

Ugur Koc, 11/28/2024

# Intune & EPM: Locking Down Security While Keeping Users Happy



**GREEK MICROSOFT SECURITY**  
C O M M U N I T Y

# Who is this guy?

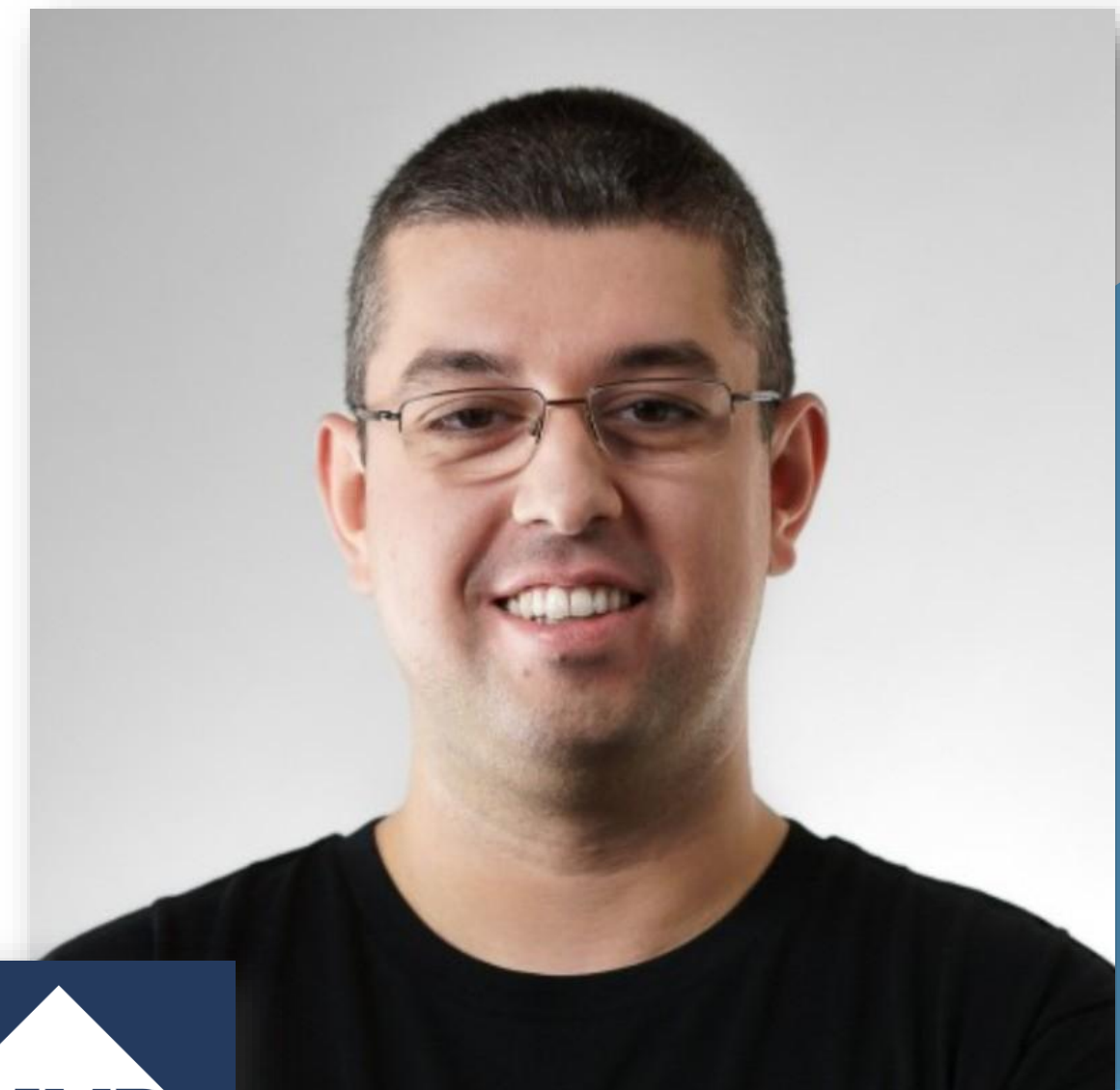
*Mastering Intune by Day, Coding Scripts and Applications by Night*

- Microsoft MVP
- Cloud Engineer, with a Focus on Intune and Endpoint Security
- You might have used some of the Projects or websites at some time:
  - KQLSearch.com
  - Kusto Insights Newsletter with Bert-Jan Pals
  - Several Intune Tools, Scripts

LinkedIn:	ugurkocde
X:	@ugurkocde
BlueSky:	@ugurkoc.de
Blog:	www.ugurkoc.de
GitHub:	ugurkocde

Let's connect!

This is me




# The Challenge

- Working at a Helpdesk or Support-Role
- People asking for Help installing software or drivers
  - “I need this new update installed, NOW!”
  - “I want to print my favorite pizza recipe!”
- Admin Password vs. Packing Applications (Bad vs. Slow)
- Super Stressful and a lot of manual work



# The Solution

-  Endpoint Privilege Management (What a surprise!)
- Elevate only specific Processes
- Separated Accounts (Virtual vs. Current User)
- No confusion! The user can only elevate what we allow him to elevate!



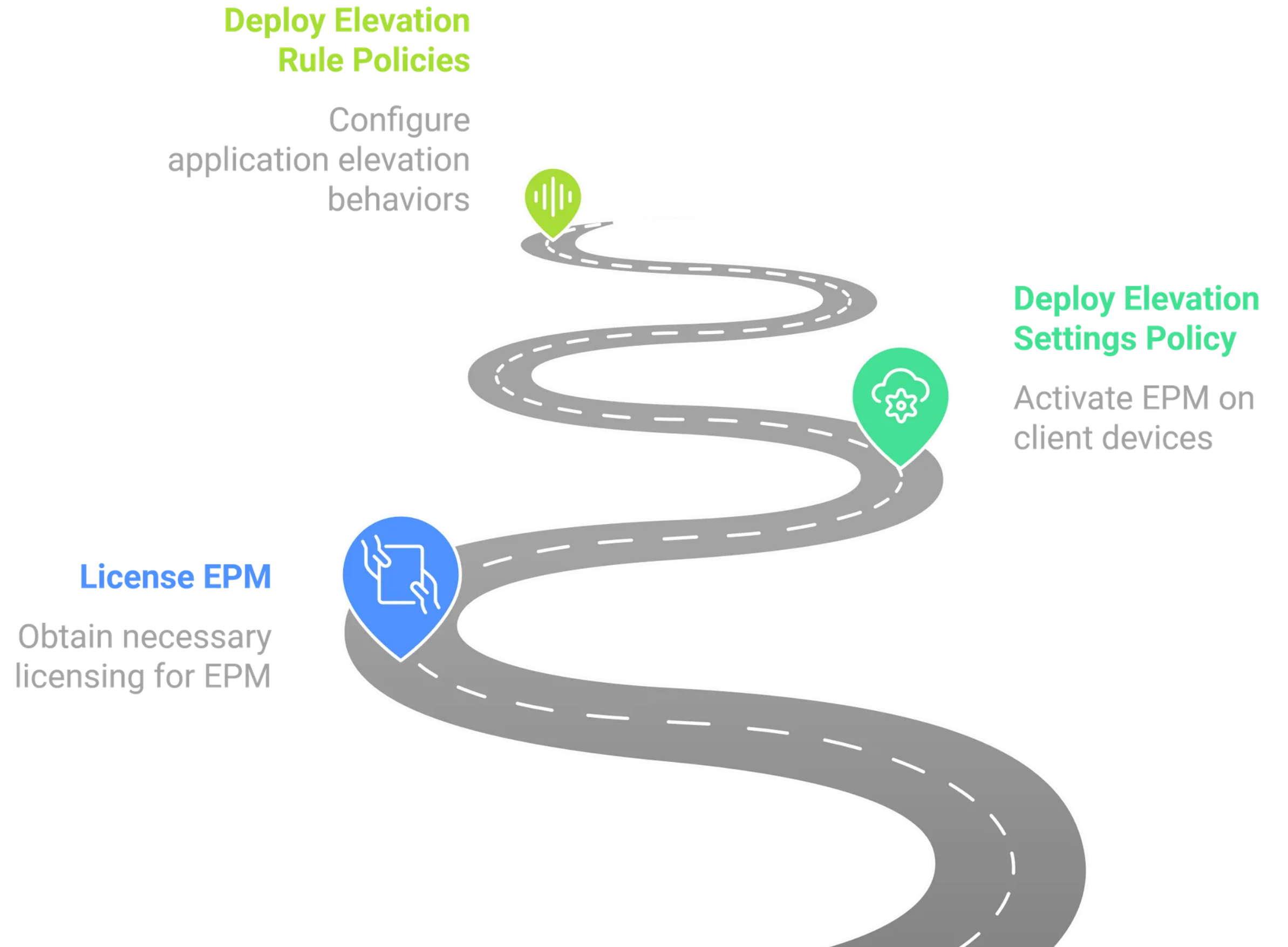
*“EPM grants standard users temporary, controlled admin access for specific tasks, enhancing productivity while reducing security risks.”*



# EPM in Action: User and Admin Experience

# Setup EPM

- Onboard Devices with a Settings Policy
- Elevation Rules for Applications



# Default elevation for unmanaged executables

- Support Approval
- Deny All
- User Confirmation

## Support Approval

Needs administrator approval for elevation requests.



## Deny All Requests

Blocks elevation requests for undefined files.



## User Confirmation

Requires user validation for elevation requests.



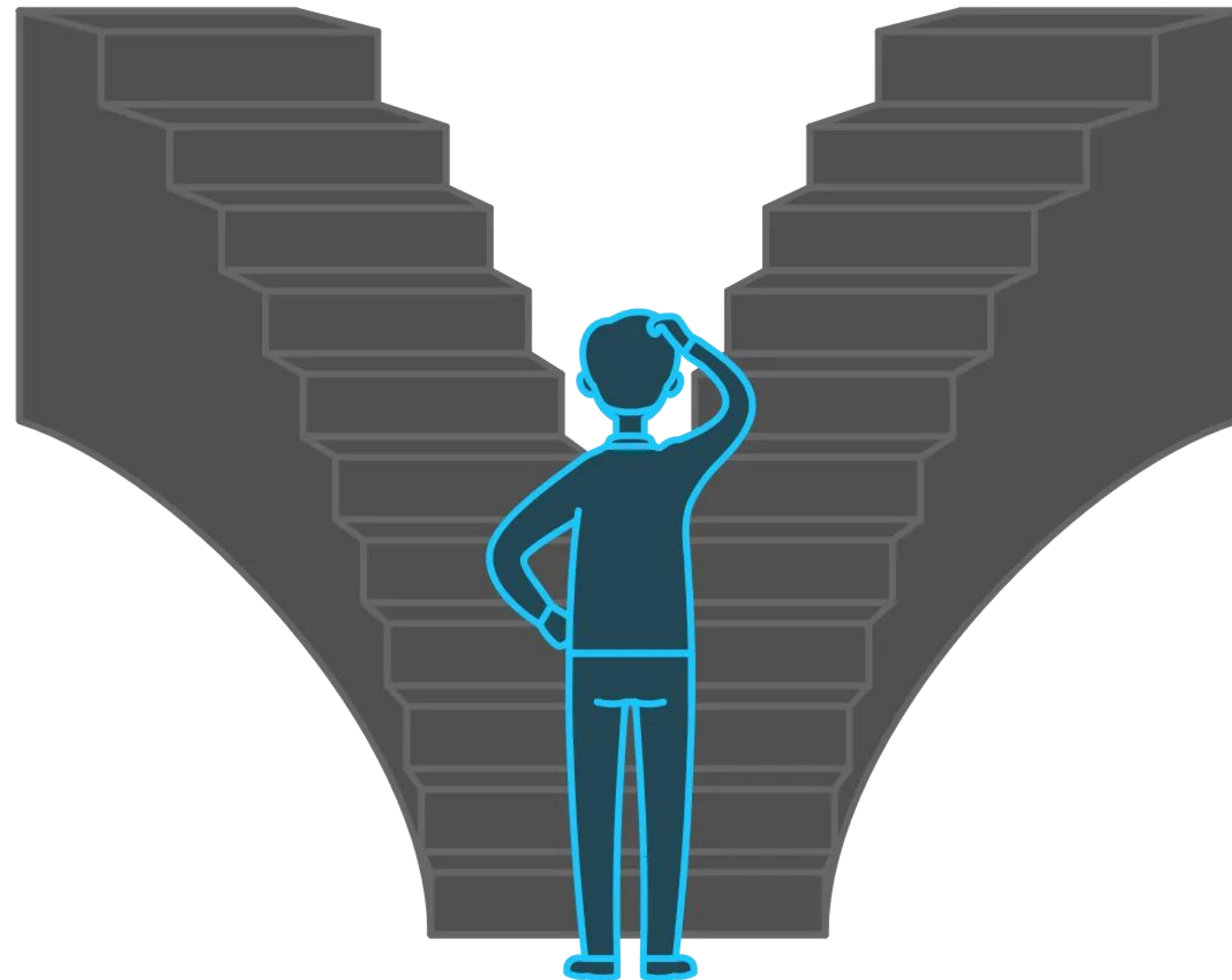


## File validation

- File hash is the strongest.
  - Use Get-FileHash

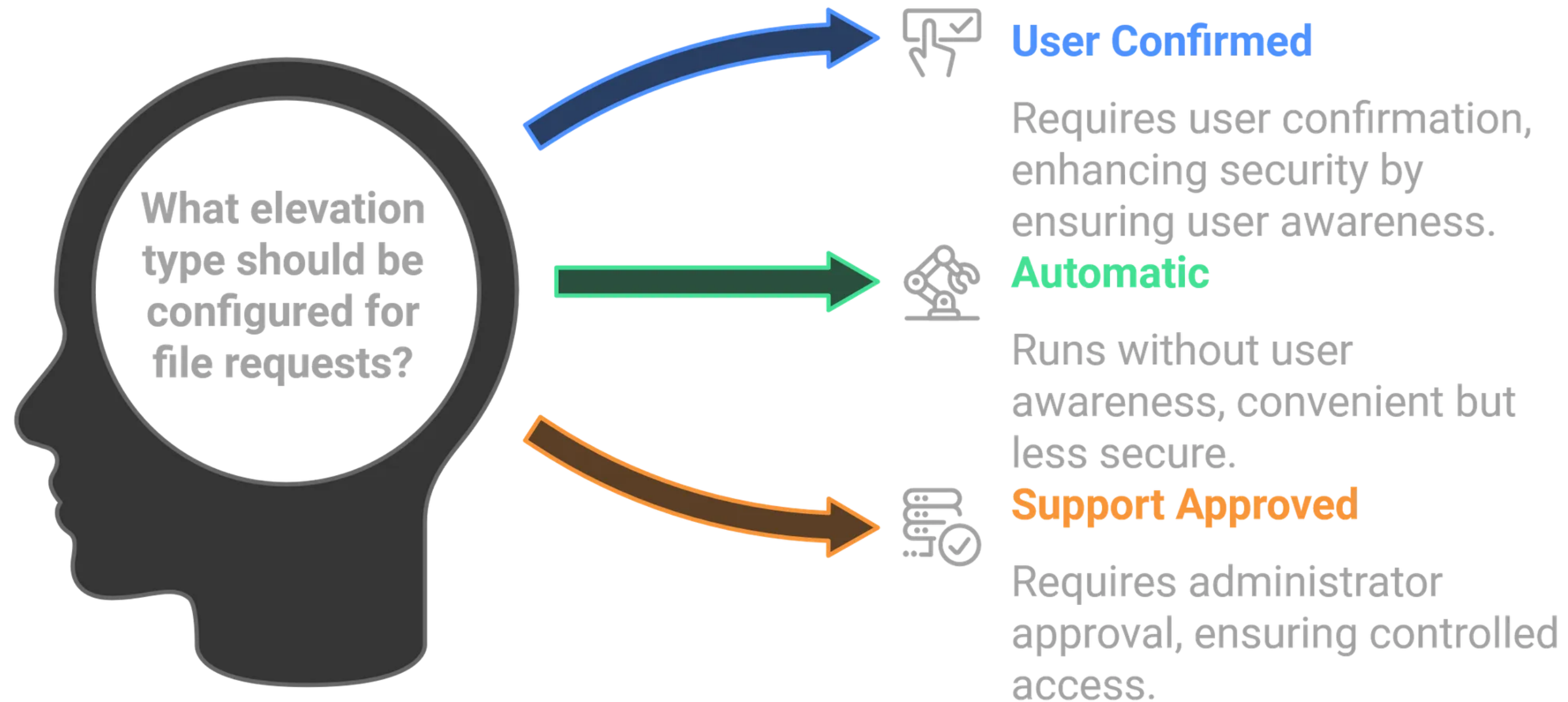
**Use File Hash**

**Use Certificate**



# Elevation Types

- User vs. Automatic vs. Support Approved



# Troubleshooting and Logs

- EpmTools PowerShell Module
- Log Collection
  - C:\Program Files\Microsoft EPM AgentLogs

## Install the EpmTools PowerShell module

The EPM Tools PowerShell module is available from any device that has received EPM policy. To import the EpmTools PowerShell module:

PowerShell

Copy

```
Import-Module 'C:\Program Files\Microsoft EPM Agent\EpmTools\EpmCmdlets.dll'
```

Following are the available cmdlets:

- **Get-Policies:** Retrieves a list of all policies received by the Epm Agent for a given PolicyType (ElevationRules, ClientSettings).
- **Get-DeclaredConfiguration:** Retrieves a list of WinDC documents that identify the policies targeted to the device.
- **Get-DeclaredConfigurationAnalysis:** Retrieves a list of WinDC documents of type MSFTPolicies and checks if the policy is already present in Epm Agent (Processed column).
- **Get-ElevationRules:** Query the EpmAgent lookup functionality and retrieves rules given lookup and target. Lookup is supported for FileName and CertificatePayload.
- **Get-ClientSettings:** Process all existing client settings policies to display the effective client settings used by the EPM Agent.
- **Get-FileAttributes:** Retrieves File Attributes for a .exe file and extracts its Publisher and CA certificates to a set location that can be used to populate Elevation Rule Properties for a particular application.

## Good to know

- Only Supported on Windows 10 and 11
- W365 is supported but AVD is not
- Licencing Requirements: Intune Suite but also available as a Standalone add-on
- Supported File Extensions:
  - Executable files with the .exe or .msi extension
  - PowerShell Scripts with the .ps1 extension

### EPM @ Ignite

- Copilot for Intune integration → Verify that a File is safe to elevate
- macOS Support is coming

