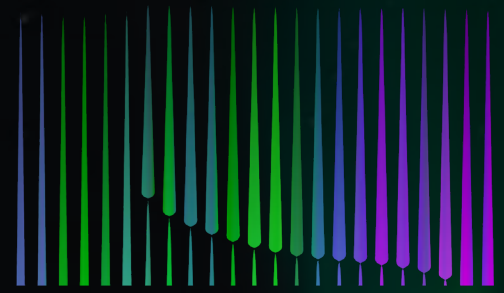


One does not simply implement EPM

What is it, how do we use it, and some valuable learnings from the field!

NORDIC
– VIRTUAL SUMMIT –

Mads Christian Mozart Johansen

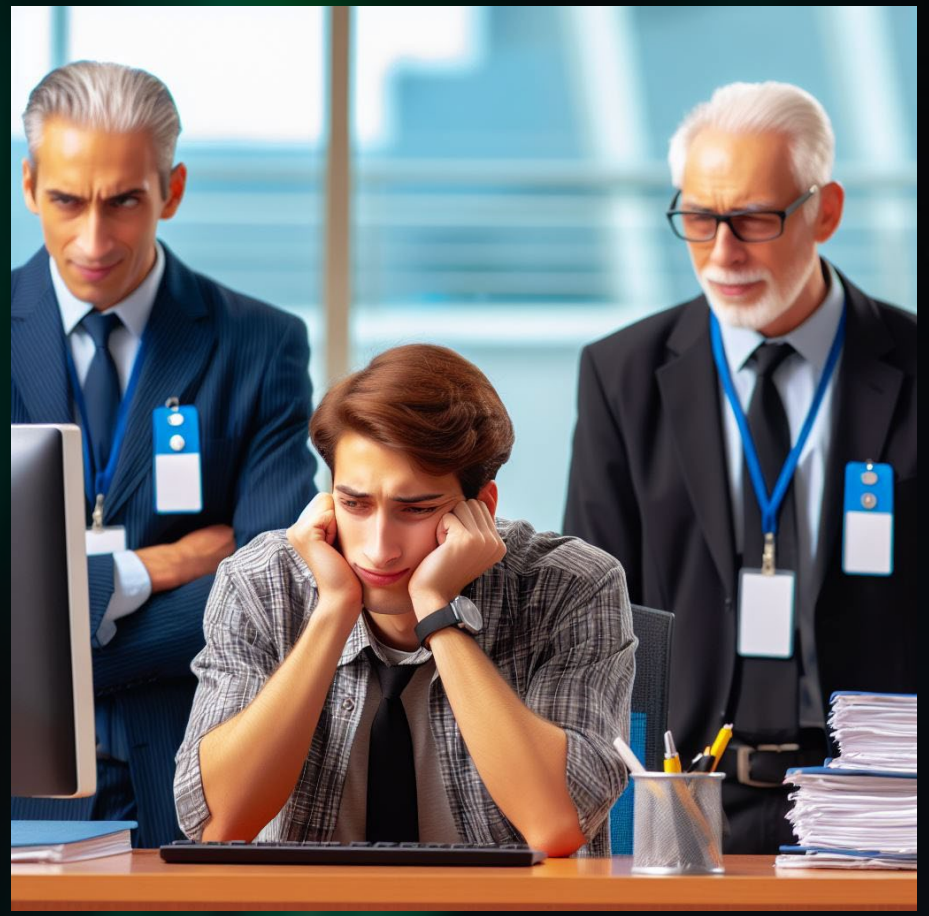
- First-time speaker for NVS
- Endpoint Management for 8 years
- Part of APENTO for the past 3 years, freelance
- Past in HPE, Ireland as an Enterprise break&fix server dude

- Assisting customers going Cloud Native for the past few years
- Modern work specialist
- 11 Microsoft Certifications, Servers and Endpoints
- 13 HPE Certifications (Most of them probably expired….)

What is a PAM and why do we need it?

NORDIC
– VIRTUAL SUMMIT –

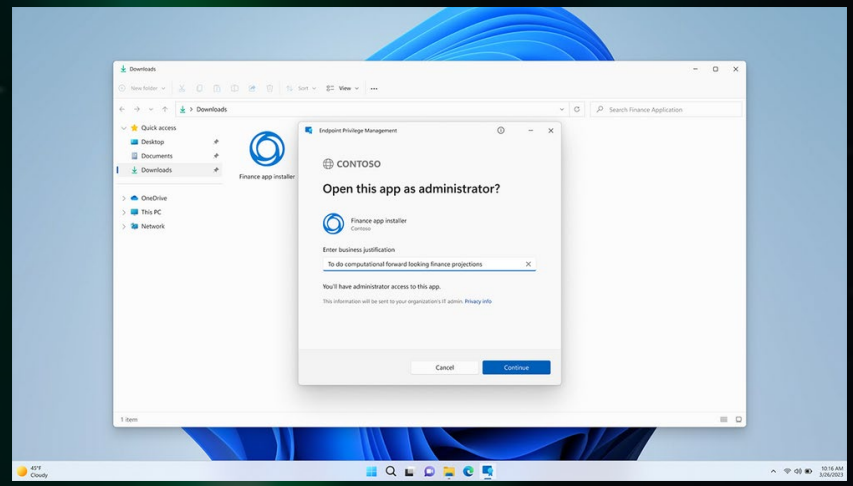
- Bridge the gap between non-privileged and privileged actions
- Empower end-user productivity
  - Apps, settings, printers etc.
- Emphasis on security, auditing and reporting
- Plenty of 3rd party tools already in this space for many years!
- LAPS not a good PAM solution!

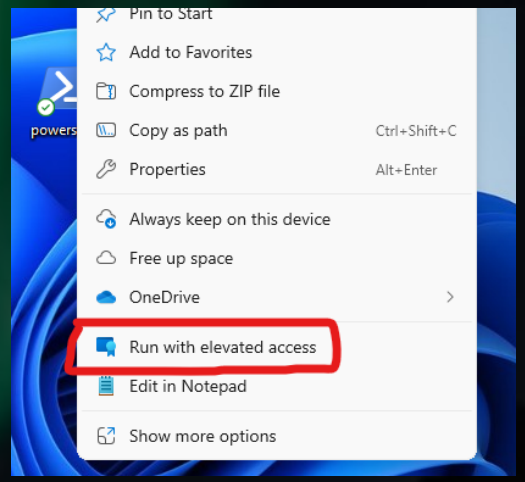


Microsoft Endpoint Privilege Management

NORDIC
— VIRTUAL SUMMIT —

- Fresh interpretation of a PAM
- Included in Microsoft Intune Suite
  - Can also be purchased as an addon
- Security first!
- End-user productivity in a guarded environment
- Approval Flow, Auto-approve and rule-based
- Create rules for each app for the best experience!





How does it all work?

Live demo!

NORDIC
– VIRTUAL SUMMIT –

EPM Summary

NORDIC
– VIRTUAL SUMMIT –

Policies and Rules

- Default elevation response: Deny
- Create a rule for each app
- Use strong detection where possible – Get-FileAttributes!
- If using certificates: Use more than filename!
- Not applicable? Check pre-prereqs!

Challenges

- “Run with elevated access” missing in most places of the Windows OS
- Secure Virtual Account
- Elevate from network shares
- Only possible to elevate .exe files
- No MacOS Support (Yet..)

More questions?

Check the official docs!

Learn about using Endpoint Privilege Management with Microsoft Intune | Microsoft Learn

NORDIC
— VIRTUAL SUMMIT —

Reference Slides

EPM Inner Workings: Summary

- Lives in the “Endpoint Security” section of Intune
- Utilizing new technology to push policies (Dual-enrolled)
- Installs a new shell extension: “Run with elevated access” (msix)
- Secure Virtual account for elevations 👍 👎
- “Run with elevated access button” still missing in most part of the operating system

EPM Policies: Summary

- “Deny all requests” is default
- Use file hash to get strongest assertion to a singular file
- If using certificates: remember to input more than filename for stronger detection!
- In doubt about file metadata: Get-FileAttributes to the rescue!

EPM Reporting: Summary

- Managed vs Unmanaged Elevations
  - Managed: EPM is elevating on behalf of the end-user
  - Unmanaged: “Run as administrator” on the endpoint
- 24 hour delay in reporting