

# Microsoft Defend Against Threats with SIEM + XDR Workshop.

Discover threats and vulnerabilities to your Microsoft cloud and on-premises environments.

nexustek nt.



**Contact Us:** <https://www.nexustek.com/contact-us/>

**Website:** <https://www.nexustek.com/>

## About Us

Trusted by thousands of businesses for over two 27 years, NexusTek, a national provider of managed IT services and full IT outsourcing solutions, offers a comprehensive portfolio comprising end-user services, cloud, infrastructure, cybersecurity, and IT consulting.

As a Microsoft Solutions Partner, NexusTek has earned a solutions designation in Modern Work. Ranked among the top MSPs in North America and a multi-year CRN Triple Crown Award winner, NexusTek's 24/7/365 domestically staffed support team designs holistic technology solutions to improve business continuity, productivity, operational efficiency, and cost-effectiveness for companies across the U.S., Canada, and Mexico.

As an SSAE 18 SOC II certified company, NexusTek conducts yearly rigorous security audits to ensure customer safety and provide optimal service.



Modern Work



# Objectives

## Discover

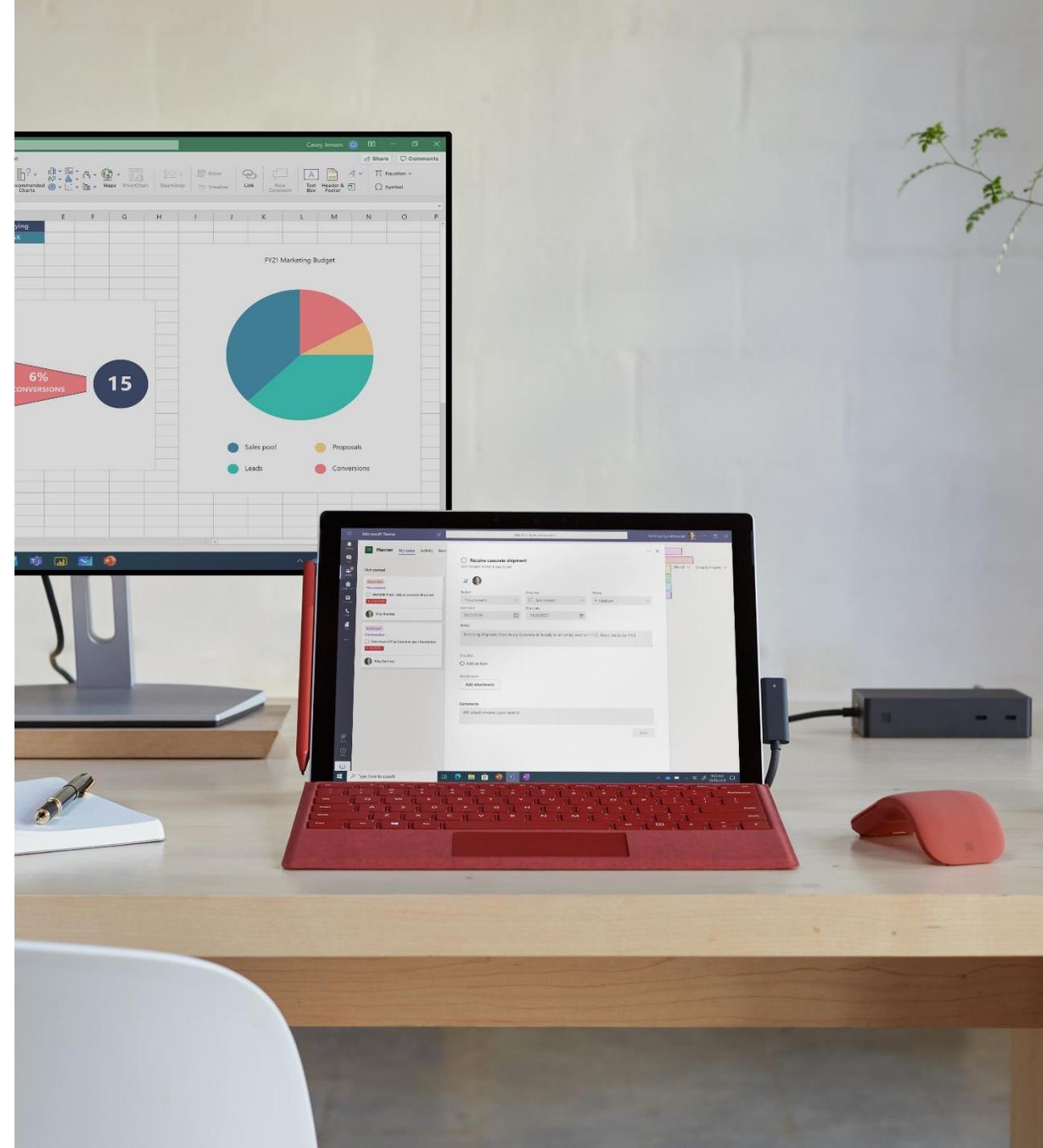
Gain visibility into the customer's endpoint management and security goals and objectives.

## Showcase Microsoft Intune, Azure AD and Defender for Endpoint

Present Microsoft Intune, Azure AD and Defender for Endpoint features related to managing the entire device lifecycle and protecting your users, data and devices from anywhere. Enable these features in the customer environment focusing on cloud-only management and protection for selected users and devices.

## Define results and next steps

Provide the customer with the results of all activities included in the Endpoint Management with Security Workshop and agree on the next steps that will help the customer to move to a modern management solution based on Microsoft Intune, Azure AD and Microsoft Defender for Endpoint.



# What we'll do during the workshop



**Focus** on learning about your priorities, initiatives and key influences in your endpoint management and identity protection strategy



**Learn** how Microsoft Intune supports managing the entire device lifecycle and how Azure AD and Defender for Endpoint secures your data, identities and devices



**Work** together on showcasing cloud-based endpoint management and protection in your production environment

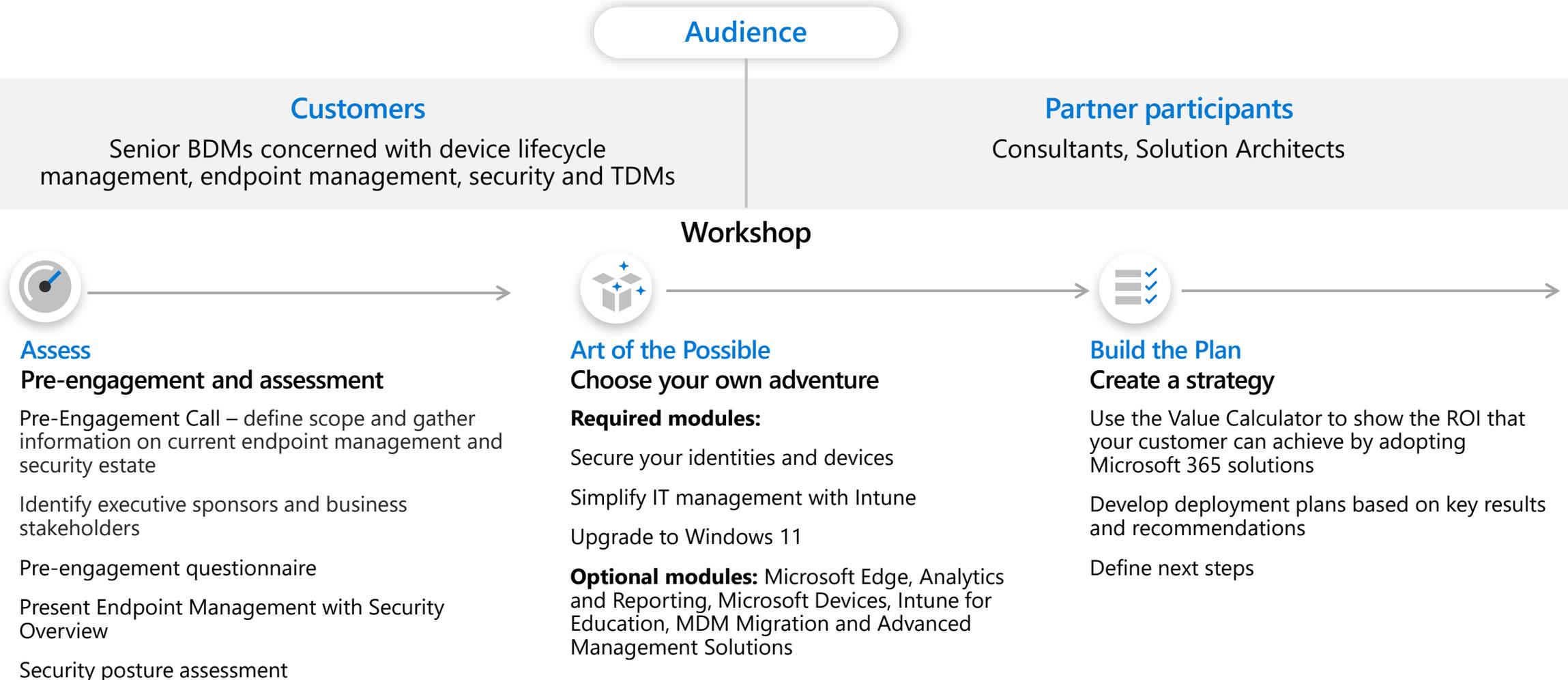


**Plan** next steps on how we can work together



# Endpoint Management with Security Workshop overview

The Endpoint Management with Security Workshop enables partners to lead customer conversations around modernizing their endpoint management and security capabilities by leveraging Microsoft 365. By making use of **Microsoft Intune, Intune with Tenant Attach, Azure Active Directory, Defender for Endpoint, Autopilot, and Endpoint analytics**, this workshop gives customers visibility into their IT estate and will help define clear next steps and the best ways to manage and secure endpoints at the enterprise level.



# Customer benefits of the Endpoint Management with Security Workshop

Today's users are looking for more ways to remain productive while working on any device. 95% of organizations allow personal devices in the workspace while 70 million smartphones are lost every year. With users asking for more ways to work the way that they want, this workshop will show you how to manage and protect both company-owned and user-chosen devices in the cloud and how to secure identities, devices and data in your organization.

**This workshop will show you how to leverage intelligent security, risk-based controls, zero-touch provisioning, and advanced analytics to enable cloud management for the devices your users need.**



**Learn** how to improve your knowledge of cloud-based device management and security using Microsoft solutions



**Discover and protect** your endpoints by enforcing policies and deploying security tools



**Secure** your identities with multi-factor authentication and conditional access from any device



**Enable** your users to be productive with the applications they need, on the devices they want



# Who should attend

## IT Management decision makers

C-Suite

Chief Information Security Officer (CISO)

Chief Information Officer (CIO)

Chief Security Officer (CSO)

Endpoint management owners/decision makers

## Other roles

IT Security

IT Operations

Security Architect

Security Engineers

Application business owners

## Top concerns

Users don't have the same secure, productive experiences from home as they do from the office.

Modern device management has expanded from desktops and laptops to include all user devices.

Organizations want to ensure that Windows endpoints are up-to-date and secured.

Users want to have access to the latest versions of Office apps on any device.

IT wants to implement policies that enable productivity, but not at the expense of company security.

BYOD is common with remote workers; these devices need to be configured for secure access to prevent data leakage.

Provisioning new devices quickly and managing updates and patches for all devices can be a struggle.

**Contact us to  
schedule a workshop  
today!**

**Contact Us:**

<https://www.nexustek.com/contact-us/>

**nexustek nt.**