

Episode Title: Configure and manage Exploit Protection

Objectives:

At the end of this episode, I will be able to:

1. Define what Exploit Protection is
2. Understand where to configure Exploit Protection
3. Export Exploit Protection settings to Intune for scalable deployments

Key Points:

Key Point 1

Exploit Protection is built-in to the Windows operating system and provides program-specific and OS-level settings. These settings include Control Flow Guard, Data Execution Prevention, and Randomized memory allocation.

Key Point 2

All of these settings are enabled by default for Windows operating systems. You can customize them as-needed for your applications.

Key Point 3

After customizing the settings as-needed, you can export them from the client to use with Microsoft Intune. This allows you to deploy the customized settings at scale to specific or all computers in the organizations.

- If additional resources are used during the episode, they can be obtained using the download link on the overview episode (e.g. diagrams, no powerpoints)

External Resources:

If external resources were used during this episode, you can reference the following external resources for supplementary tools and information, if none were used, then this section will be blank:

- Enable exploit protection
: <https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection?view=o365-worldwide>