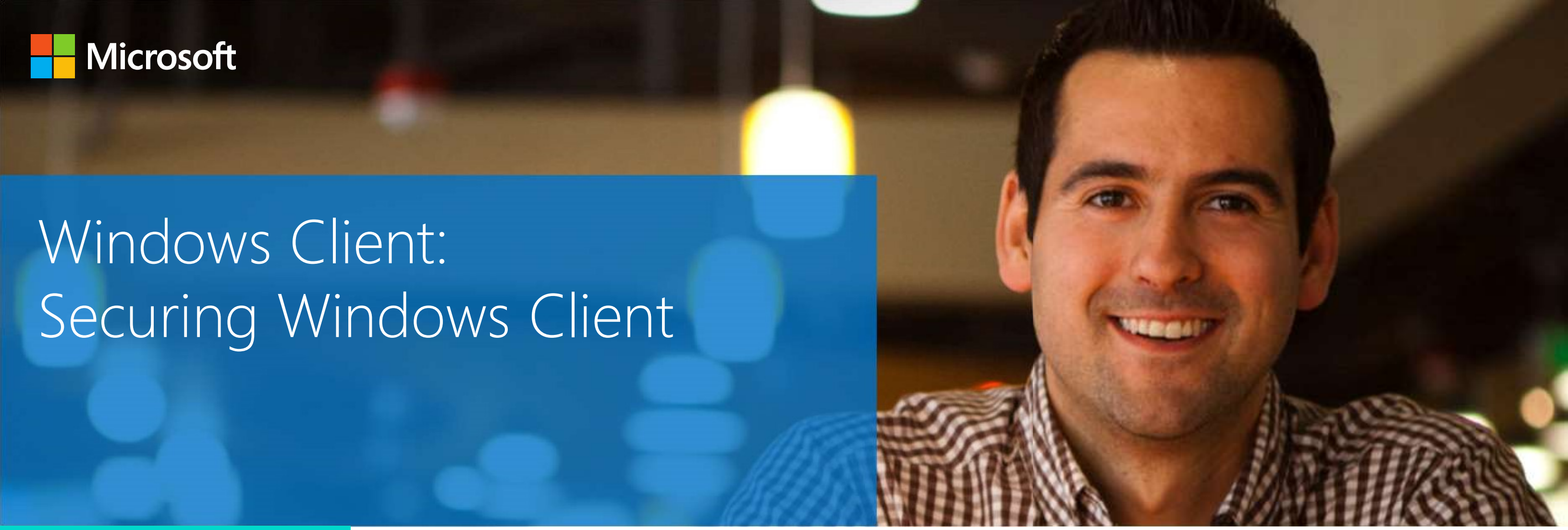

Windows Client: Securing Windows Client

Workshop*PLUS*

Target Audience

This WorkshopPLUS is targeted at the following IT professionals who deploy, design, and implement Windows Client environments:

- *IT Administrators*
- *Windows Infrastructure Engineers*
- *Desktop Administrators*
- *IT Security staff and Administrators*

Key Features and Benefits

- *Hands-on labs and demos*
- *Workshop structure is modularized and can be customized according to customer's needs*

Overview

Security threats are increasingly a focal point for many enterprises. Cyber-crime, industrial espionage, and diversity of malware are expanding dramatically. There is no single tool that can protect your assets against all threats. However, by protecting your client infrastructure with defenses at different layers of security, you can significantly reduce the potential exposure.

Corporate client machines and devices can introduce significant security risk. This Workshop*PLUS* demonstrates Microsoft's technologies, tools, and methods which can be used to design, deploy, and control client-side security by significantly decreasing several risks in Windows 10 environments.

The three-day Securing Windows Client Workshop*PLUS* provides students with the skills required to protect Windows clients against unintended access or intrusion.

This Workshop*PLUS* covers:

- Understanding the full story behind Credential Theft and Pass the Hash (PtH) attacks and know all the mitigations and countermeasures available for Windows 7 and later operating systems.
- New and existing security features in Windows 10 (including version 1803).
- Virtualization-based security.
- Exploit Guard.
- Securing the boot process, including BitLocker and Secure Boot.
- Virtual Smart Cards and Windows Hello for Business.
- Protecting network communications, including Windows Firewall, IPsec and VPN.

Technical Highlights

After completing this WorkshopPLUS, you will be able to:

- Understand an implement security features and built-in tools of Windows 10.
- Understand the current threat landscape and have an understanding of the most important mitigations.

Prerequisites

The students must possess knowledge of the following:

- *Security threats and vulnerabilities*
- *Group policy management*
- *Windows Firewall*
- *Network security concepts*

Hardware Requirements

Labs are hosted on the Labs On Demand Internet platform. Students need access to the Internet for the entire length of this workshop. For best user experience it is recommended to provide two monitors for each user.

Syllabus

This Workshop*PLUS* suggested duration three full days. Students should anticipate consistent start and end times for each day. Early departure on any day is not recommended.

Module 1: Today's IT Security Landscape, Credential Theft and Mitigations. This module provides an overview of the current security landscape and goes in detail on credential theft techniques and the corresponding mitigations.

Module 2: Security Features at OS Level. This module details tools that have been available since Windows 7 but are still not very well known (Address Space Layout Randomization (ASLR), User Account Control (UAC), Mandatory Integrity Control (MIC) , AppLocker) as well as some new features introduced in Windows 10.

Module 3: Securing the Windows Boot Process. This module presents file and data layer security, and protections against offline attacks on client assets. The technologies reviewed in this module include BitLocker and Secure Boot.

Module 4: Virtualization-based Security. This module covers System Guard Container, Credential Guard, Device Guard Lockdown State, Windows Defender Application Guard.

Module 5: User Authentication. During this module we will discuss alternatives to password-based authentication (virtual smart cards, Windows Hello for Business).

Module 6: Protecting Client Network Communication: This module focuses on securing the network layer by providing a deep insight of built-in Windows Firewall, IPsec and VPN capabilities.

Module 7: Windows Defender Exploit Guard: This feature is new in Windows 10 version 1803, but some parts of it used to be known as EMET. During this module you will have a look into all four components of Exploit Guard.