Workplace Ninja User Group Finland

27.9.2024

WP Ninja Summit terveiset

Kimmo Pitkänen/Panu Saukko

Ohjelma

- Mikä on Workplace Ninja Summit
- Secure Foundation Initiative
- Intune uudistukset
- Muita uusia asioita
- Kysymyksiä

Workplace Ninja Summit

Mikä oli Workplace Ninja Summit?

- Iso neljän päivän seminaari Sveitsissä
- Noin 650 osallistujaa
- Viisi yhtäaikaista luentoa samaan aikaan
- Paljon Microsoftin tuoteryhmän väkeä
  - Pomoja ja tuotepäälliköitä
- Tekninen sisältö
- Suomesta puhujina:
  - Sami, Petri, Sandy ja Panu

Workplace Ninja Summit 2024 -tunnelmia

Suomi-Ninjat Sveitsissä

- **Petri Paavola**:
  - "SuperBoost Your IT Admin Skills with AI: Ninja Edition 2024"
  - "Enhance your Windows and Intune troubleshooting skills with (Petri's) community tools - NinjaEdition"

- **Panu Saukko** (Merlijn Van Waeyenberghen kanssa):
  - "Endpoint Analytics and Advanced Analytics"
  - "Let's build our own AI assistant for Intune"

Suomi-Ninjat Sveitsissä

www.wpninjas.fi

- **Sami Laiho:**
  - "Forward to the Past and Back to the Future - Cybercrime in 2023/2024"
  - "Zero Trust - Dope or Nope?"

- **Sandy Zeng:**
  - "Intune Automation Magic" (Maurice Dalyn kanssa)
  - "The Art of Log Collection - Navigating the Many Paths to Log Analytics" (Jan Ketil Skanken kanssa)

Miksi osallistua?

- Tekninen sisältö / luennot
- Viimeisin tieto /uutiset MS –teknologioiden osalta
- Mahdollisuus tavata asiantuntijoita
- Mahdollisuus tutustua ihmisiin vastaavissa rooleissa ympäri maailman, kokemusten vaihto
- Verkosto / uudet ihmiset, kokemusten vaihto

Kuvia

Installation of various software causes slowdowns and reliability issues.
SSD lifespan increases
Decreases the need for reinstallations.
Due to more reliable systems productivity is increased
The attack surface of malware is greatly reduced and helps limit propagation
Because it decreases the amount of money needed in extra security solutions
ADMIN RIGHTS ARE NOT HUMAN RIGHTS

WORKPLACE NINJA SUMMIT
#WPNinjaS
www.wpninjas.eu

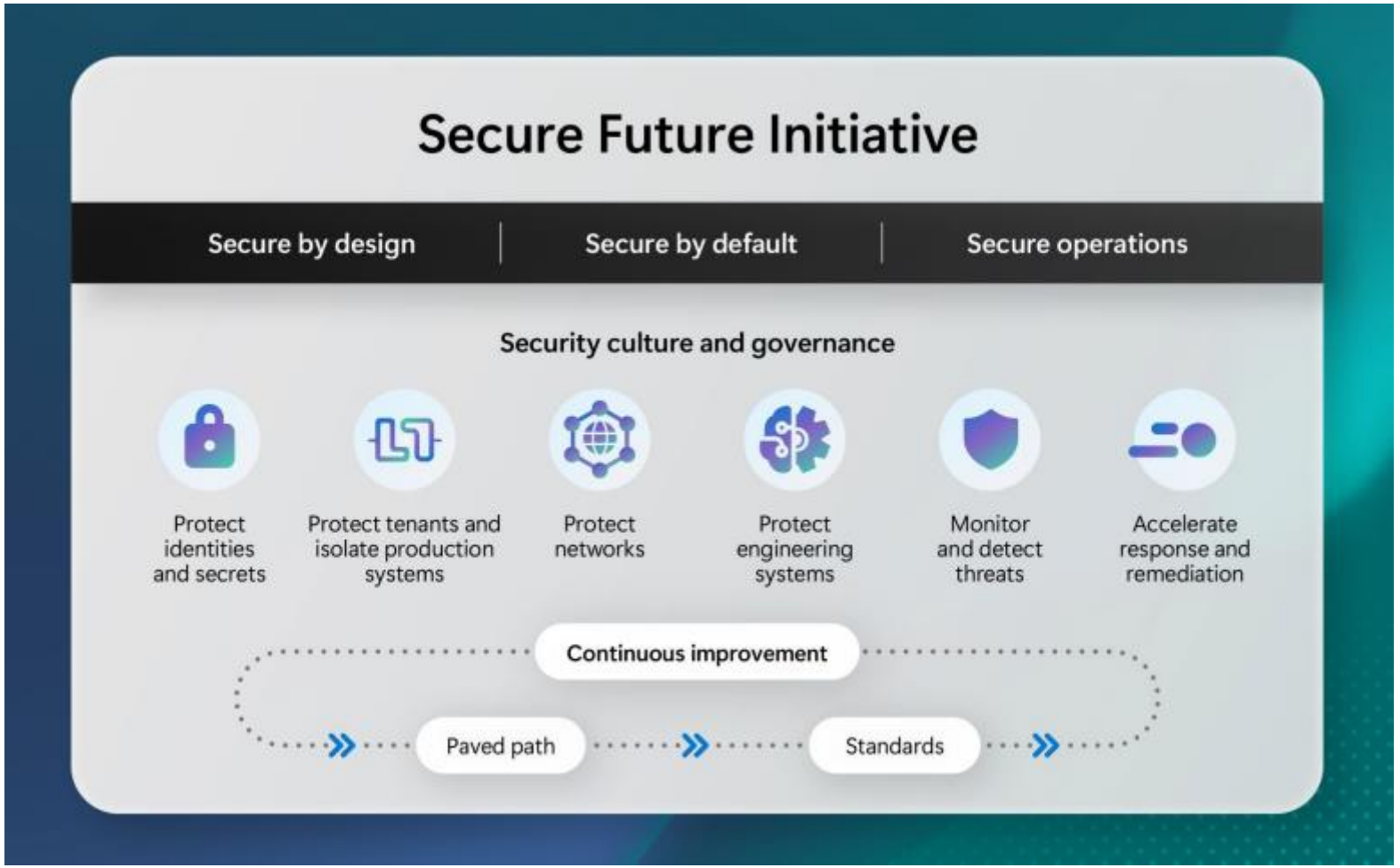
WP Ninja Summit 2025

www.wpninjas.fi

Workplace Ninja Summit 2025 (wpninjas.ch)

Pääaiheita

Secure Future Initiative (SFI)



Alkoi 11/2023. 05/2024 Microsoftin ykkösprioriteetti.

“Starting fiscal year 2025, security became a "Core Priority" in performance reviews for all employees, ensuring it remains central to our planning, execution, and governance”

SFI ja Intune

Vähemmän resursseja koodata
uusia ominaisuuksia
→ Kehitystahti hidastunut

Aikaa käydä läpi vanhempaa koodia
→ Alustan tietoturva
ja suorituskyky parempi

Windows Cloud Native

>50% Windows devices
managed natively
in the cloud

33% YoY in Cloud Native
Intune only devices

96% Co-managed devices
use cloud workloads

¾ co-managed
devices
have cloud enforced
security policies

Tulevaisuuden kehityskohteet

Data

Foundation of modern management in the cloud

Insights

End-to-end context and analysis, reasoning over vast data sets

Action

Execution and remediation to targeted apps, users and devices

AI unlocks everything for better outcomes.

Latenssin vähentäminen

Payload to a device

1. Create a group
2. Assign payload to group
3. Device notified to check-in
4. Entitlements evaluated on check-in
5. Payload applied

Accelerating payload delivery

1. Enrollment time grouping removes dynamic group sync latency
2. Notifications are optimized to enable faster check-ins. Creating more throughput in ASUs
3. Smoothing techniques for peak hours

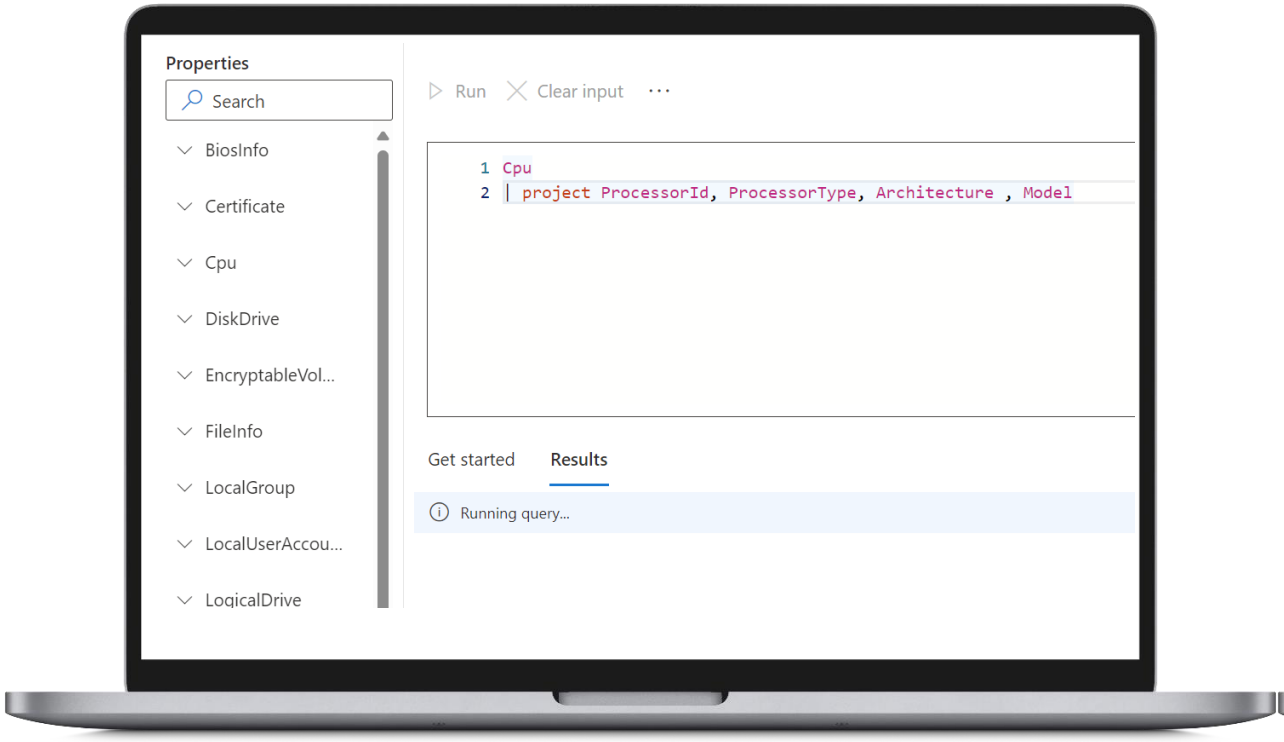
Reducing latency across the full lifecycle

Device query and device inventory

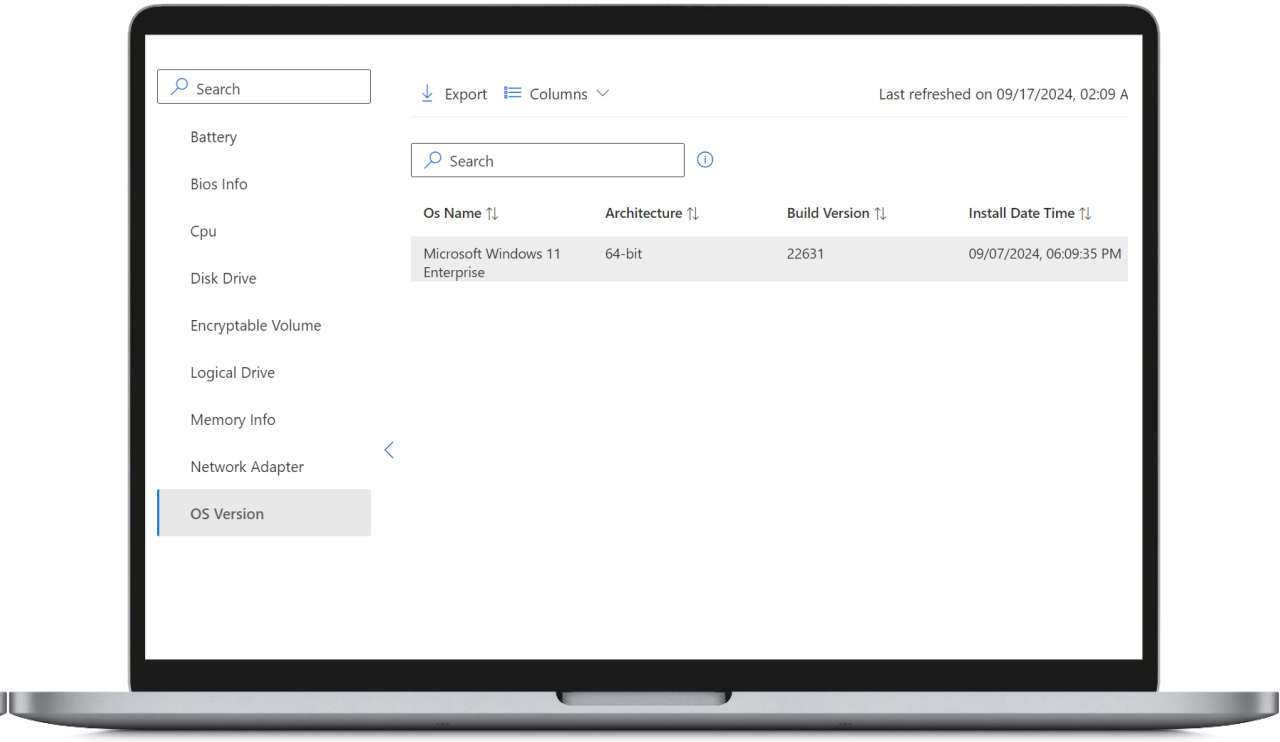
1. Introduction

Device Query AND Device Inventory!

Combining the two powers!



Device Query



Device Inventory

2. Why Device Query

Proactive Problem Solving:

•Troubleshooting features like Device Query allow IT teams to address issues in real-time before they escalate.

•Enables quick identification of problems, reducing downtime and improving user productivity.

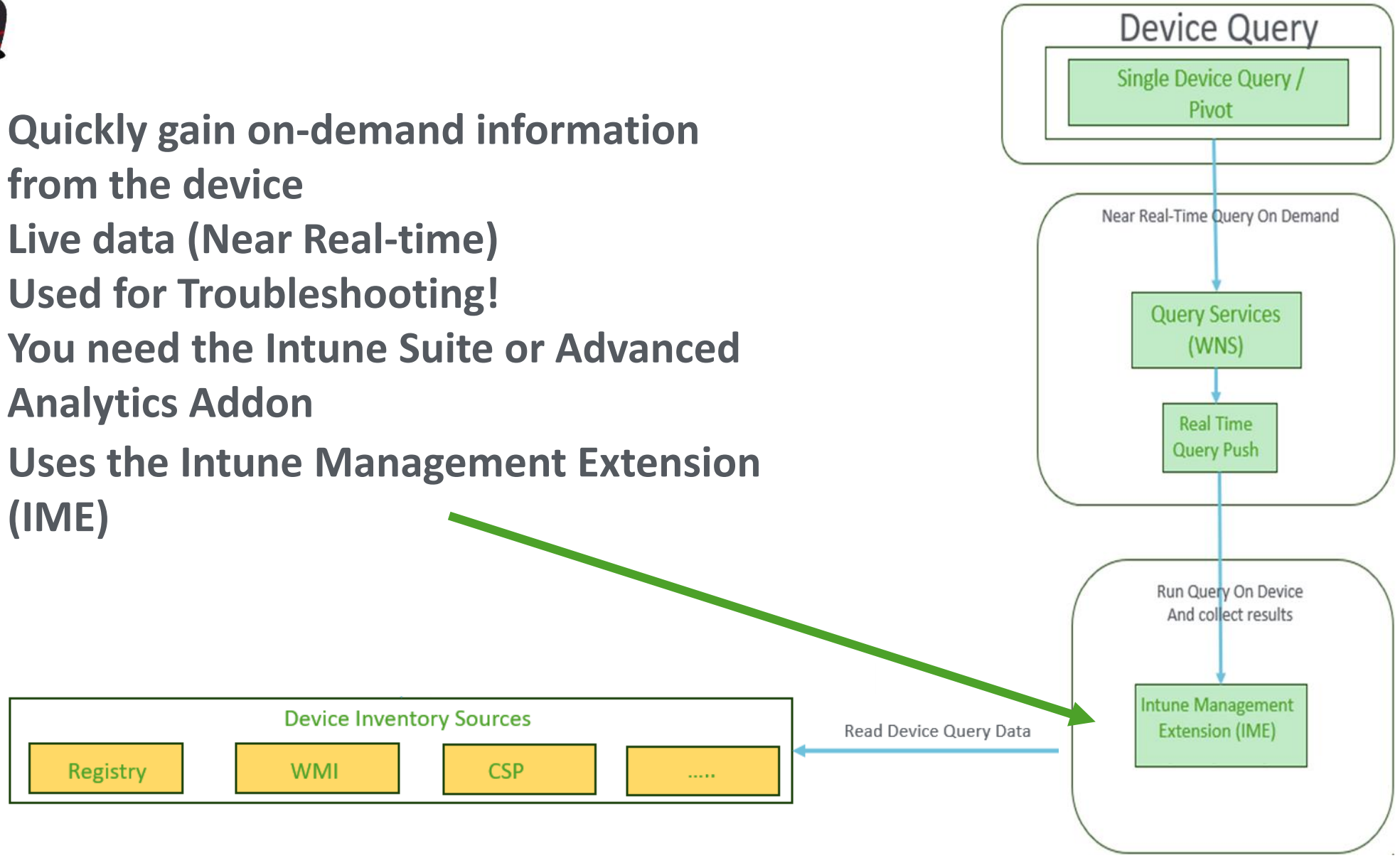
Informed Decision-Making:

•Comprehensive reports offer valuable data insights for strategic planning and resource allocation.

•Helps in making informed decisions about device upgrades, replacements, and maintenance.

Device Query Key Capabilities

- Quickly gain on-demand information from the device
- Live data (Near Real-time)
- Used for Troubleshooting!
- You need the Intune Suite or Advanced Analytics Addon
- Uses the Intune Management Extension (IME)



It’s very simple to use!

www.wpninjas.fi

DESKTOP-V1B154U | Device query ···

Search

Overview

Manage

- Properties

Monitor

- Resource explorer (preview)
- Hardware
- Discovered apps
- Device compliance
- Device configuration
- App configuration
- Local admin password
- Recovery keys
- User experience
- Device diagnostics
- Group membership
- Managed Apps
- Filter evaluation
- Enrollment
- Remediations (preview)
- Device query

Properties

Search

- BiosInfo
- Certificate
- Cpu
- DiskDrive
- EncryptableVolume
- FileInfo
- LocalGroup
- LocalUserAccount
- LogicalDrive
- MemoryInfo
- OsVersion
- Process
- SystemEnclosure
- SystemInfo
- Tpm

Run | Clear input | Cancel

```
1 Certificate
2 | where ValidToDateTime < now()
3 | project ValidToDateTime, SubjectName, CommonName
```

Query Input

Get started | Results

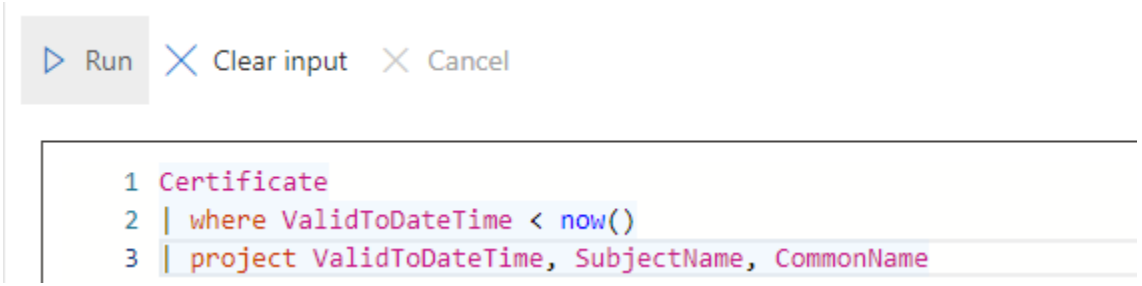
Query Results

Columns

ValidToDateTime	SubjectName	CommonName
2016-10-24T23:59:59Z	OU=www.verisign....	www.verisign.com/CPS Incorp.by Ref. LIABILITY I
2002-12-31T07:00:00Z	CN=Microsoft Win...	Microsoft Windows Hardware Compatibility
2021-05-09T23:28:13Z	CN=Microsoft Roo...	Microsoft Root Certificate Authority
2020-12-31T23:59:59Z	CN=Thawte Timest...	Thawte Timestamping CA
2020-12-31T07:00:00Z	CN=Microsoft Roo...	Microsoft Root Authority

How good is your KQL?

- Device Query uses KQL (Kusto Query Language)
- Kusto Query Language is used in Log Analytics, Sentinel, and now also for Device Query
- Used for exploring the data and discovering patterns
- KQL operators are sequenced by using a pipe (|)
- Use Copilot to create the KQL queries for you!



Demo Time and let's look at some KQL examples!!!

Properties

Search

BiosInfo
Certificate
Cpu
DiskDrive
EncryptableVolume
FileInfo
LocalGroup
LocalUserAccount
LogicalDrive
MemoryInfo
OsVersion
Process
SystemEnclosure
SystemInfo
Tpm
WindowsAppCras...
WindowsDriver
WindowsEvent
WindowsQfe

Run Clear input Cancel

```
1
```

Get started Results

Query the properties of this device on demand, based on device, app, and management properties. Query using the properties provided, or write a custom query using Kusto Query Language (KQL). Learn more about Device query

Prerequisites

To use Device query in your tenant, you must have a license that includes Microsoft Intune Advanced Analytics. To use Device query on a device, the device must be enrolled in Endpoint Analytics. Learn more about Device query prerequisites

Kusto database

Learn about the Kusto query language
Learn more about entities you can query
Learn common operators for Kusto Query Language

2.Reporting and Troubleshooting

Proactive Problem Solving:

•Troubleshooting features like Device Query allow IT teams to address issues in real-time before they escalate.

•Enables quick identification of problems, reducing downtime and improving user productivity.

Informed Decision-Making:

•Comprehensive reports offer valuable data insights for strategic planning and resource allocation.

•Helps in making informed decisions about device upgrades, replacements, and maintenance.

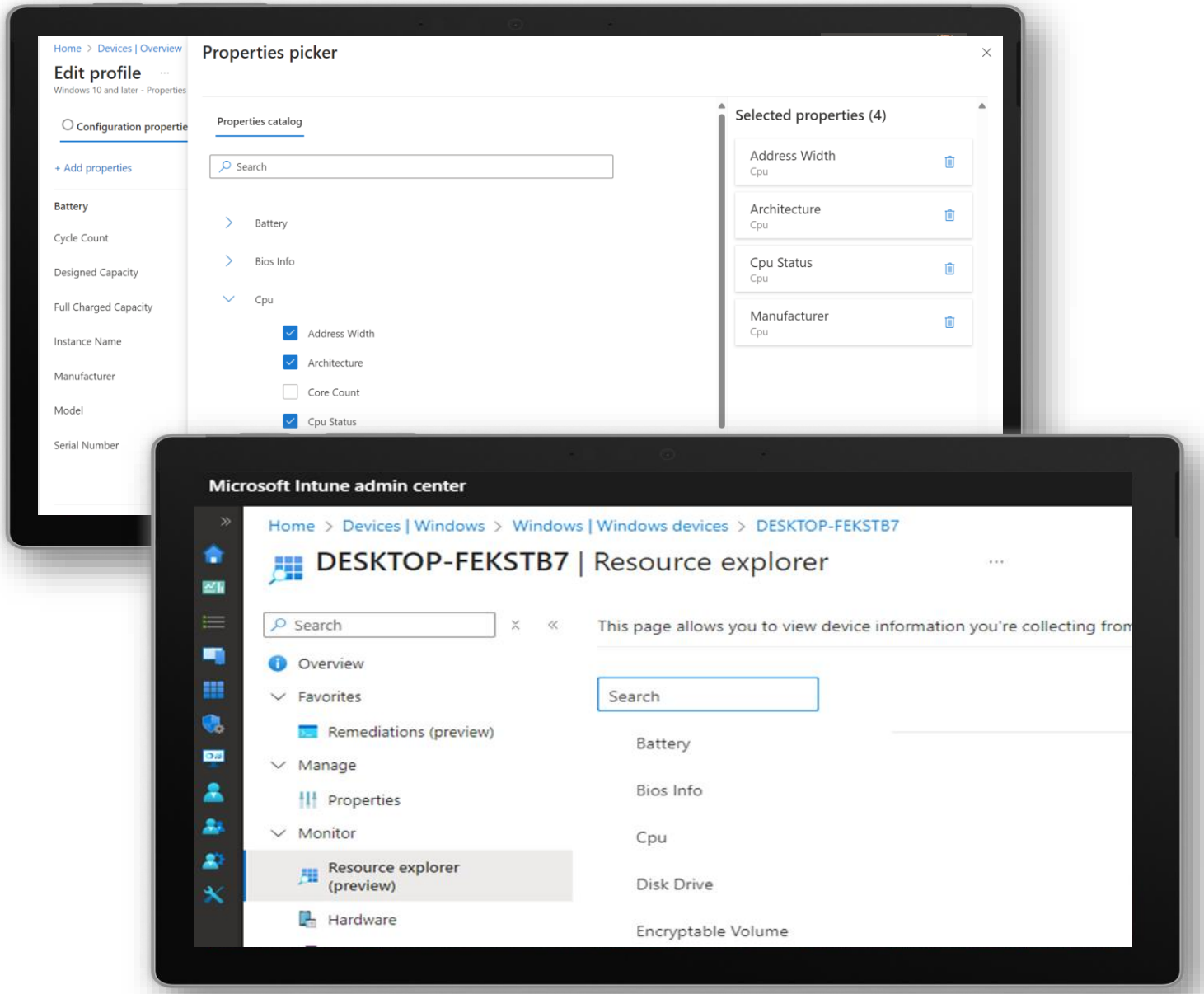
Visibility into Device Health:

•Reporting tools such as Device Inventory provide a clear overview of device health and status across the organization.

•Helps identify patterns or recurring issues that may need broader attention.

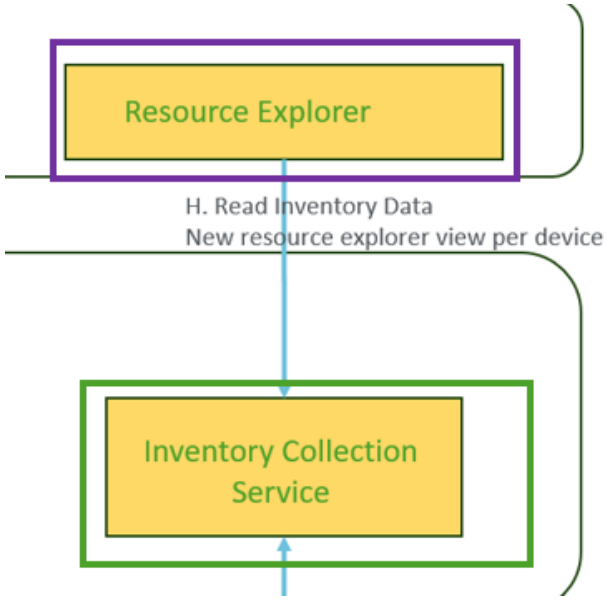
Enhanced inventory: Key capabilities

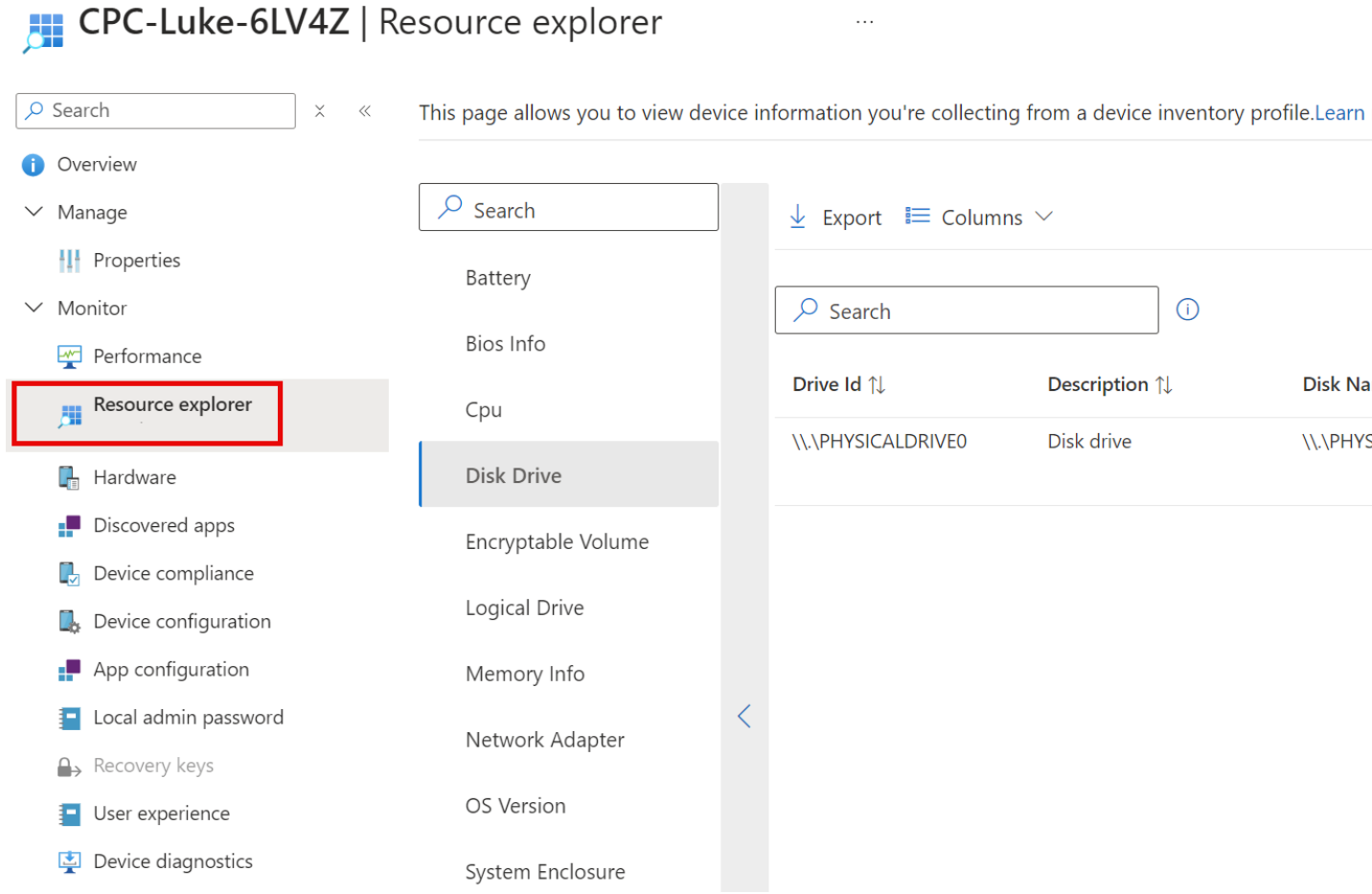
- Intune Core (plan 1) feature!
- Declarative Schema – Enables various sources and across platforms.
- Configure from available entities in Inventory Catalog.
- Expansion of available entities.
- Reporting on configuration.
- Per device view of collected Inventory.
- Visibility into data freshness
- Efficient collection mechanisms to minimize overhead on network and device compute
- Low latency pipeline.



Resource Explorer

- Resource Explorer will start showing the data after policy has been deployed and the initial harvesting
- The initial harvest will happen in a randomized timeframe.
- No data will be shown if you did not add the property in the properties settings policy
- If Microsoft adds more properties, you need to change the policy manually to add them!





It’s Data driven pipeline!

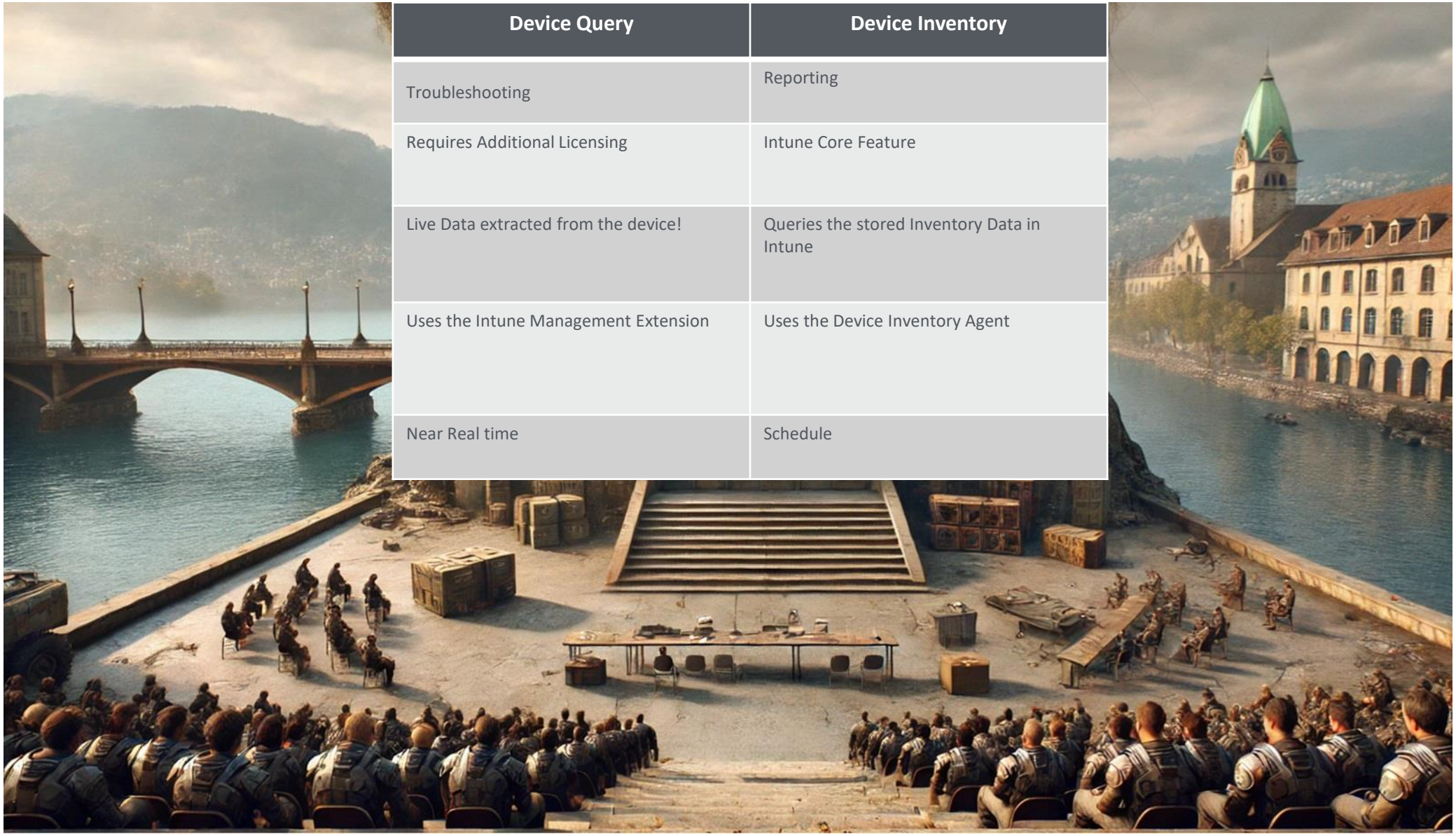
Data driven and declarative

- **Flexible Setup: The system is built to handle different entities without needing extra coding.**
- **Automatic Adaptation: It automatically adjusts to new entities by using a predefined structure.**
- **No Manual Updates: You don’t have to manually update the code for new queries; the system does it for you.**

Device Query |Device Inventory

www.wpninjas.fi

Device Query	Device Inventory
Troubleshooting	Reporting
Requires Additional Licensing	Intune Core Feature
Live Data extracted from the device!	Queries the stored Inventory Data in Intune
Uses the Intune Management Extension	Uses the Device Inventory Agent
Near Real time	Schedule



Conclusion!

- Device Query is for troubleshooting
- Device Query uses the IME and WNS
- Device Inventory is for reporting
- Device Inventory has its own agent
- Device Inventory is going to be a core Intune feature!
- Device Inventory is coming to a town near you!! Pretty soon!

Milloin?

Microsoft Intune: Enhanced device inventory for Windows devices

Rollout Start: October 2024

Gain more inventory information about your Windows devices. Choose which device properties you want to collect from which device and then view that information for your devices.

Feature ID: 408169
Added to roadmap: 8/1/2024
Last modified: 8/1/2024
Product(s): Microsoft Intune
Cloud instance(s): Worldwide (Standard Multi-Tenant)
Platform(s): Desktop
Release phase(s): General Availability

Microsoft 365 Roadmap | Microsoft 365

Muita juttuja

- “ConfigMgr is feature complete”
  - It is supported at least 10 years from the date Microsoft says it will deprecated.
  - Reason: If a product is used in government, there needs to be 10 years of heads up before deprecating anything
  - WSUS is deprecated. Supported with ConfigMgr
- Missä järjestyksessä Intune asentaa sovellukset?
  - Jos laitteeseen on kohdistettu useita sovelluksia
- Copilot, copilot, copilot

Ask The Ninjas!

Kaikki

Kiitos

Workplace Ninja
User Group Finland