Microsoft Security

Microsoft 365 Threat Protection Workshop

OLIVE + GOOSE

Date

Agenda:

1. Introduction & overview

2. Funding & nomination flow

3. Workshop modules
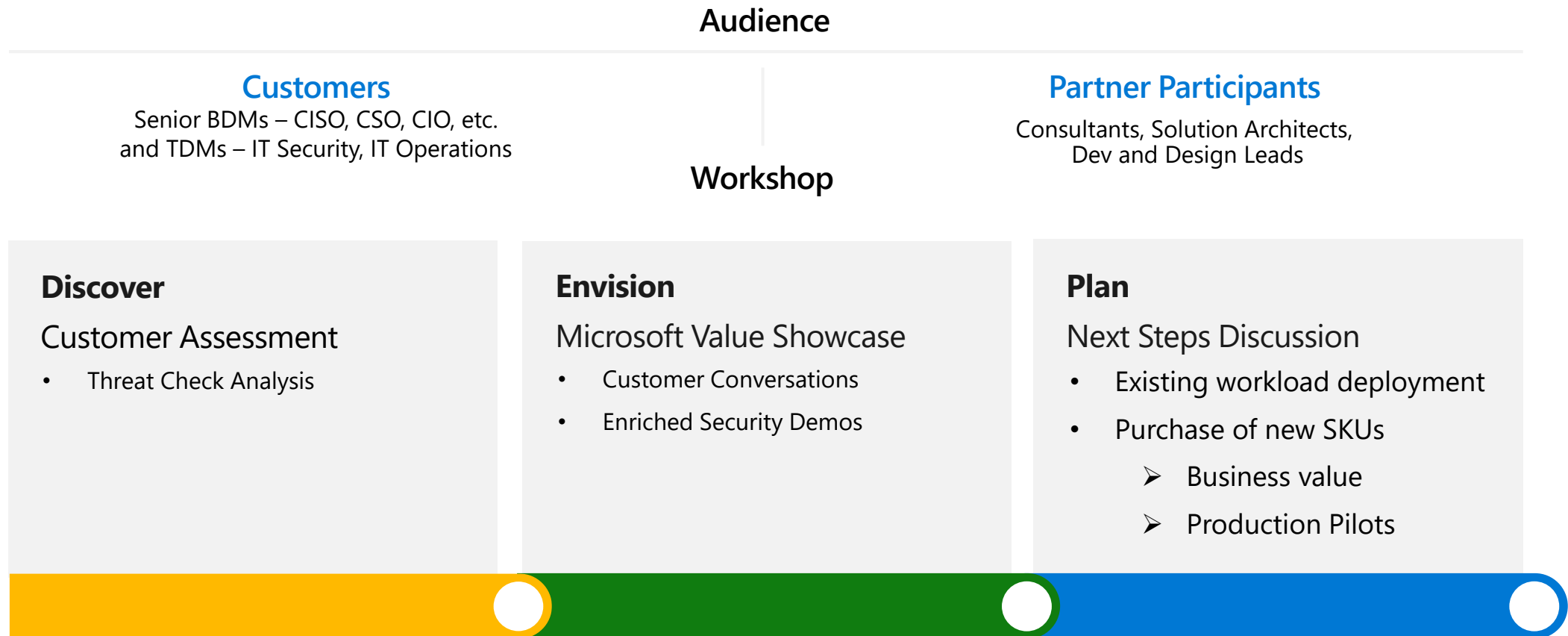
4. Workshop delivery phases

5. Resources

Introducing the Microsoft 365 Threat Protection Workshop

An executive deep dive into security strategy, tailored to your customers' organization.
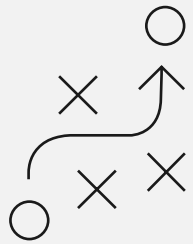
# Microsoft 365 Threat Protection Workshop overview

Designed as a three-day engagement, the **Threat Protection Workshop** enables partners to build intent for sales and deployment of advanced Microsoft Security workloads. The workshop uses a specialized Threat Check SKU for identifying real-time threats in a customer environment and will help define clear next steps and the best ways to mitigate risks.

Audience

Customers
Senior BDMs – CISO, CSO, CIO, etc.
and TDMs – IT Security, IT Operations

Partner Participants
Consultants, Solution Architects, Dev and Design Leads

Workshop

Discover

Customer Assessment

• Threat Check Analysis

Envision

Microsoft Value Showcase

• Customer Conversations

• Enriched Security Demos

Plan

Next Steps Discussion

• Existing workload deployment

• Purchase of new SKUs

  ➢ Business value
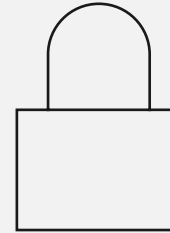
  ➢ Production Pilots
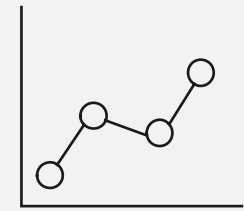
What is expected during workshop delivery

Focus on learning about customer's priorities, initiatives and key influences on your security strategy.
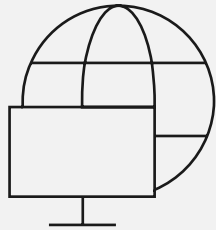
Discover threats to customer's environment across email, identity, and data.

Present Microsoft's approach to security with an immersive experience.

Plan next steps on how you and customer can work together.

Why deliver the Microsoft 365 Threat Protection Workshop

Customer benefits

Customized: exclusively focused on their specific security needs.

Real data: threat analysis based on customer's environment.

Solution oriented: mitigation solutions & actionable next steps.

Partner benefits

Use Microsoft funding to acquire new customers.

Position yourself as the trusted advisor for security strategy.

Opportunity to pitch deployment and managed services with Microsoft recommended outcomes.

Microsoft 365 Threat Protection Workshop modules

Threat Protection Workshop brings modular flexibility

Threat Protection Workshop

⚠️ **Day 1 – Microsoft 365 Threat Check**
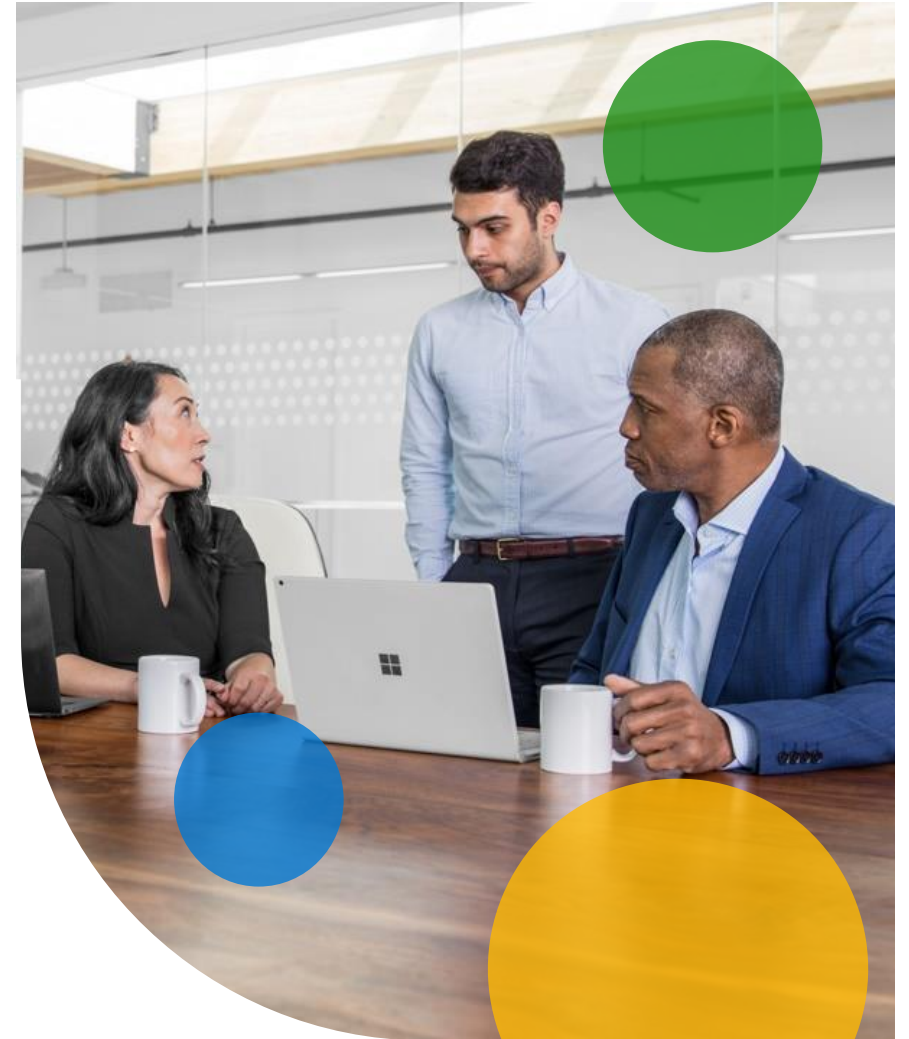
Day 2 - Optional Modules Demonstrating Microsoft 365 Security

💬 **Day 3 - Security Conversations**

Day 4 – Demo Microsoft 365 Security Products for Customer

Day 5 - Recommendations and Next Steps
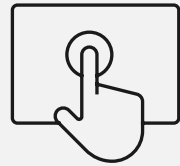
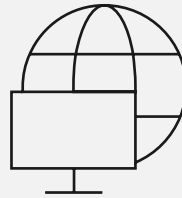# Microsoft 365 Threat Check module

Endpoint Protection optional module

# What we'll do during the Endpoint Protection optional module

Analyze your requirements and priorities for an endpoint detection and response solution

Define scope & deploy Microsoft Defender for Endpoint in your production environment, onboarding up to 100 Windows 10 devices
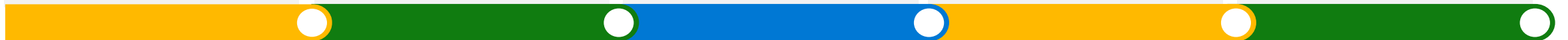
Discover threats to the included Windows 10 devices and demonstrate how to investigate and respond to threats
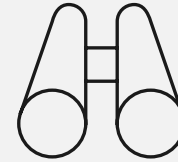
Discover existing endpoint weaknesses and what can be done to harden the endpoint surface area

Recommend next steps on how to proceed with a production implementation of Microsoft Defender for Endpoint
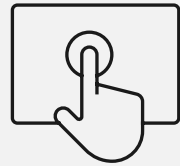
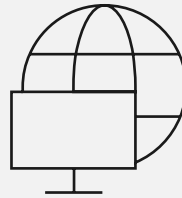# Hybrid Identity Protection
optional module

# What we'll do during the Hybrid Identity Protection optional module

Analyze your Active Directory structure and existing solutions that secure it.

Define scope & deploy Microsoft Defender for Identity in your production environment, setting up sensors on agreed Active Directory servers.
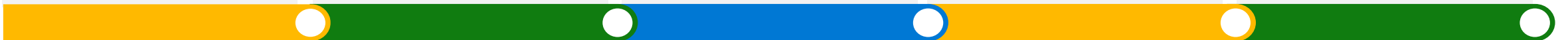
Discover threats to the Active Directory and demonstrate how to investigate and respond to them.
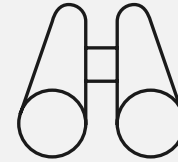
Discover existing weaknesses and what can be done to harden the Active Directory surface area.
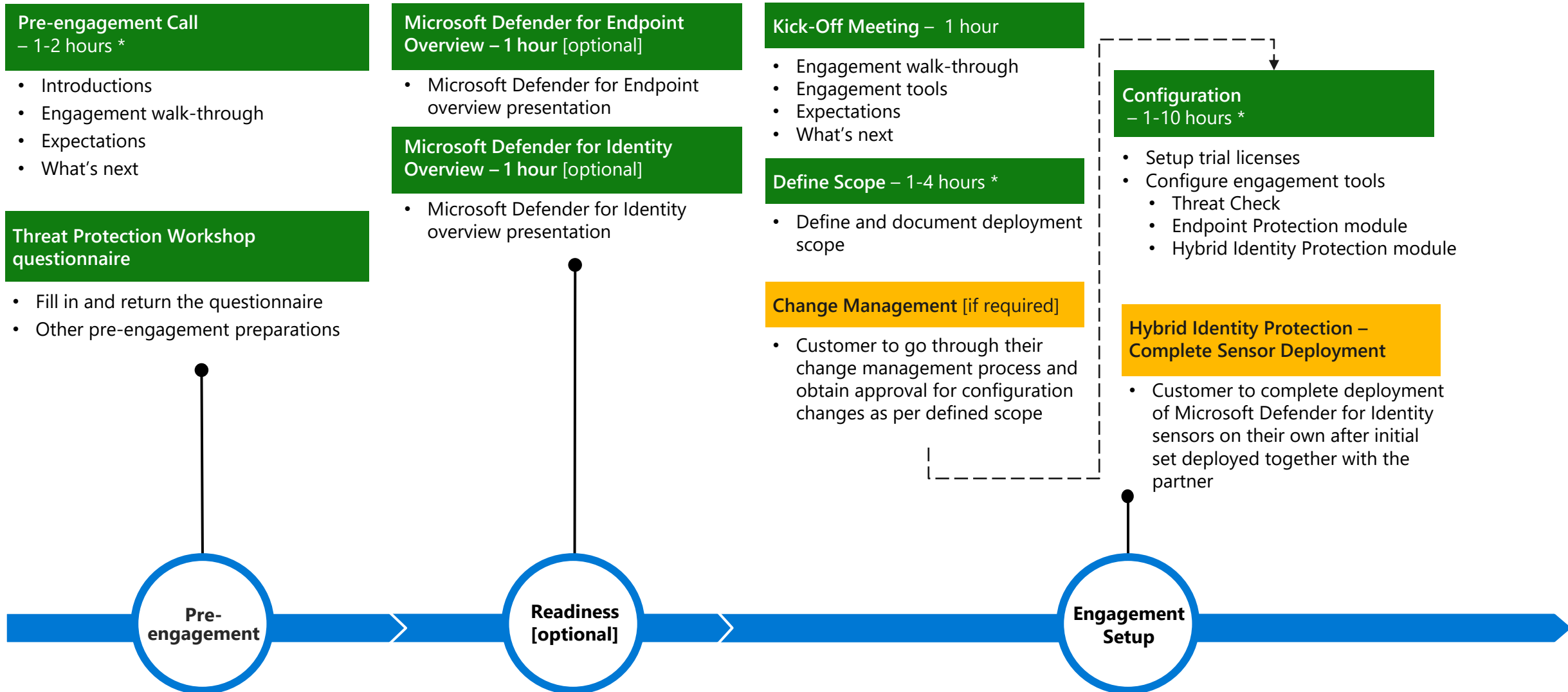
Recommend next steps on how to proceed with a production implementation of Microsoft Defender for Identity.

Microsoft 365 Threat Protection Workshop delivery phases

Threat Protection Workshop phases and activities

Pre-engagement Call
– 1-2 hours *

- Introductions
- Engagement walk-through
- Expectations
- What's next

Threat Protection Workshop questionnaire

- Fill in and return the questionnaire
- Other pre-engagement preparations

Microsoft Defender for Endpoint Overview – 1 hour [optional]

- Microsoft Defender for Endpoint overview presentation

Microsoft Defender for Identity Overview – 1 hour [optional]

- Microsoft Defender for Identity overview presentation

Kick-Off Meeting – 1 hour

- Engagement walk-through
- Engagement tools
- Expectations
- What's next

Define Scope – 1-4 hours *

- Define and document deployment scope

Change Management [if required]

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

Configuration
– 1-10 hours *

- 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 [optional]** → **Engagement Setup**

* Effort depends on modules delivered

Threat Protection Workshop phases and activities

Cloud Discovery Log Collection – 1 hour

- Upload cloud discovery logs

Threat Exploration and Report Generation – 4-16 hours *

- Threat Exploration
    - Threat Check
    - Endpoint Protection module
    - Hybrid Identity Protection module
- Proactive threat hunting [optional]
    - Endpoint Protection module
- Report Generation
    - Threat Check
    - Endpoint Protection module
    - Hybrid Identity Protection module

Threat Results Presentation – 2 hours

- Present and discuss results
- Record next steps

Customer Conversations - 1 hour

- Selected MS Security Conversation
- Customer Cost Savings Conversation

Microsoft Security Demos – 2 hours

- MS security experience

Next Steps Discussion – 1 hour

- Discuss next steps

Engagement Decommissioning – 1-2 hours

- Remove uploaded logs
- Remove configuration changes
- Deactivate trial licenses

Data Collection

2-3 weeks

Threat Exploration Report generation

*** Effort depends on modules delivered**

Workshop Day

Engagement Decommis-sioning

Data Collection

Data Collection

» Threats to identity, email and data detected by the engagement tools.

» Upload of Cloud Discovery logs (towards the end).

Threat Results Presentation

Threat Check findings

» Gain visibility into threats to your cloud environment obtained through Microsoft 365 security products.

» Get recommendations from Olive + Goose experts on how to mitigate or avoid cyberattacks.
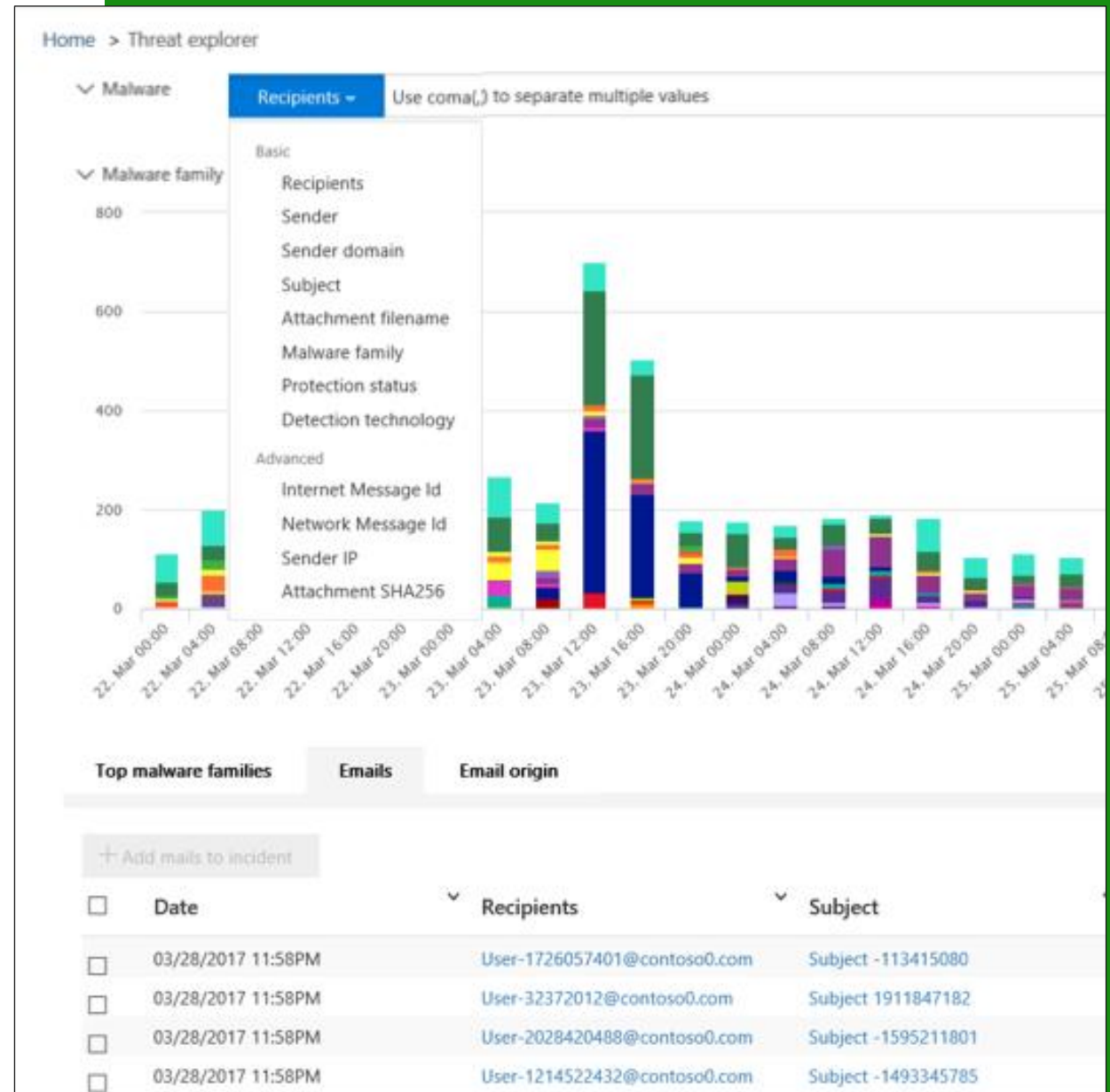
Customer Cost Savings optional module
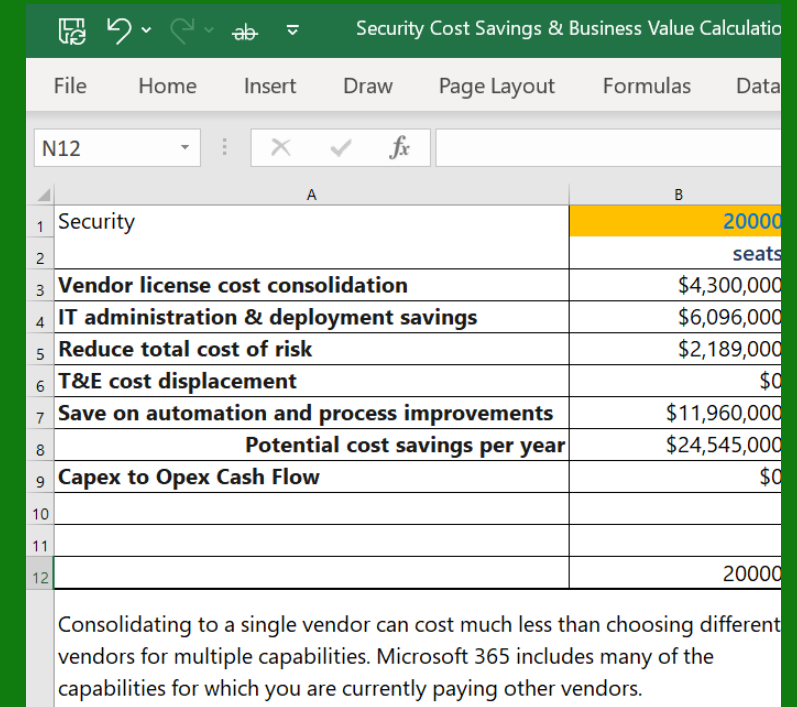
Cost Savings Conversations

Objective: Focus on how Microsoft 365 Security can help your customers reduce costs, while showcasing the value they realize with our integrated approach to security.

Assets: *Streamline and strengthen* presentation deck & *Cost Savings & Business Value* calculation worksheet.

» Streamline and strengthen your security

» Reduce costs

Assets to support the customer conversation deck

Pre-engagement call

- Discuss the cost savings deliverables

Explain what the customer will gain by the module

Customer questionnaire

- Gather customer values for calculation worksheet

Cost Savings & Business Value Estimations
Please provide information on cost dependencies

Question	Answer	Comment
Cloud access security broker license costs	$ per license	
Email protection license costs	$ per license	
Endpoint protection platform license costs	$ per license	
Endpoint detection and response license costs	$ per license	

Collects customer data in advance to update calculation worksheet

Calculation worksheet update

- Customer values for calculation worksheet

	A	B
14	**Vendor license cost consolidation**	
	License costs that can be avoided/retired	
15	**(all costs per user per month unless noted)**	
16	Number of users	20,000
17	Cloud access security broker	$ 6
18	Email protection	$ 5
19	Endpoint protection platform	$ 7
20	Endpoint detection and response	$ 7
21	Identity governance and protection	$ 5
22	minus E5 Compliance	$ 12
23	**Potential Annual savings**	$ 4,300,000

Allows customization of conversation decks to align to customer scenario

Can be used to adjust cost savings presentation if customer is comfortable providing info in questionnaire, or can be completed in real-time during the Workshop Day

Deliver Workshop Cost Savings conversation

Conversation Deck

- Offers cost savings calculation explanation.
- Allows for easy customization before presentations.

Explains how the calculations in the deck have been done incl. references for having strong customer conversations.

Calculations Workbook

You can customize the calculations in the conversation deck, offering a starting point to explain to customers how we can help them with Cost Saving & Business Value.

Microsoft Security Demos

Microsoft Security Demos

Objective: Demonstrate how Microsoft security products can enable customers to get better insights into potential threats that span across identities, users, endpoints, apps, and data.
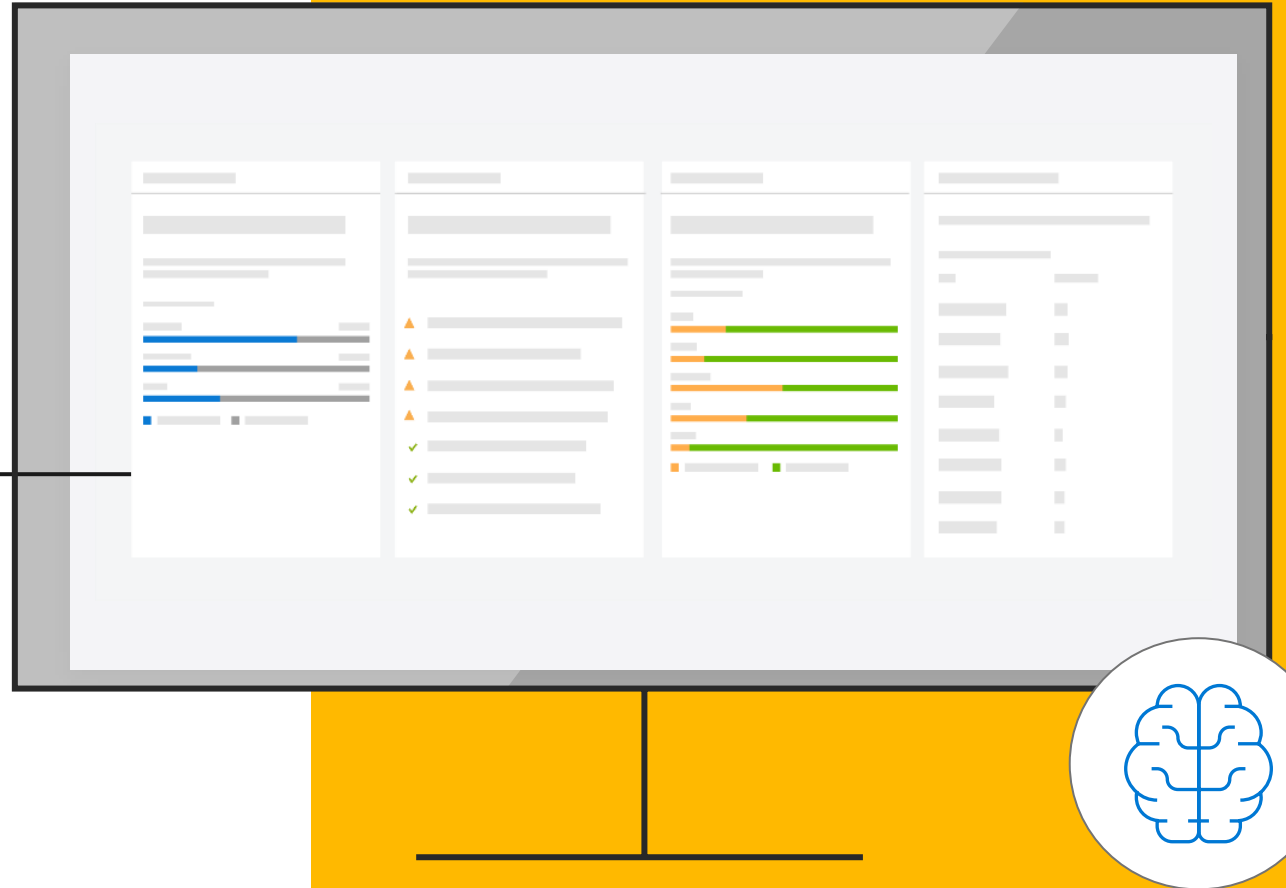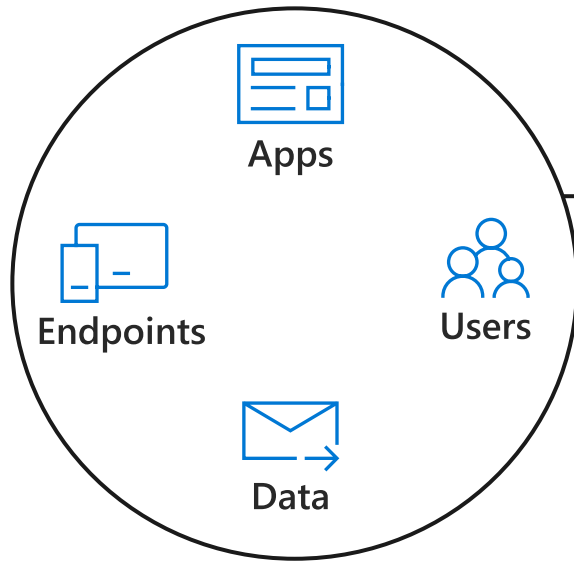
Next Steps Discussion

» Technical-level next steps, such as quick deployments

» Strategic-level next steps

» Agree on follow-up engagements

Engagement Decommissioning (Optional)

» Remove uploaded logs

» Remove configuration changes

» Deactivate trial licenses

Resources

Resources

· Threat Protection workshop partner webpage: https://aka.ms/ThreatProtectionWorkshop

· Delivery resource & guides: https://aka.ms/ThreatProtectionWorkshop/Resources

· Threat Protection Workshop FAQ: https://aka.ms/ThreatProtectionWorkshop/FAQ

· Security & Identity Partner webpage: https://aka.ms/Security-Identity-Partners

Join the Microsoft Security, Compliance & Identity Yammer Group

Microsoft Security

Thank you.
OLIVE + GOOSE