Admin Bouncers

How Endpoint Privilege Management Keeps Your Local Admin Party Exclusive!

Agenda

- Introduction
- What exactly is the problem?
- Who is this Suite guy?
- EPM, wasn’t that Entra Permission Management?
- Fine, what can I work with?
- Pudding time!
- Q&A

Who am I?

- Jens Du Four
  - Linkedin.com/in/jensdufour
  - Jensdufour.be
- Cloud Endpoint TS @ Microsoft
- Traveler
- Musician
- Beekeeper

What is the problem?

- All-powerful access
- Pass-the-hash attacks
- Lateral movement
- Common passwords
- Lack of visibility

Who is this Suite guy?

Intune Plan 1

Included in EMS E3 or Microsoft 365 E3, ME5, F1, F3, and Business Premium plans

- Cross-platform endpoint management
- Endpoint security built in
- Endpoint analytics
- App protection policies
- Shared device management
- Device compliance
- Risk and app based conditional access
- Proactive remediation
- Integrated Microsoft 365 and security

Intune Suite

Add to Plan 1 to utilize these solutions*

- Remote Help
- **Endpoint Privilege Management**
- Advanced Analytics
- Enterprise Application Management
- Cloud PKI
- **All Intune Plan 2 features**

Prerequisite

- Intune Plan 1

Intune Plan 2

Add to Plan 1 to utilize these features

- Tunnel for Mobile App Management
- Mobile firmware update management
- Specialty device management
- Multiple managed accounts (future)

Prerequisite

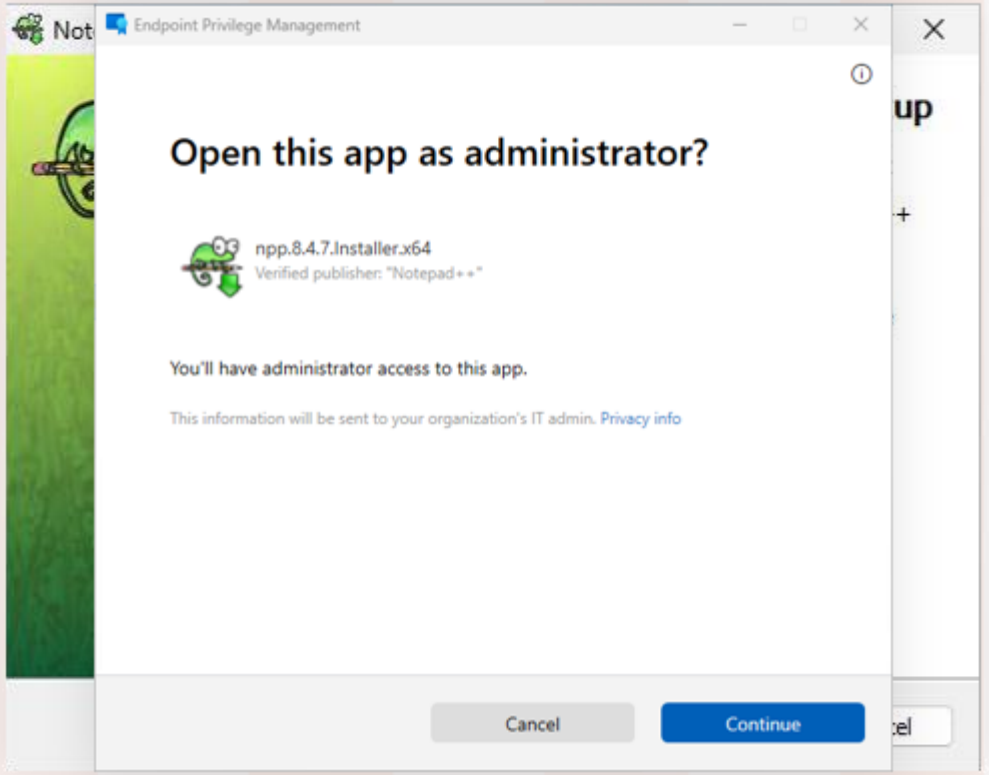
- Intune Plan 1

EPM, wasn't that Entra Permission Management?

- Well, yes, but it's not this!
- Run elevated actions as a standard user
- Windows/MacOS (in the future)
- Enforce least privilege access
  - Zero Trust Framework
- "Lock it down!" VS "Let me do my job!"

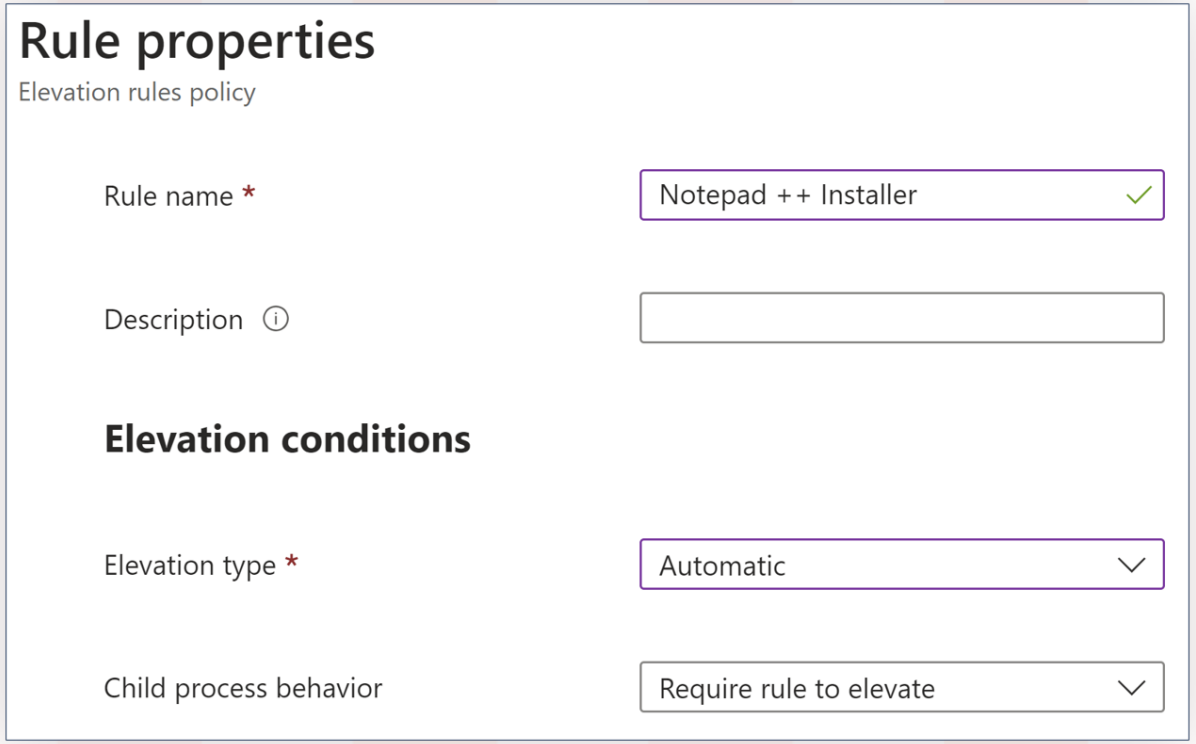
Trigger me, please!

- EPM identifies a process
- User selects “Run elevated”



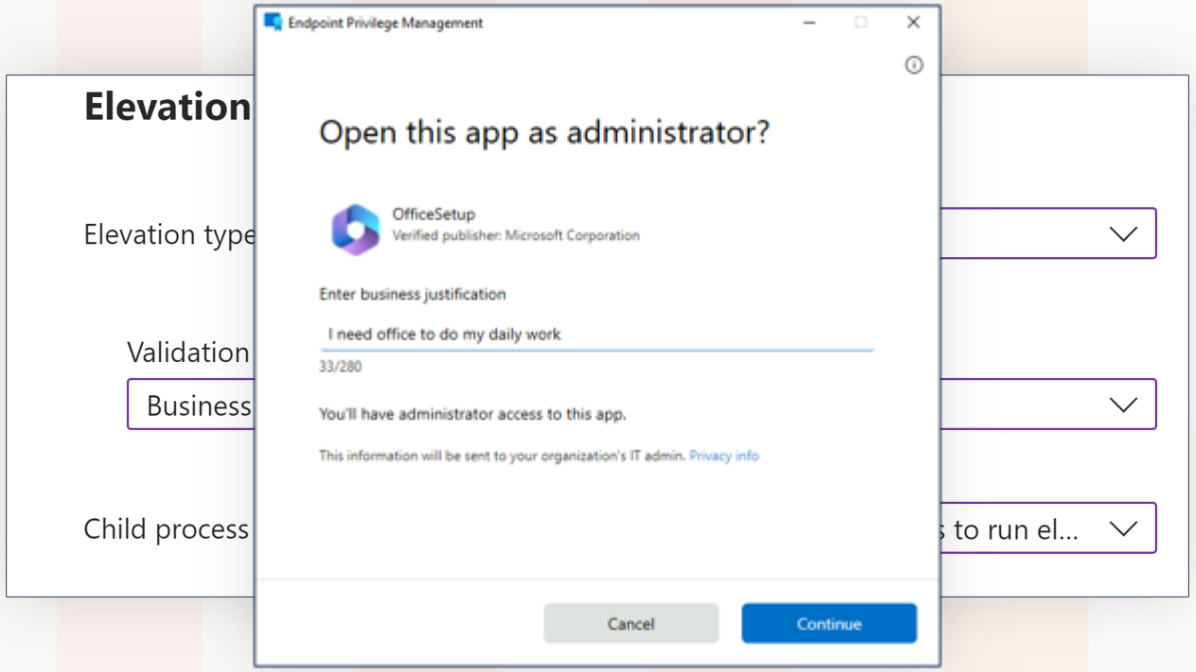
Fine, what can I work with?

- **Automatic elevation**
  - Audit trail
  - Opaque to the end-user
- User-confirmed elevation
- Support-approved elevation



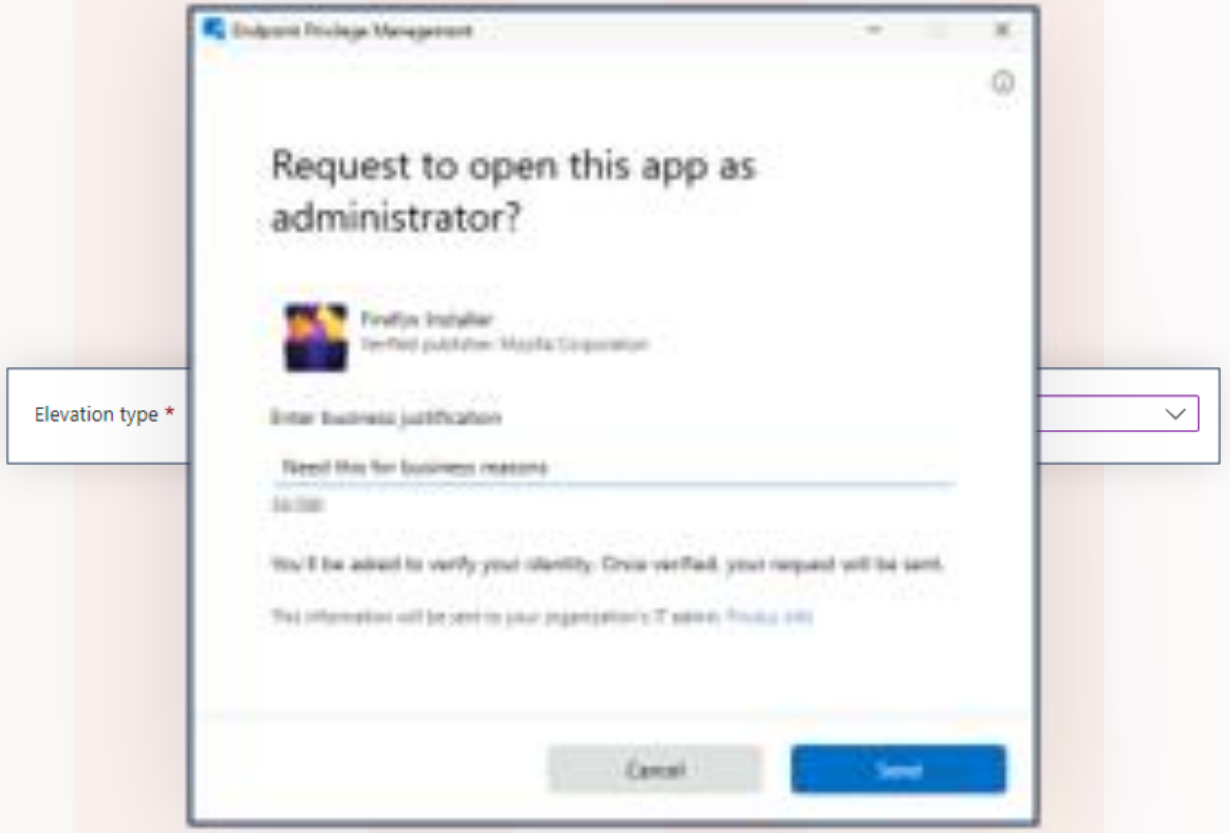
Fine, what can I work with?

- Automatic elevation
- **User-confirmed elevation**
  - Audit trail
  - Additional controls
  - Only a constrained set of binaries can be elevated
    - Bouncers check the guest list!
- Support-approved elevation



Fine, what can I work with?

- Automatic elevation
- User-confirmed elevation
- **Support-approved elevation**
  - Audit trail
  - Bouncers can approve uninvited guests!



Pudding time!

Q&A