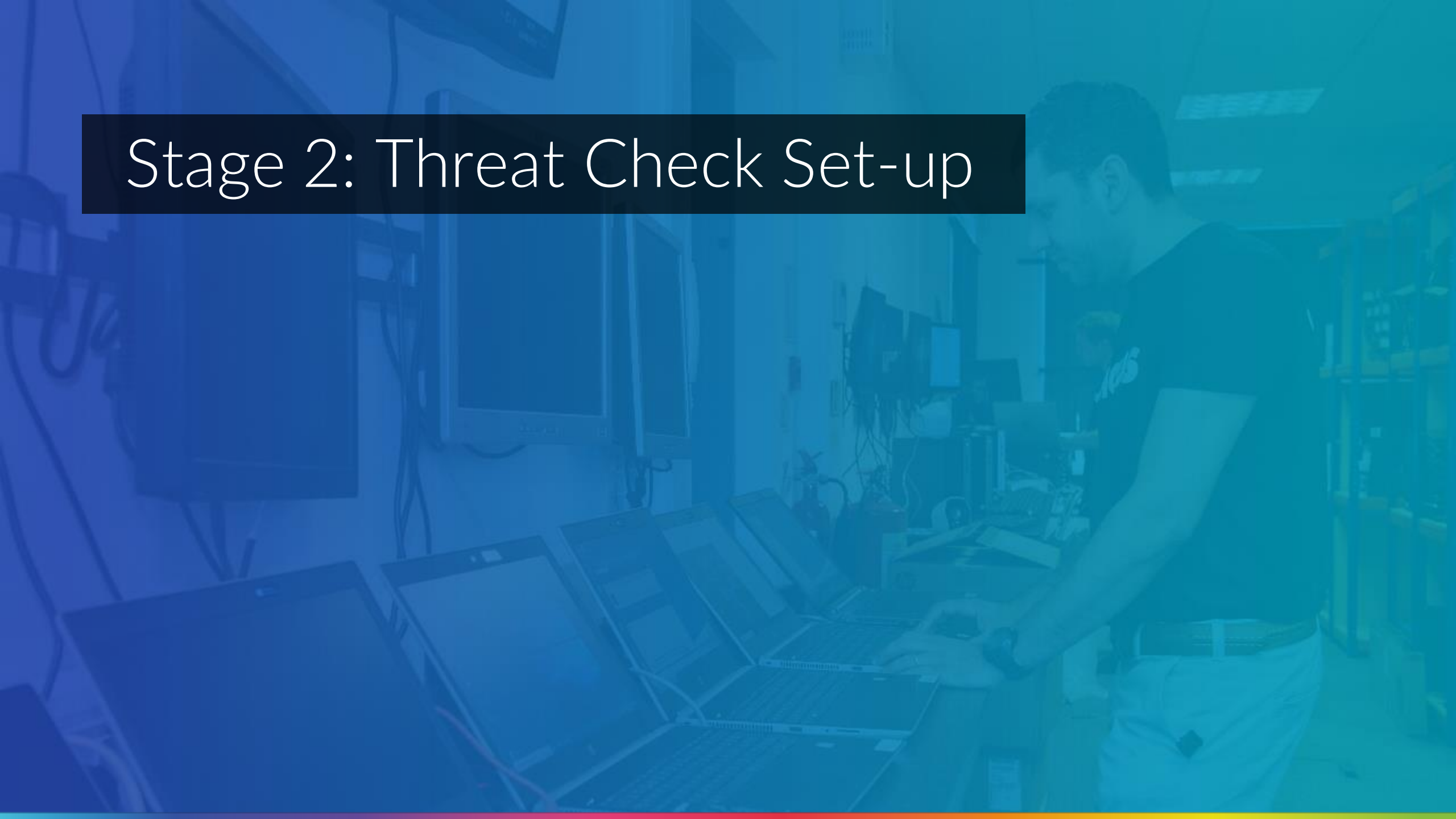
- Provide access to the tenant to set up the Threat Check (Microsoft 365 E5 trial) and provide read-only access for us to create the reports (duration of exercise only).

Stage 1: Kick-off Call

Kick-off Call

- Introduce team members and expected responsibilities
- Review and agree on engagement:
  - Objectives, approach and outcomes
  - Timelines and agenda
  - Tools necessary for conducting the engagement
  - Next steps
- Agree on project governance

Stage 2: Threat Check Set-up



Threat Check Overview

Microsoft 365 E5 Trial to discover and analyse live threats on your environment across email, identity and data.

Tools:

- Azure Active Directory Identity Protection
- Microsoft Cloud App Security
- Microsoft Defender for Office 365

Runs for **2 weeks** before the security workshop.

- **No impact** to users' experience or to their devices
- Set up with one of your Office 365 Admins and Azure admins: simple **step-by-step** instructions
- Requires read-only access for us to create reports (only for duration of workshop)
- Decommissioning of trial

Objectives

Discover threats

- Gain visibility into live threats to your Microsoft 365 cloud environment across email, identity and data

Mitigate threats

- Help you understand how Microsoft 365 security products can help you mitigate and protect against the threats found during this engagement

Out of Scope

- Deep analysis/investigation of threats found during the engagement or forensic analysis
- Technical designs or implementation
- Review of on-premise infrastructure threats

Outcomes

Threat Check Results report

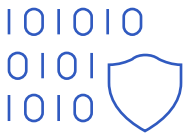
- Lists and interprets cyberattack threats targeting currently your organization, observed in this engagement

Threat Check Recommendations

- Maps observed threats to Microsoft 365 security products and features in order to mitigate impact of these threats

These will be presented at the Security workshop

Threat Check Tools



Azure Active Directory Identity Protection

Identity threat detection system

- Detect user identity threats such as compromised credentials or attempted sign-ins

Cloud App Security

Cloud Access Security Broker

- Raise alerts on user or file behavior anomalies in cloud apps leveraging their API connectors

Microsoft Defender for Office 365

Office 365 threat detection and prevention

- Detect threats to email and data such as attempts of phishing and malware

Stage 3: Security Workshop

Workshop Day Agenda

9 am – 10:30 am	15 min	10:45 am – 12 pm	1 hr	1 pm – 2pm	2pm – 3pm
Discovery Session	Break	Microsoft Security Overview	Lunch	Threat Check findings	Recommendations and Next Steps






Discovery Session

IT Objectives

- Outline current situation and pain points/challenges and discuss key IT objectives and initiatives

Security Priorities

- We assess your current maturity levels and priorities

Evaluation Report

- Interactive report to outline objectives, priorities and planned initiatives to feed into wider strategy

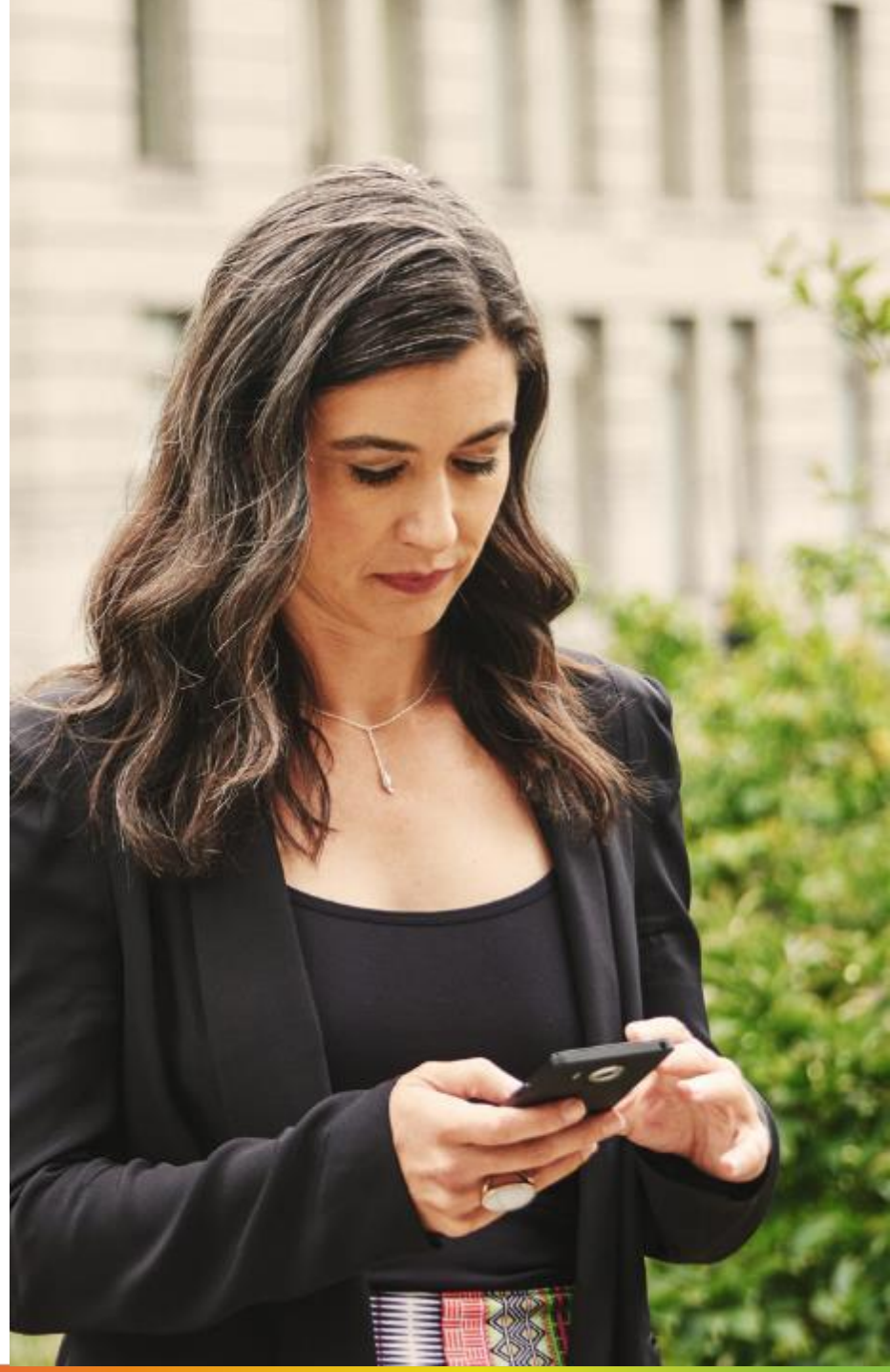
Microsoft Security Overview

Cyber security landscape

- Discuss the challenges and opportunities around modern cyber security in a cloud and mobile world
- Moving to a zero-trust approach; balancing tight security with end user experience

Microsoft security tools

- Discuss the various security tools available from Microsoft – what they are, features, capabilities and how they work together



Threat Check Results

Threat Check Report

- Go through the report and findings from the Microsoft 365 E5 trial to see what was discovered during the 2-week threat check trial on your environment

Threat Check Recommendations

- Present and discuss our recommendations based on discovered threats and outline how Microsoft tools can mitigate the risks

Recommendations

Discussion

- Review the day, outcomes, learnings and answer any final questions you may have

Recommendations

- Discuss our recommendations and best practices based on the day's findings

Next Steps

- We will work together to outline the best approach and next steps to fulfil your goals

Follow-up

Decommissioning

- We will show you how to decommission the Threat Check trial, or do this with you (requires admin access)

Reports and Documentation

- We will send the reports, recommendations and slides from the workshop

Next Steps

- We can discuss proposed next steps and see how you would like to proceed

northdoor
Store IT · Protect IT · Use IT

Contact us

+44 207 448 8500

info@northdoor.co.uk

www.northdoor.co.uk