NORDIC

— VIRTUAL SUMMIT —

Managing Your Risk of Vulnerabilities with MDE

- Jörgen Nilsson
- Principal Consultant, Onevinn
- X @ccmexec
- MVP / MCT

- Stefan Schörling
- Head of MDR, Onevinn
- X @stefanschorling
- MVP / MCT

Agenda

- Risk of Vulnerabilities
- What to patch
- Working with TVM in MDE
- How to patch
- Reporting

Risk of vulnerabilities

- Initial Access
- Privilege Escalation

What do we need to patch

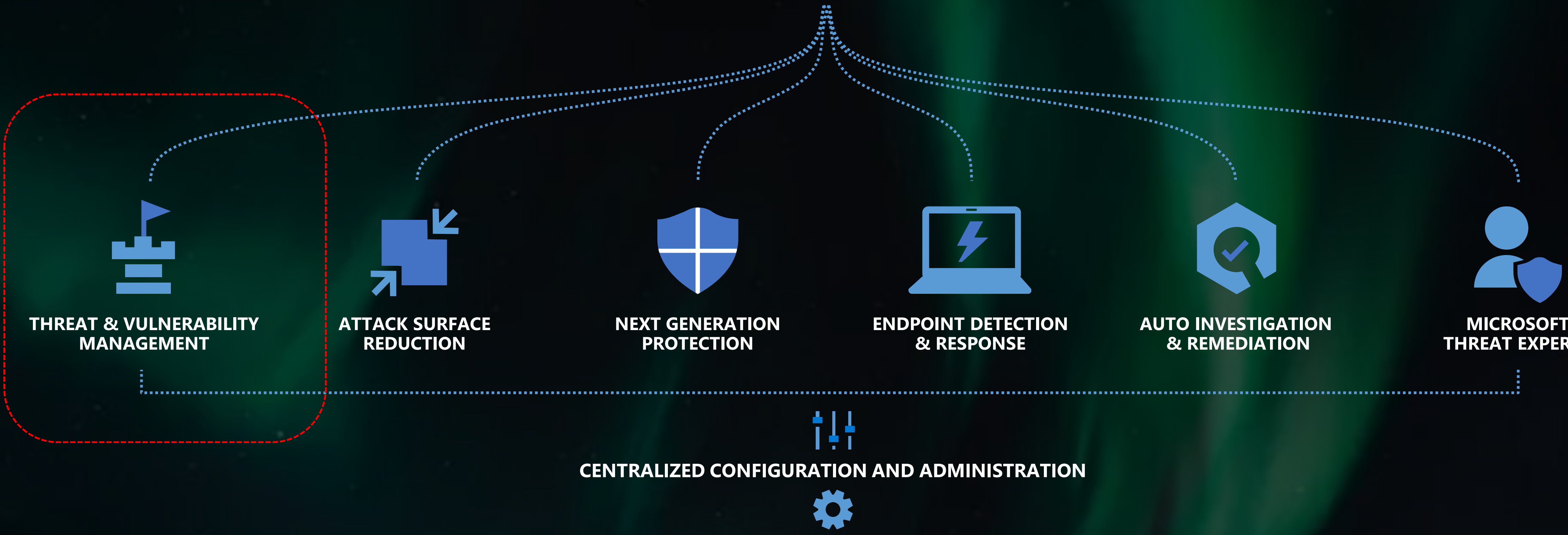
EVERYTHING

What to patch?!

- Operating System
- Microsoft 365 Apps
- Microsoft Teams
- Microsoft Edge
- OneDrive
- Bulit-in apps/store apps
- 3rd Party Applications
- Firmware / Drivers

Microsoft Defender for Endpoint

Threats are no match.



THREAT & VULNERABILITY MANAGEMENT

ATTACK SURFACE REDUCTION

NEXT GENERATION PROTECTION

ENDPOINT DETECTION & RESPONSE

AUTO INVESTIGATION & REMEDIATION

MICROSOFT THREAT EXPERTS

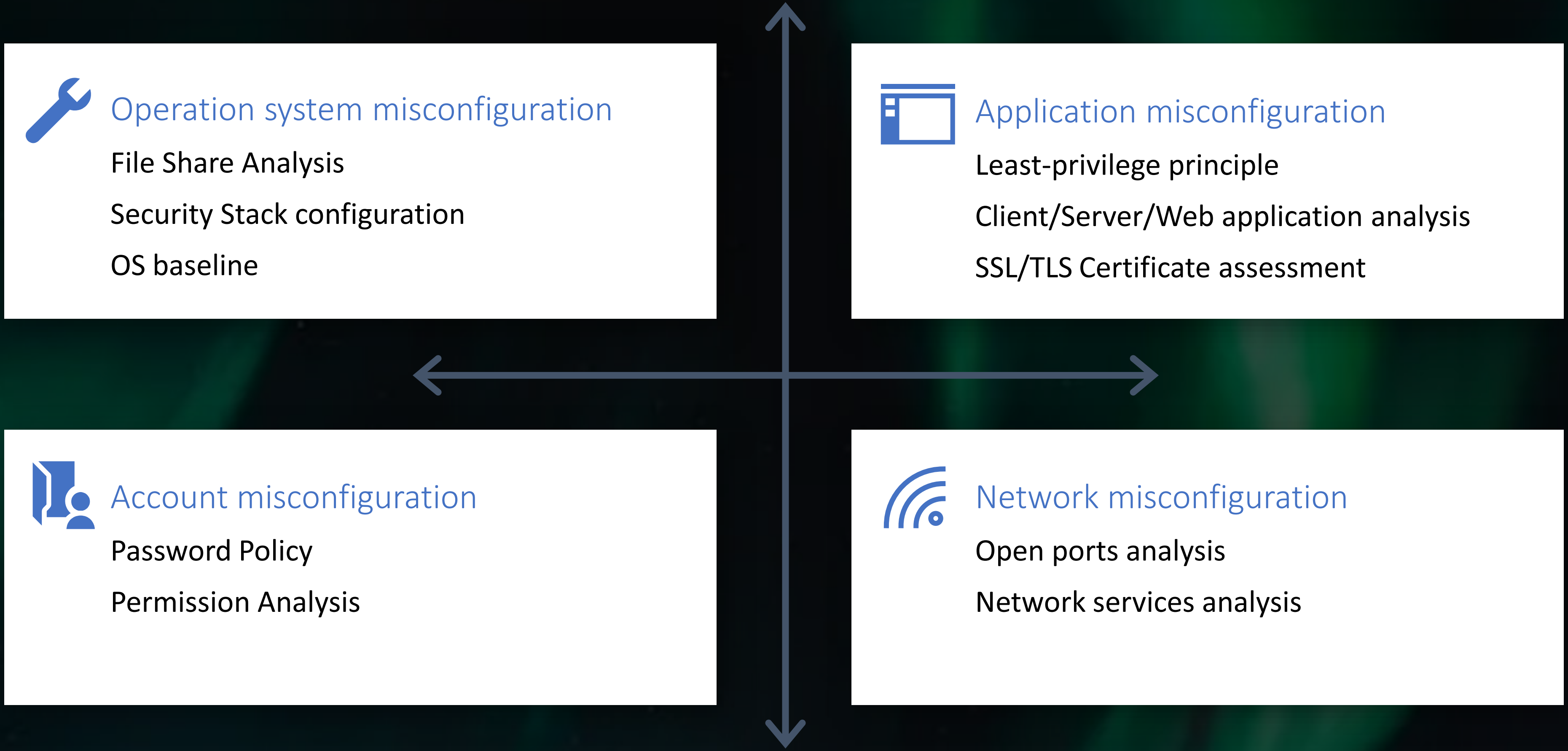
CENTRALIZED CONFIGURATION AND ADMINISTRATION

APIS AND INTEGRATION

1

Continuous Discovery

Broad secure configuration assessment



Operation system misconfiguration

File Share Analysis

Security Stack configuration

OS baseline

Application misconfiguration

Least-privilege principle

Client/Server/Web application analysis

SSL/TLS Certificate assessment

Account misconfiguration

Password Policy

Permission Analysis

Network misconfiguration

Open ports analysis

Network services analysis

1

Continuous Discovery

Extensive vulnerability assessment across the entire stack

NORDIC
– VIRTUAL SUMMIT –

Easiest to exploit

Application extension vulnerabilities

Application-specific vulnerabilities that relate to component within the application.

For example: Grammarly Chrome Extension (CVE-2018-6654)

Application run-time libraries vulnerabilities

Reside in a run-time libraries which is loaded by an application (dependency).

For example: Electron JS framework vulnerability (CVE-2018-1000136)

Application vulnerabilities (1st and 3rd party)

Discovered and exploited on a daily basis.

For example: 7-zip code execution (CVE-2018-10115)

OS kernel vulnerabilities

Becoming more and more popular in recent years due to OS exploit mitigation controls.

For example: Win32 elevation of privilege (CVE-2018-8233)

Hardware vulnerabilities (firmware)

Extremely hard to exploit, but can affect the root trust of the system.

For example: Spectre/Meltdown vulnerabilities (CVE-2017-5715)

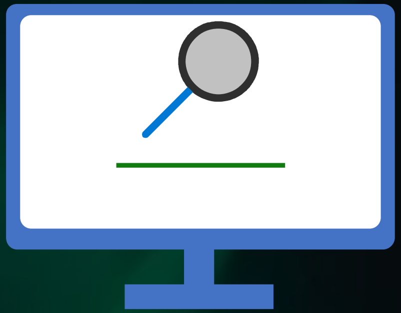
Hardest to discover

2

Threat & Business Prioritization ("TLV")

Helping customers focus on the right things at the right time

NORDIC
— VIRTUAL SUMMIT —



T

Threat Landscape

Vulnerability characteristics (CVSS score, days vulnerable)

Exploit characteristics (public exploit & difficulty, bundle)

EDR security alerts (Active alerts, breach history)

Threat analytics (live campaigns, threat actors)

L

Breach Likelihood

Current security posture

Internet facing

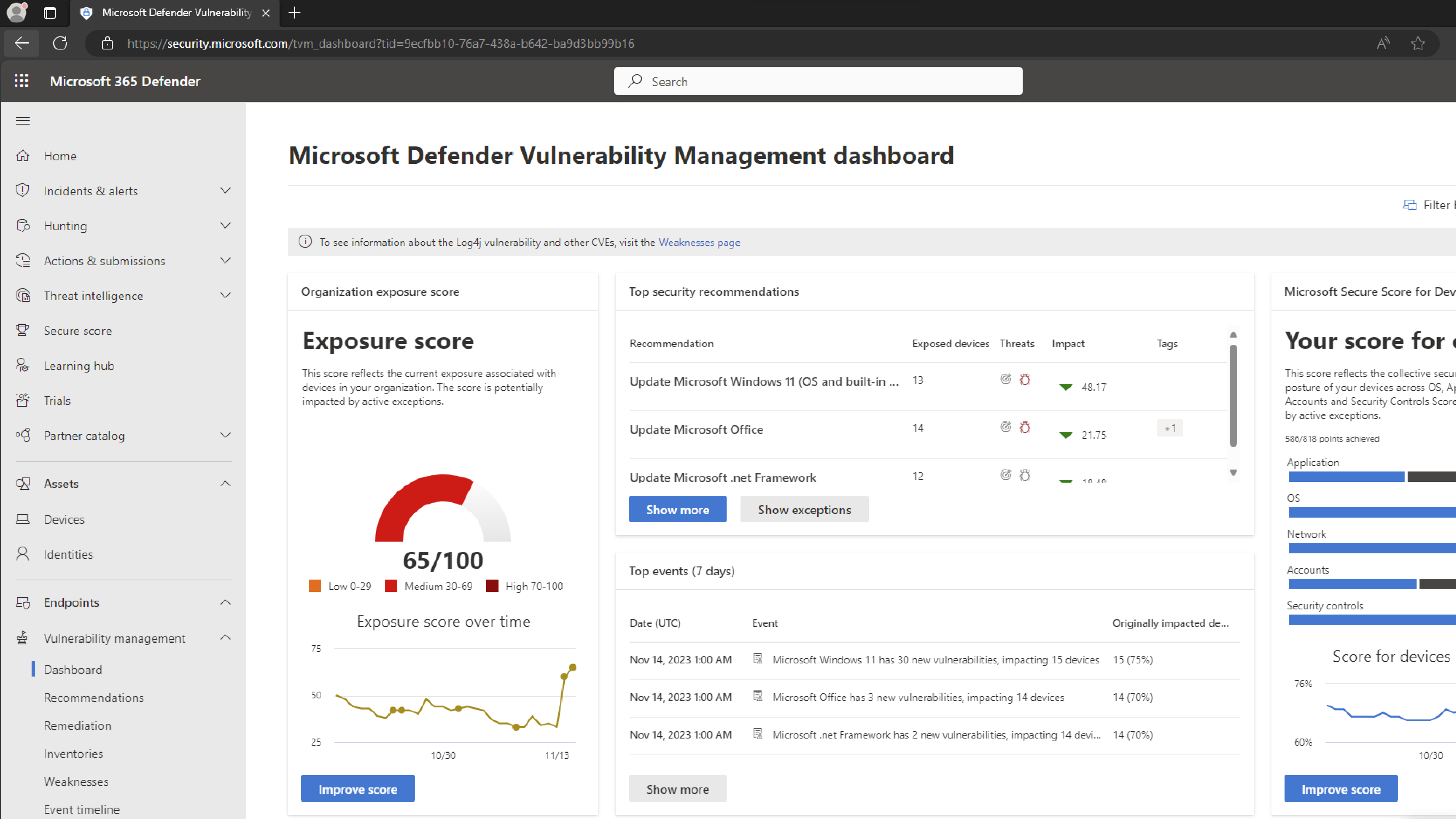
Exploit attempts in the org

V

Business Value

HVA analysis (WIP, HVU, critical process)

Run-time & Dependency analysis



Microsoft Defender Vulnerability Management dashboard

ⓘ To see information about the Log4j vulnerability and other CVEs, visit the Weaknesses page

Organization exposure score

Exposure score

This score reflects the current exposure associated with devices in your organization. The score is potentially impacted by active exceptions.

65/100

🟧 Low 0-29 🟥 Medium 30-69 🟥 High 70-100

Top security recommendations

Recommendation	Exposed devices	Threats	Impact	Tags
Update Microsoft Windows 11 (OS and built-in ...	13		▼ 48.17	
Update Microsoft Office	14		▼ 21.75	+1
Update Microsoft .net Framework	12			

Top events (7 days)

Date (UTC)	Event	Originally impacted de...
Nov 14, 2023 1:00 AM	Microsoft Windows 11 has 30 new vulnerabilities, impacting 15 devices	15 (75%)
Nov 14, 2023 1:00 AM	Microsoft Office has 3 new vulnerabilities, impacting 14 devices	14 (70%)
Nov 14, 2023 1:00 AM	Microsoft .net Framework has 2 new vulnerabilities, impacting 14 devi...	14 (70%)

Microsoft Secure Score for Dev

Your score for

This score reflects the collective secu posture of your devices across OS, Ap Accounts and Security Controls Score by active exceptions.

586/818 points achieved

How fast do we need to patch?

- Of the 30 common vulnerabilities and exposures (CVEs) analyzed, three were exploited within **hours** of public disclosure and 63% were exploited within 12 weeks of the public disclosure

- Of the 15 remote code execution (RCE) vulnerabilities analyzed by Unit 42, 20% were targeted by ransomware gangs **within hours** of disclosure, and 40% of the vulnerabilities were exploited within 8 weeks of publication

Recommendation:

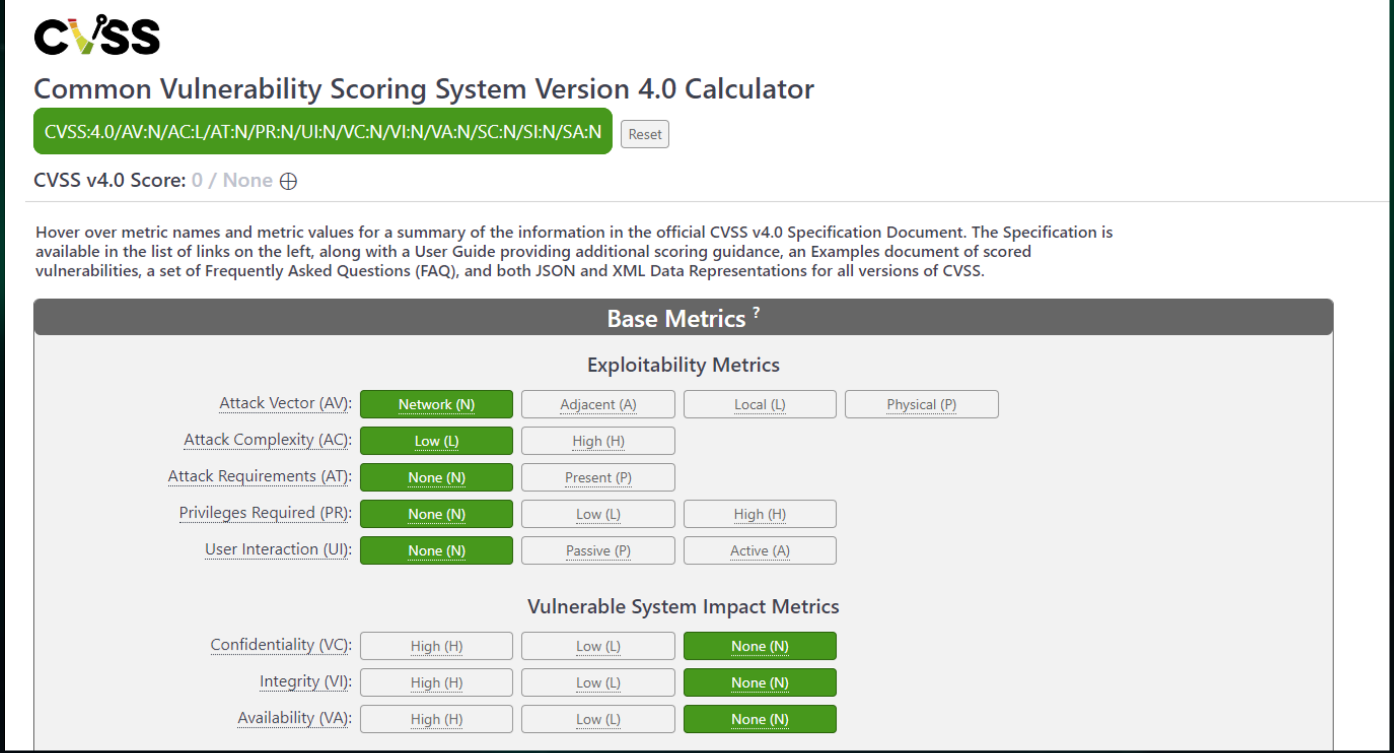
- Have a documented emergency patching process.
- Decide on Patch Tuesday based on CVE rating and if it affects your organization.

Source: Unit 42 Attack Surface Threat Report

CVSS 4.0

- https://www.first.org/cvss/v4.0/user-guide

CVSS
COMMON VULNERABILITY
SCORING SYSTEM



CVSS

Common Vulnerability Scoring System Version 4.0 Calculator

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N Reset

CVSS v4.0 Score: 0 / None ⊕

Hover over metric names and metric values for a summary of the information in the official CVSS v4.0 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, a set of Frequently Asked Questions (FAQ), and both JSON and XML Data Representations for all versions of CVSS.

Base Metrics ?

Exploitability Metrics

Attack Vector (AV): ● Network (N) ○ Adjacent (A) ○ Local (L) ○ Physical (P)
Attack Complexity (AC): ● Low (L) ○ High (H)
Attack Requirements (AT): ● None (N) ○ Present (P)
Privileges Required (PR): ● None (N) ○ Low (L) ○ High (H)
User Interaction (UI): ● None (N) ○ Passive (P) ○ Active (A)

Vulnerable System Impact Metrics

Confidentiality (VC): ○ High (H) ○ Low (L) ● None (N)
Integrity (VI): ○ High (H) ○ Low (L) ● None (N)
Availability (VA): ○ High (H) ○ Low (L) ● None (N)

NVD & CISA

- https://nvd.nist.gov/vuln
- https://www.cisa.gov/known-exploited-vulnerabilities-catalog

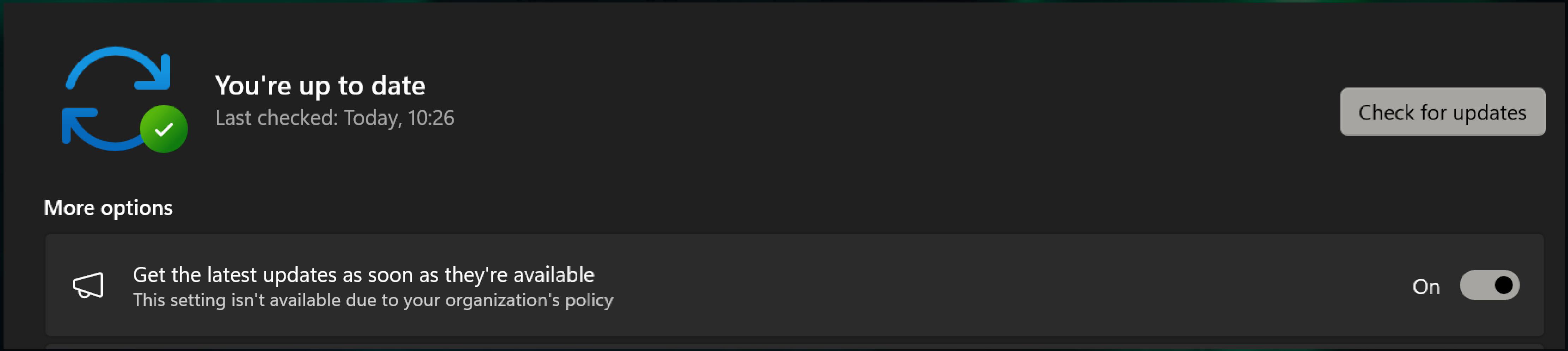
NIST NATIONAL VULNERABILITY DATABASE NVD

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Minimize risk by using the CU-preview release

NORDIC
— VIRTUAL SUMMIT —

- Released last Tuesday every month (except December!!)
- Includes all non-security related updates included in the coming CU
- Used way too little today!
- Deploy to your Pilot ring



You're up to date

Last checked: Today, 10:26

More options

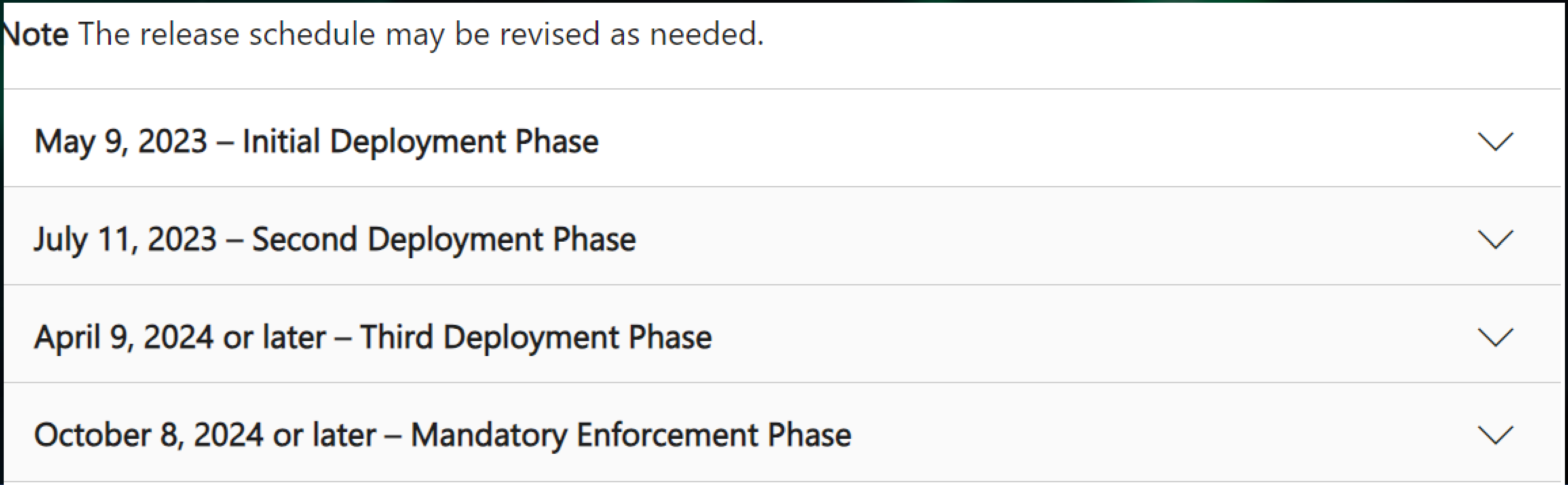
Get the latest updates as soon as they're available

This setting isn't available due to your organization's policy

On

CU which requires manual steps 2023/2024

- CVE-2023-21563 - January 2023 – BitLocker bypass
- CVE-2023-24932 - May 2023 – Secureboot bypass
- CVE-2023-32019 - June 2023 – Kernel vulnerability (enforced in August CU)
- CVE-2024-20666 – January 2024 Bitlocker Bypassing vulnerability



Note The release schedule may be revised as needed.

May 9, 2023 – Initial Deployment Phase

July 11, 2023 – Second Deployment Phase

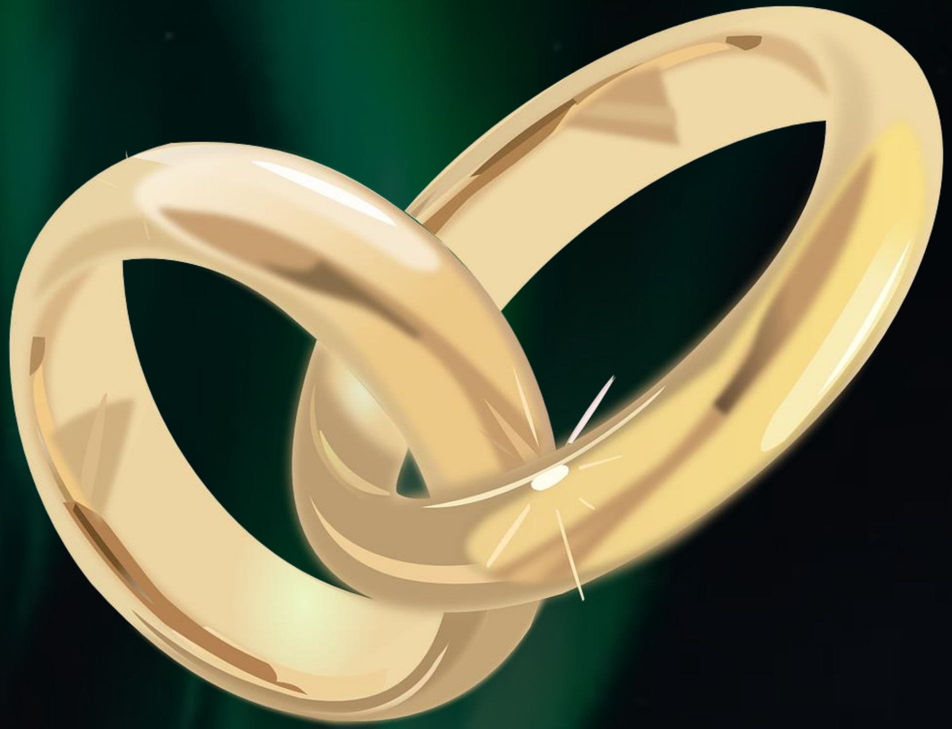
April 9, 2024 or later – Third Deployment Phase

October 8, 2024 or later – Mandatory Enforcement Phase

Example update rings

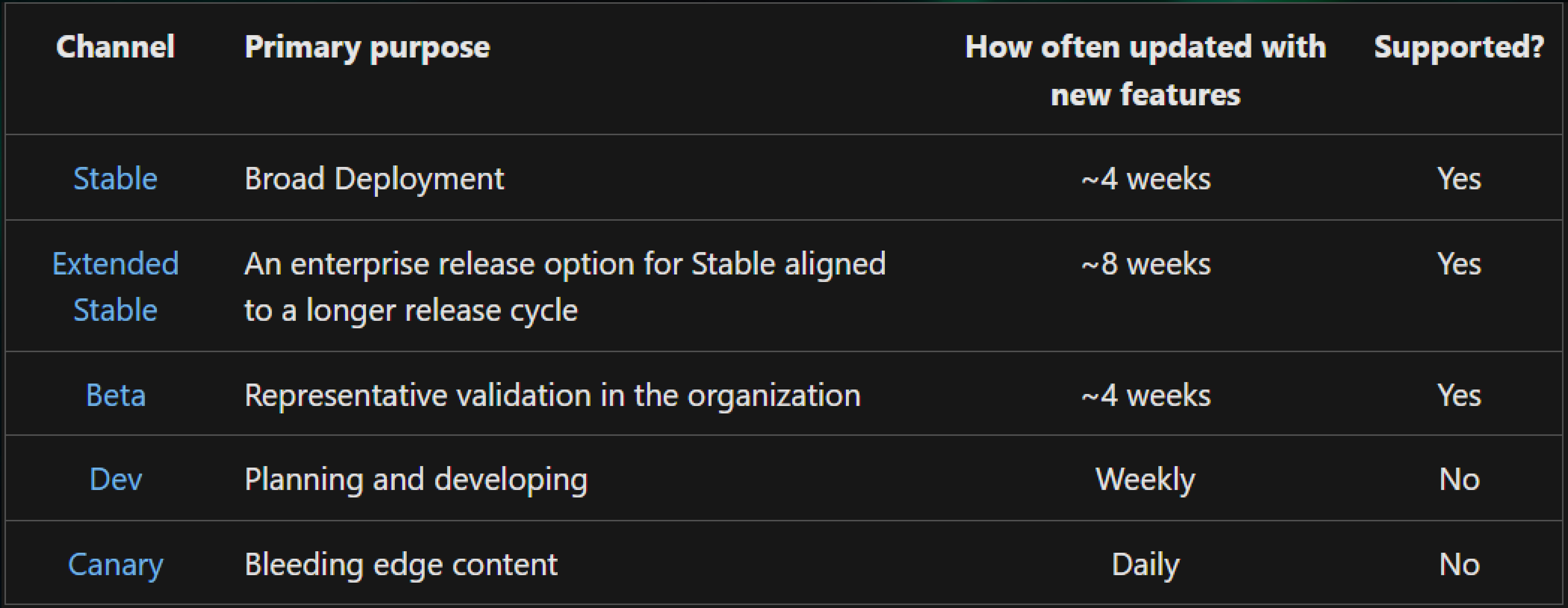
<u>Ring 0 - Test</u>

- Windows Monthly Preview Updates
- Onedrive – Production ring
- Microsoft Edge Beta
- Microsoft Edge
- Microsoft 365 Apps – monthly channel
- Drivers / Firmware – 0 days delay
- Defender
  - Engine update channel
  - Metered connection updates
  - Platform update channel
  - Security Intelligence Updates Channel



Edge

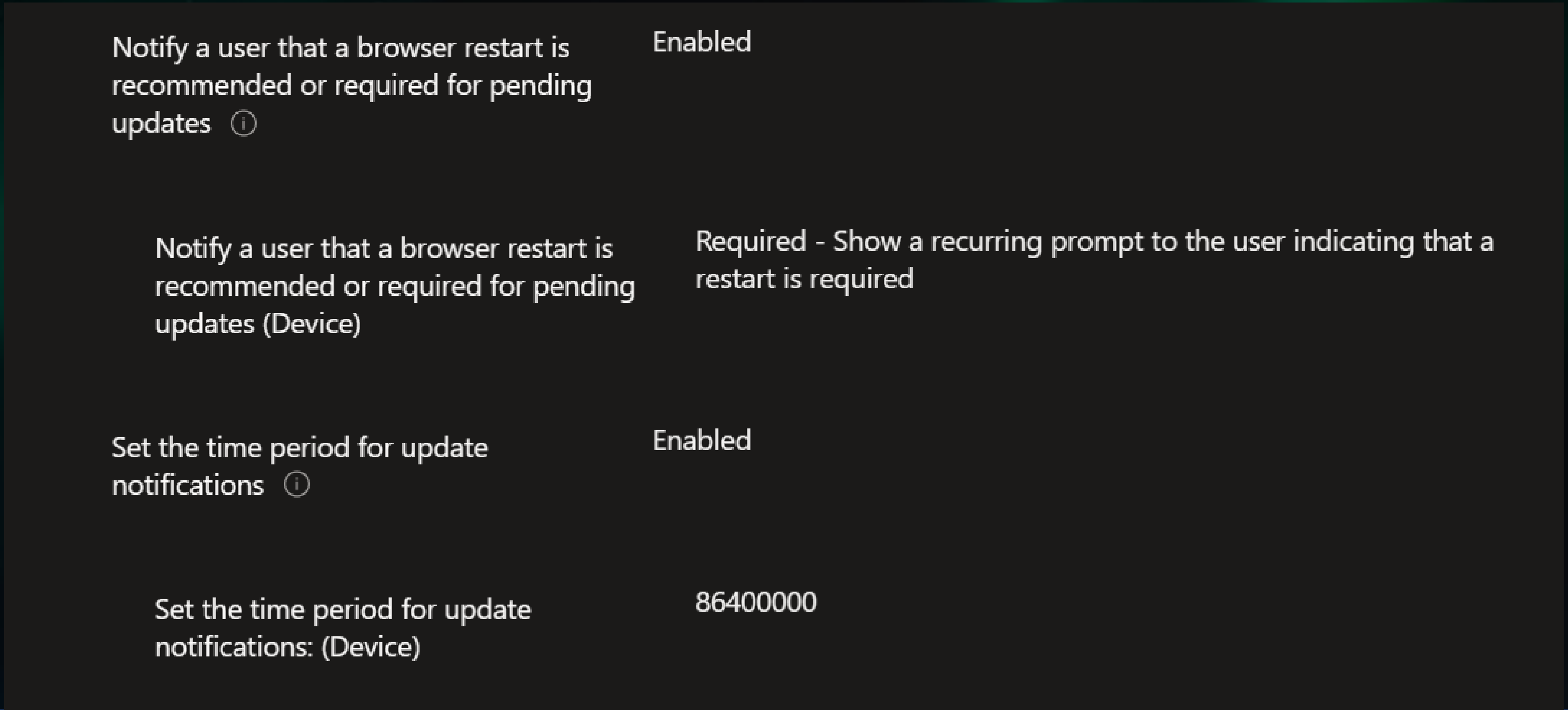
- Beta channel (application developers, app owners)
- Stable channel – 4 weeks
- Extended channel – 8 weeks



Channel	Primary purpose	How often updated with new features	Supported?
Stable	Broad Deployment	~4 weeks	Yes
Extended Stable	An enterprise release option for Stable aligned to a longer release cycle	~8 weeks	Yes
Beta	Representative validation in the organization	~4 weeks	Yes
Dev	Planning and developing	Weekly	No
Canary	Bleeding edge content	Daily	No

Increase Edge update success rate

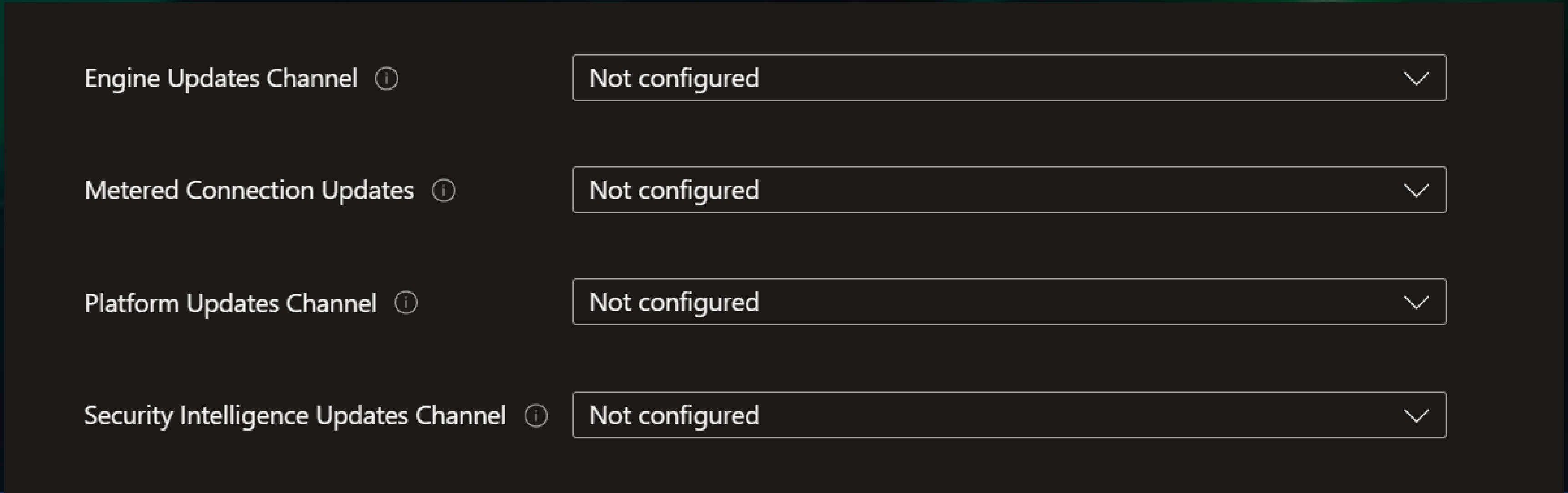
- Edge is updated when it is shutdown
- Prompt the user to close the browser to complete updates.



Notify a user that a browser restart is recommended or required for pending updates ⓘ	Enabled
Notify a user that a browser restart is recommended or required for pending updates (Device)	Required - Show a recurring prompt to the user indicating that a restart is required
Set the time period for update notifications ⓘ	Enabled
Set the time period for update notifications: (Device)	86400000

Defender updates

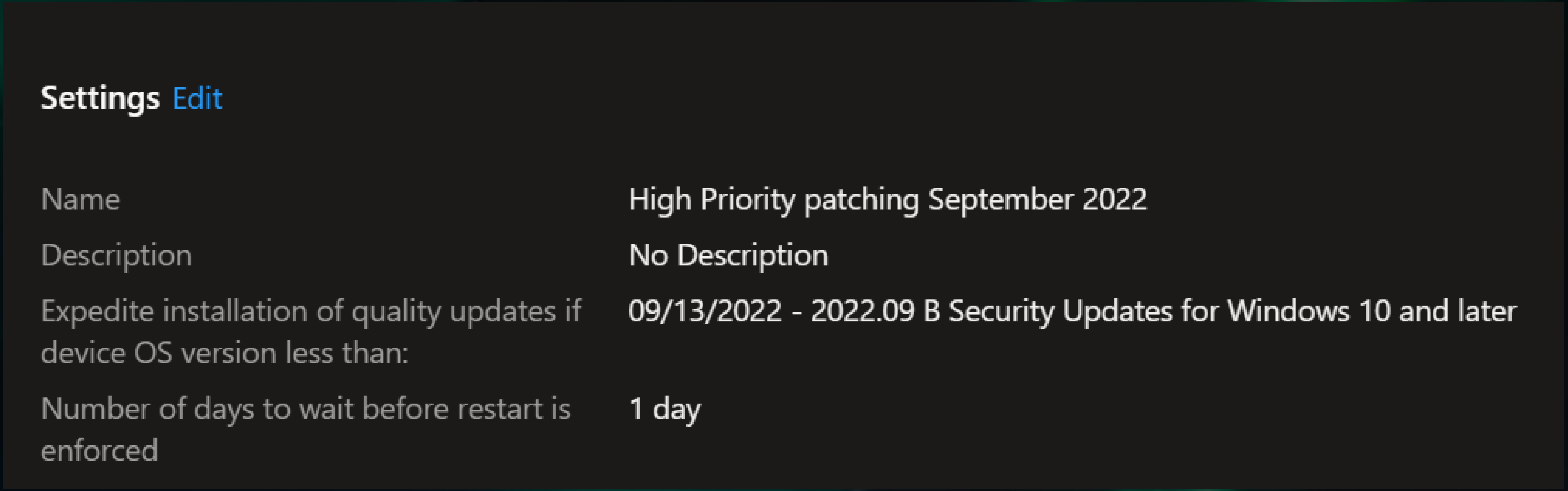
- Engine update channel
- Metered connection updates
- Platform update channel
- Security Intelligence Updates Channel



Engine Updates Channel ⓘ	Not configured
Metered Connection Updates ⓘ	Not configured
Platform Updates Channel ⓘ	Not configured
Security Intelligence Updates Channel ⓘ	Not configured

Expedite updates - Intune

- Overrides Patch rings
- Forces reboot
- Requires KB4023057 - Update Health Tools

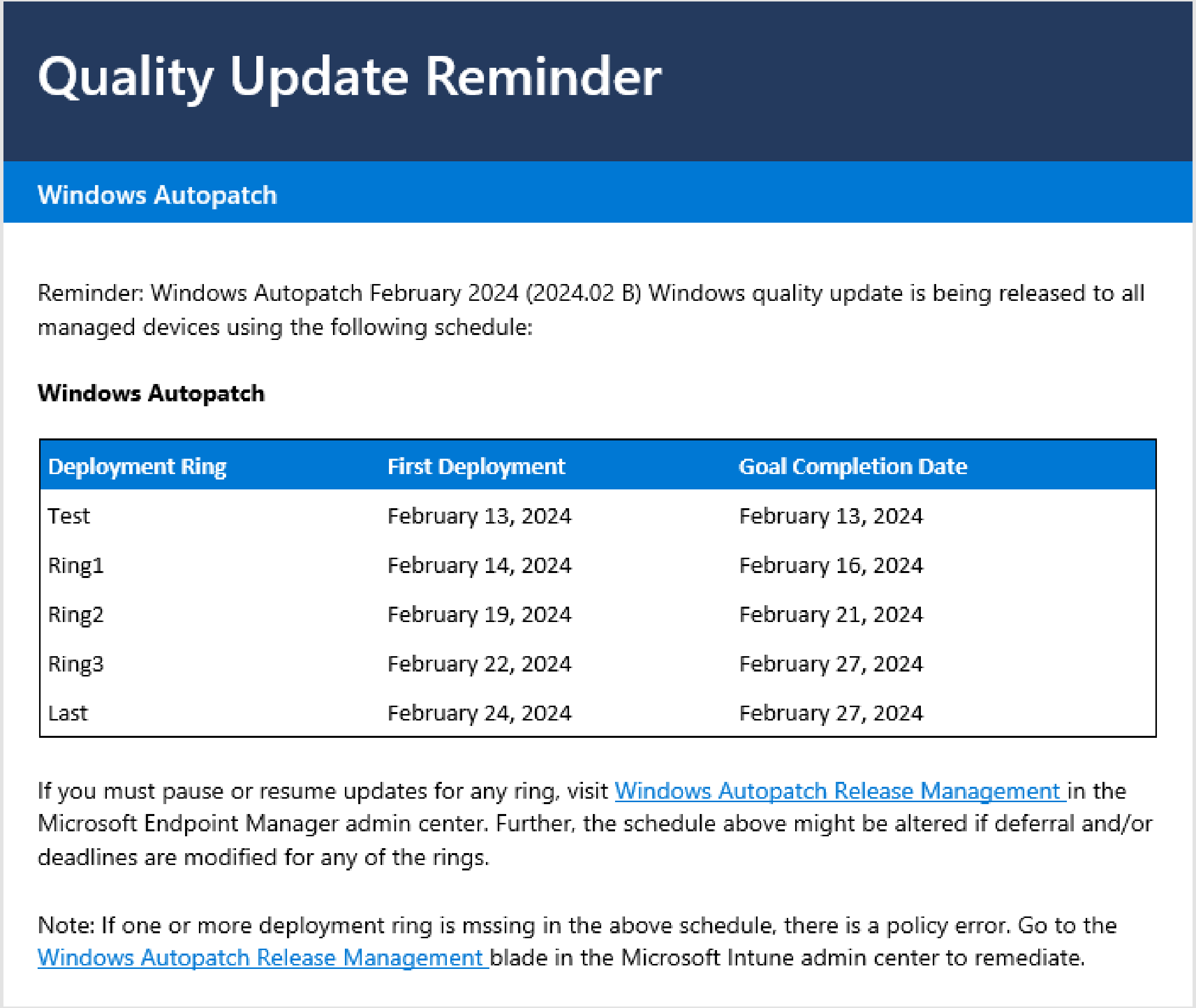


Settings Edit

Name	High Priority patching September 2022
Description	No Description
Expedite installation of quality updates if device OS version less than:	09/13/2022 - 2022.09 B Security Updates for Windows 10 and later
Number of days to wait before restart is enforced	1 day

AutoPatch

- Microsoft manages patching of:
  - Windows 10/11
  - M365 Apps for Enterprise
  - Microsoft Edge
  - Microsoft Teams
- What do we get?
  - Intelligent update rings
  - Deployment schedule
  - Reporting
  - Monitoring
- Included in E3/E5 licensing



Quality Update Reminder

Windows Autopatch

Reminder: Windows Autopatch February 2024 (2024.02 B) Windows quality update is being released to all managed devices using the following schedule:

Windows Autopatch

Deployment Ring	First Deployment	Goal Completion Date
Test	February 13, 2024	February 13, 2024
Ring1	February 14, 2024	February 16, 2024
Ring2	February 19, 2024	February 21, 2024
Ring3	February 22, 2024	February 27, 2024
Last	February 24, 2024	February 27, 2024

If you must pause or resume updates for any ring, visit Windows Autopatch Release Management in the Microsoft Endpoint Manager admin center. Further, the schedule above might be altered if deferral and/or deadlines are modified for any of the rings.

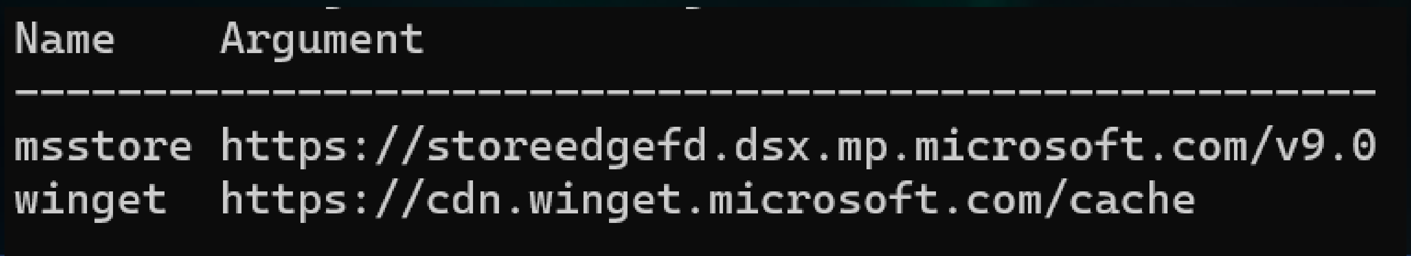
Note: If one or more deployment ring is mssing in the above schedule, there is a policy error. Go to the Windows Autopatch Release Management blade in the Microsoft Intune admin center to remediate.

https://techcommunity.microsoft.com/t5/windows-it-pro-blog/what-s-new-in-windows-autopatch-february-2024/ba-p/4056151

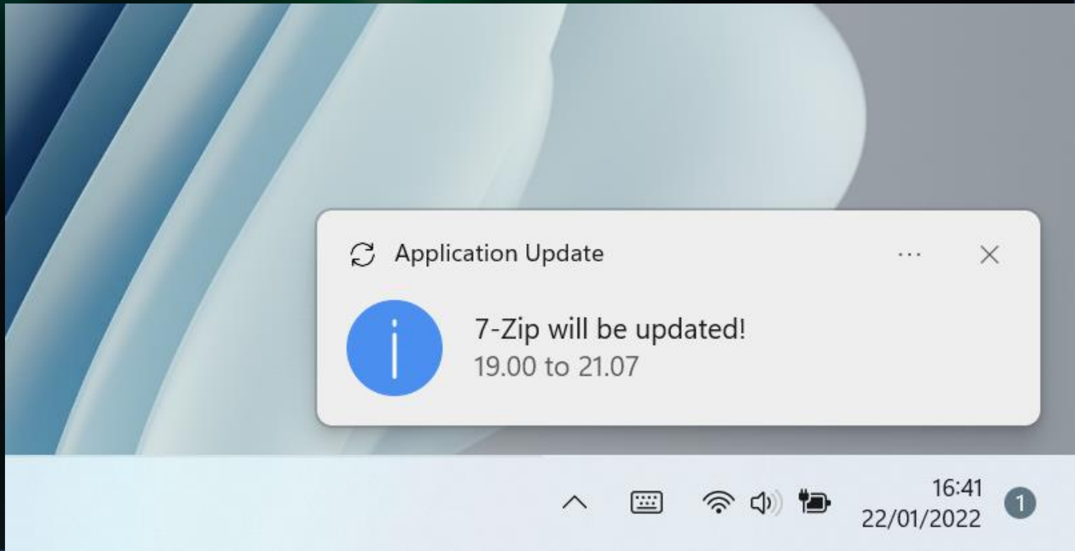
3rd party patching Winget

- Default two repositories
  - MS Store
  - WinGet community repo
- Free
- Great community scripts to manage autoupdate - https://github.com/Romanitho/Winget-AutoUpdate/blob/main/README.md

Challenge: NO SLA



```
Name     Argument
-------------------------------------------------------
msstore https://storeedgefd.dsx.mp.microsoft.com/v9.0
winget  https://cdn.winget.microsoft.com/cache
```



Application Update

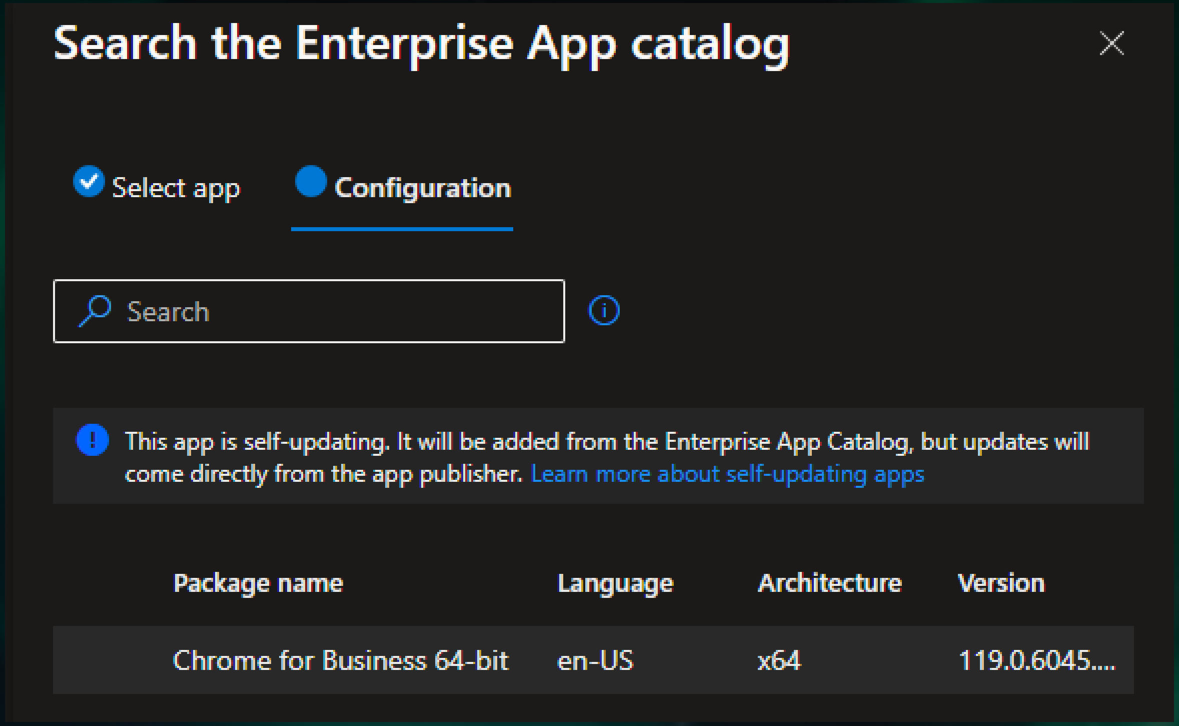
7-Zip will be updated!
19.00 to 21.07

3rd party patching products

- Beneficial if they integrate with Intune/ConfigMgr because of Application Control for Business Trusted Installer support
- Patching unmanaged applications = works great!
- Patching managed applications make sure to adjust the detection method in Intune/Configuration Manager!

Intune Suite – Enterprise App Catalog

- Available as stand-alone license or as part of the Intune Suite
- Integrated in Intune
- 101 applications / versions (today)



Search the Enterprise App catalog

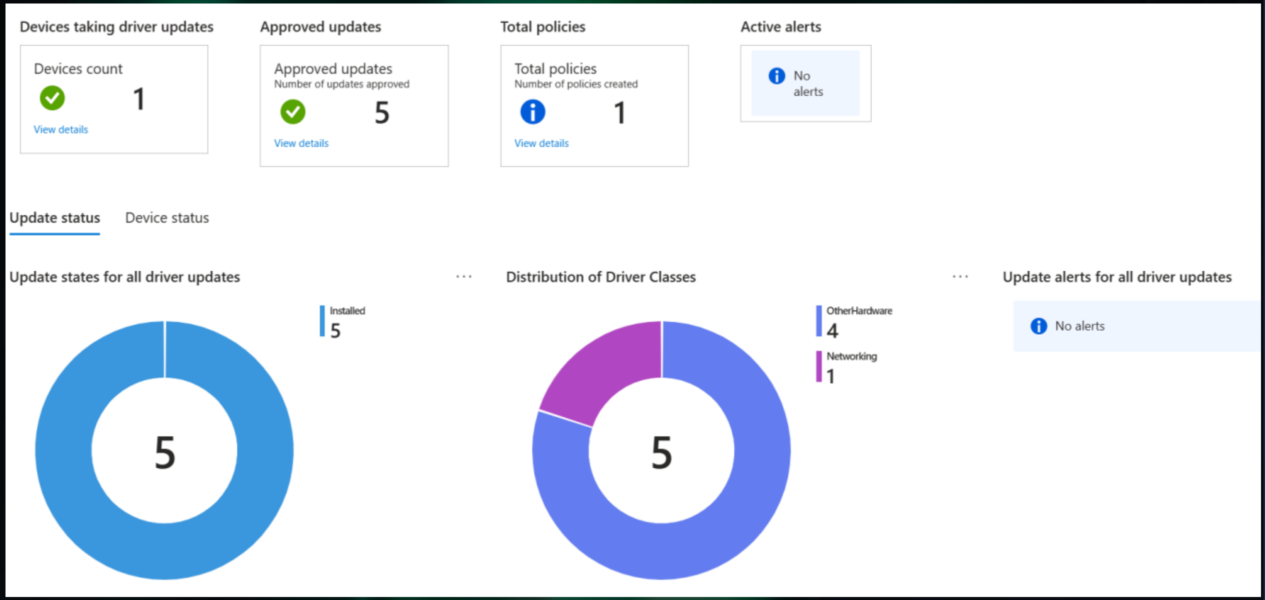
This app is self-updating. It will be added from the Enterprise App Catalog, but updates will come directly from the app publisher. Learn more about self-updating apps

Package name	Language	Architecture	Version
Chrome for Business 64-bit	en-US	x64	119.0.6045....

7-Zip
Igor Pavlov
Amazon AWS Tools for Windows
Amazon Web Services Developer
Amazon Corretto 16
Amazon
Amazon Kindle
Amazon
Android Studio 2022
Android
Android Studio 3
Android
Android Studio 4
Android
Araxis Merge
Araxis
Artweaver Free
Boris Eyrich Software
Atomi Systems ActivePresenter
Atomi Systems, Inc.
Audacity
Audacity
Beyond Compare
Scooter Software, Inc.
Blender
Blender Foundation
BlueJeans 2
Blue Jeans
Brady Workstation
Brady Corporation
Burp Suite Community Edition
PortSwigger
Burp Suite Professional Edition
PortSwigger
Calibre
Kovid Goyal
Cisco Jabber 14
Cisco Systems, Inc.
Cisco Webex Meetings
Cisco Webex LLC
Cisco WebEx Recorder and Player
Cisco Webex LLC
Cisco WebEx Recording Editor
Cisco Webex LLC
Cisco Webex Teams

Drivers and Firmware

- Traditionally been the hardest to patch with custom Software for each Vendor
- Summer 2023 – Windows update for Business introduced controls for Driver and Firmware updates. Intune followed
- Not perfect, depends on the vendors classification of the updates for them to be deployed – improvements are being made.



Devices taking driver updates

Devices count ✓ 1

View details

Approved updates

Approved updates
Number of updates approved
✓ 5

View details

Total policies

Total policies
Number of policies created
ⓘ 1

View details

Active alerts

ⓘ No alerts

Update status | Device status

Update states for all driver updates ···

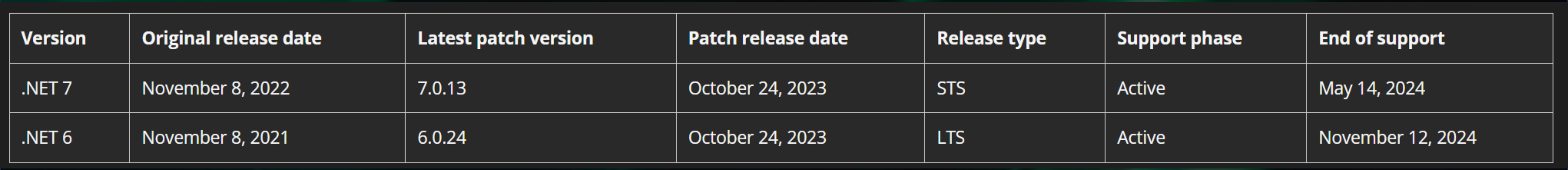
Distribution of Driver Classes ···

Update alerts for all driver updates

ⓘ No alerts

Decommission software

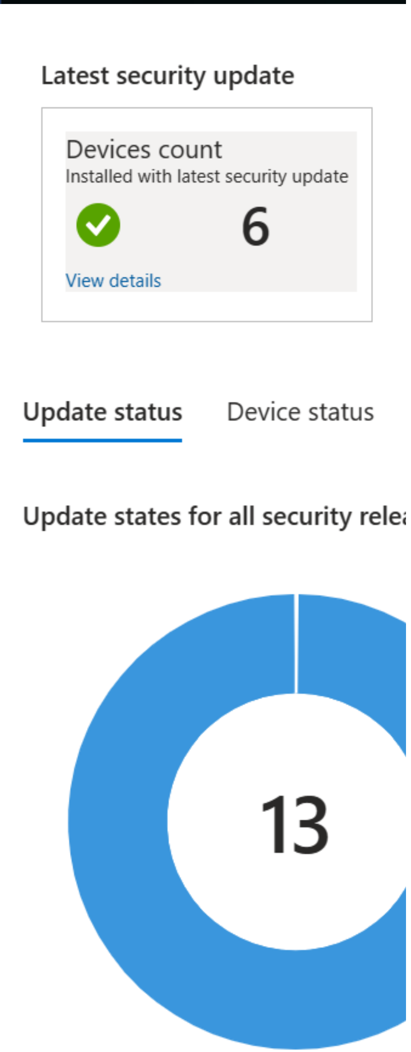
- One of the hardest things as LOB apps still is needed Example:
  - .NET Desktop Runtime
- TVM will report these as EOS version



Version	Original release date	Latest patch version	Patch release date	Release type	Support phase	End of support
.NET 7	November 8, 2022	7.0.13	October 24, 2023	STS	Active	May 14, 2024
.NET 6	November 8, 2021	6.0.24	October 24, 2023	LTS	Active	November 12, 2024

Reporting

Windows Update for Business reports



Latest security update

Devices count

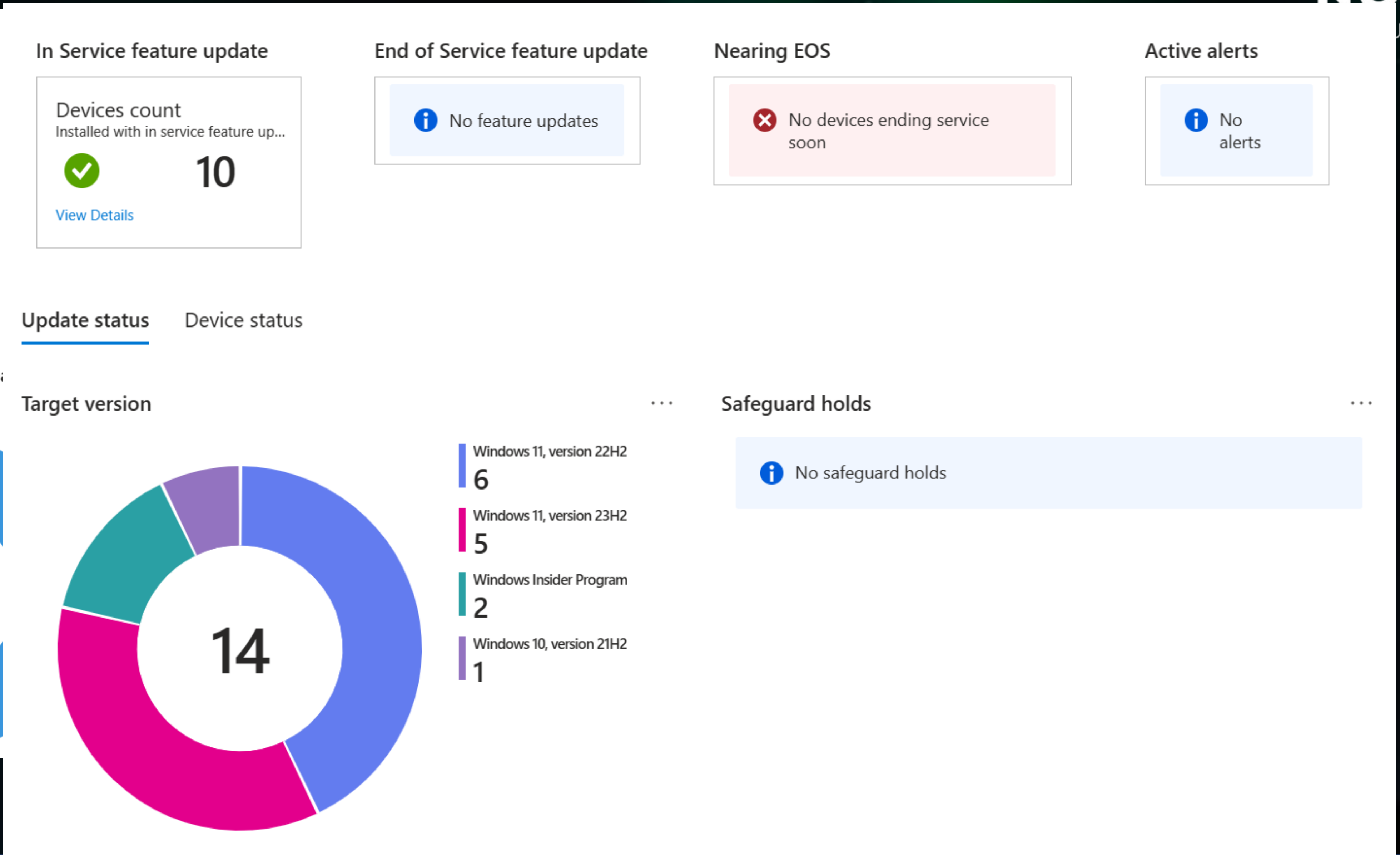
Installed with latest security update

✓ 6

View details

Update status | Device status

Update states for all security relea



In Service feature update

Devices count

Installed with in service feature up...

✓ 10

View Details

End of Service feature update

ⓘ No feature updates

Nearing EOS

☒ No devices ending service soon

Active alerts

ⓘ No alerts

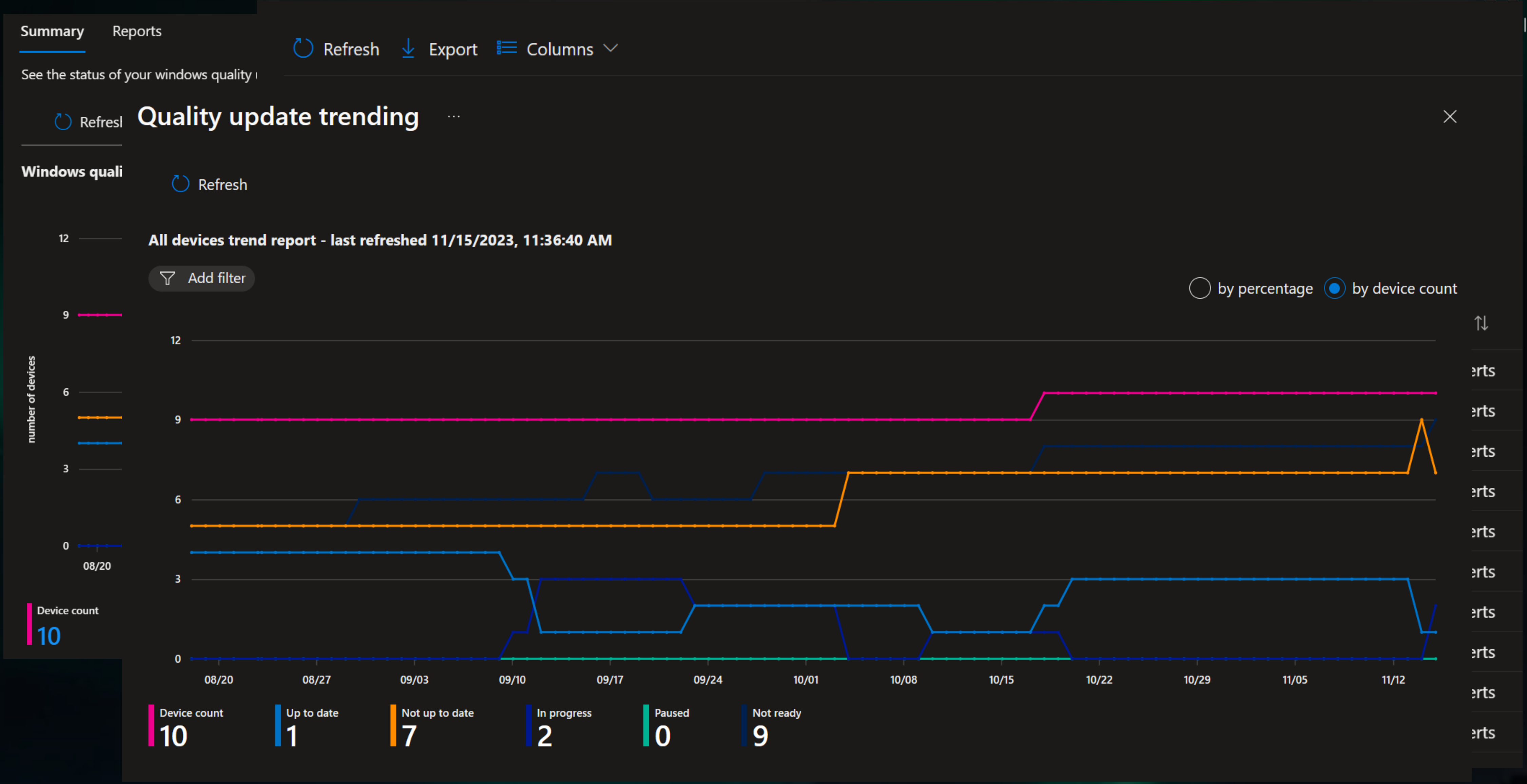
Update status | Device status

Target version ...

Safeguard holds ...

ⓘ No safeguard holds

Microsoft AutoPatch



Summary Reports

See the status of your windows quality

Refresl

Windows quali

Device count
10

Refresh Export Columns

Quality update trending

Refresh

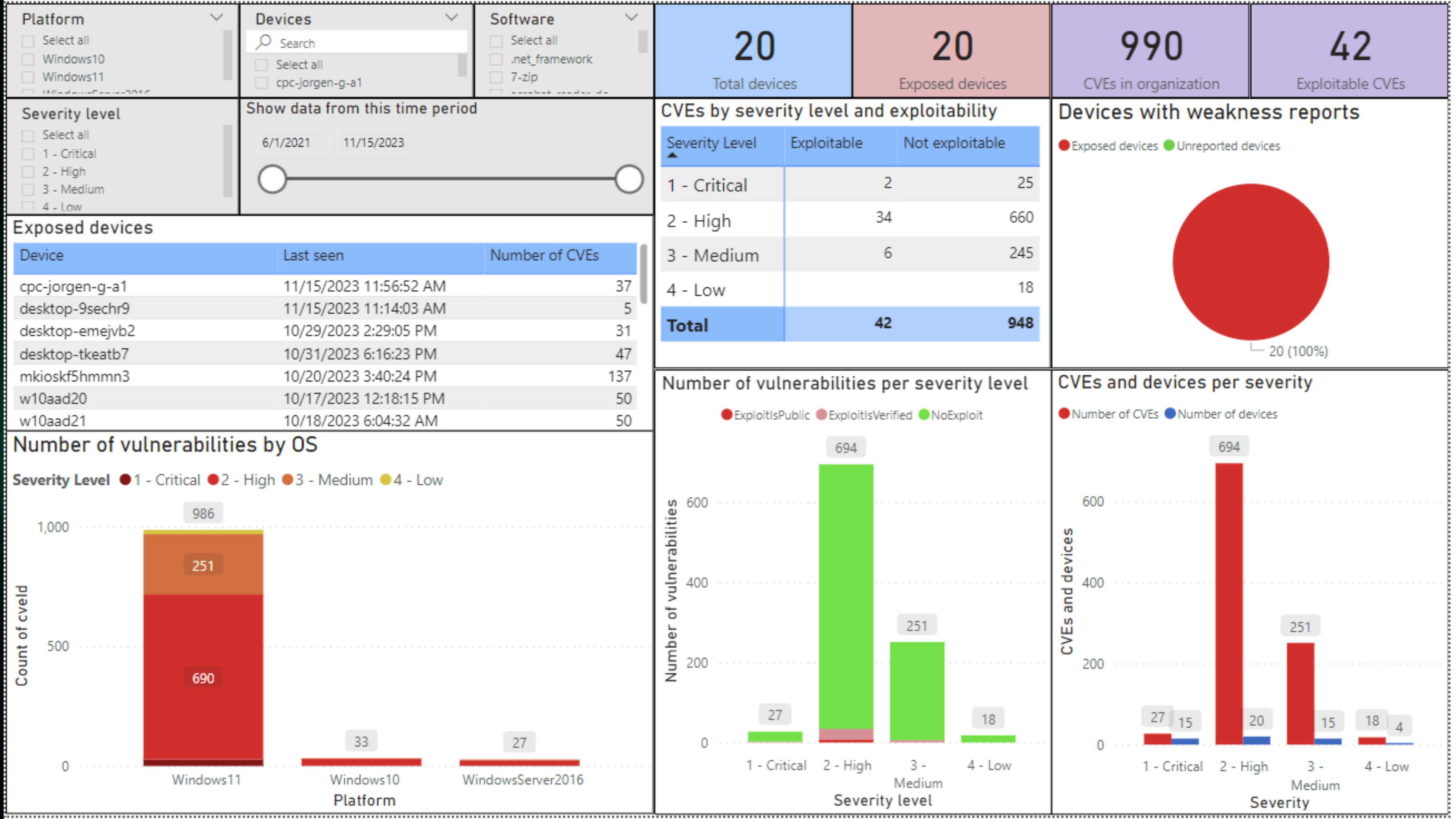
All devices trend report - last refreshed 11/15/2023, 11:36:40 AM

Add filter

○ by percentage ● by device count

Device count	Up to date	Not up to date	In progress	Paused	Not ready
10	1	7	2	0	9

PowerBI and TVM



Platform
- □ Select all
- □ Windows10
- □ Windows11

Devices
- Search
- □ Select all
- □ cpc-jorgen-g-a1

Software
- □ Select all
- □ .net_framework
- □ 7-zip

20	20	990	42
Total devices	Exposed devices	CVEs in organization	Exploitable CVEs

Severity level
- □ Select all
- □ 1 - Critical
- □ 2 - High
- □ 3 - Medium
- □ 4 - Low

Show data from this time period

6/1/2021 11/15/2023

CVEs by severity level and exploitability

Severity Level	Exploitable	Not exploitable
1 - Critical	2	25
2 - High	34	660
3 - Medium	6	245
4 - Low		18
Total	**42**	**948**

Devices with weakness reports

Exposed devices

Device	Last seen	Number of CVEs
cpc-jorgen-g-a1	11/15/2023 11:56:52 AM	37
desktop-9sechr9	11/15/2023 11:14:03 AM	5
desktop-emejvb2	10/29/2023 2:29:05 PM	31
desktop-tkeatb7	10/31/2023 6:16:23 PM	47
mkioskf5hmmn3	10/20/2023 3:40:24 PM	137
w10aad20	10/17/2023 12:18:15 PM	50
w10aad21	10/18/2023 6:04:32 AM	50

Number of vulnerabilities by OS

Number of vulnerabilities per severity level

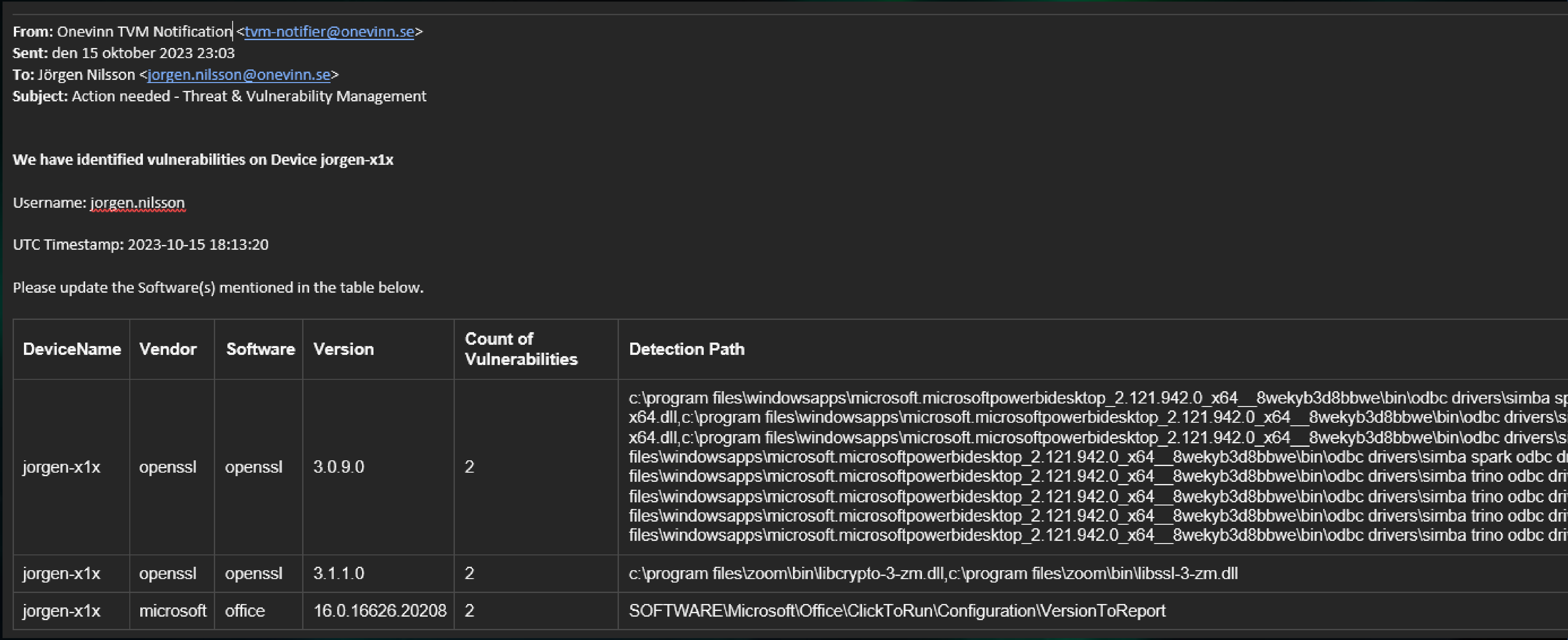
● ExploitIsPublic ● ExploitIsVerified ● NoExploit
Number of vulnerabilities
600
400
200
0
694
251
27
18
1 - Critical
2 - High
3 - Medium
4 - Low
Severity level

CVEs and devices per severity

TVM Notifier

- Keeping Devices Updated
    - Users with permissions to Install Own Applications
    - Developers
    - Power Users
    - IT

End User Notification



From: Onevinn TVM Notification <tvm-notifier@onevinn.se>
Sent: den 15 oktober 2023 23:03
To: Jörgen Nilsson <jorgen.nilsson@onevinn.se>
Subject: Action needed - Threat & Vulnerability Management

We have identified vulnerabilities on Device jorgen-x1x

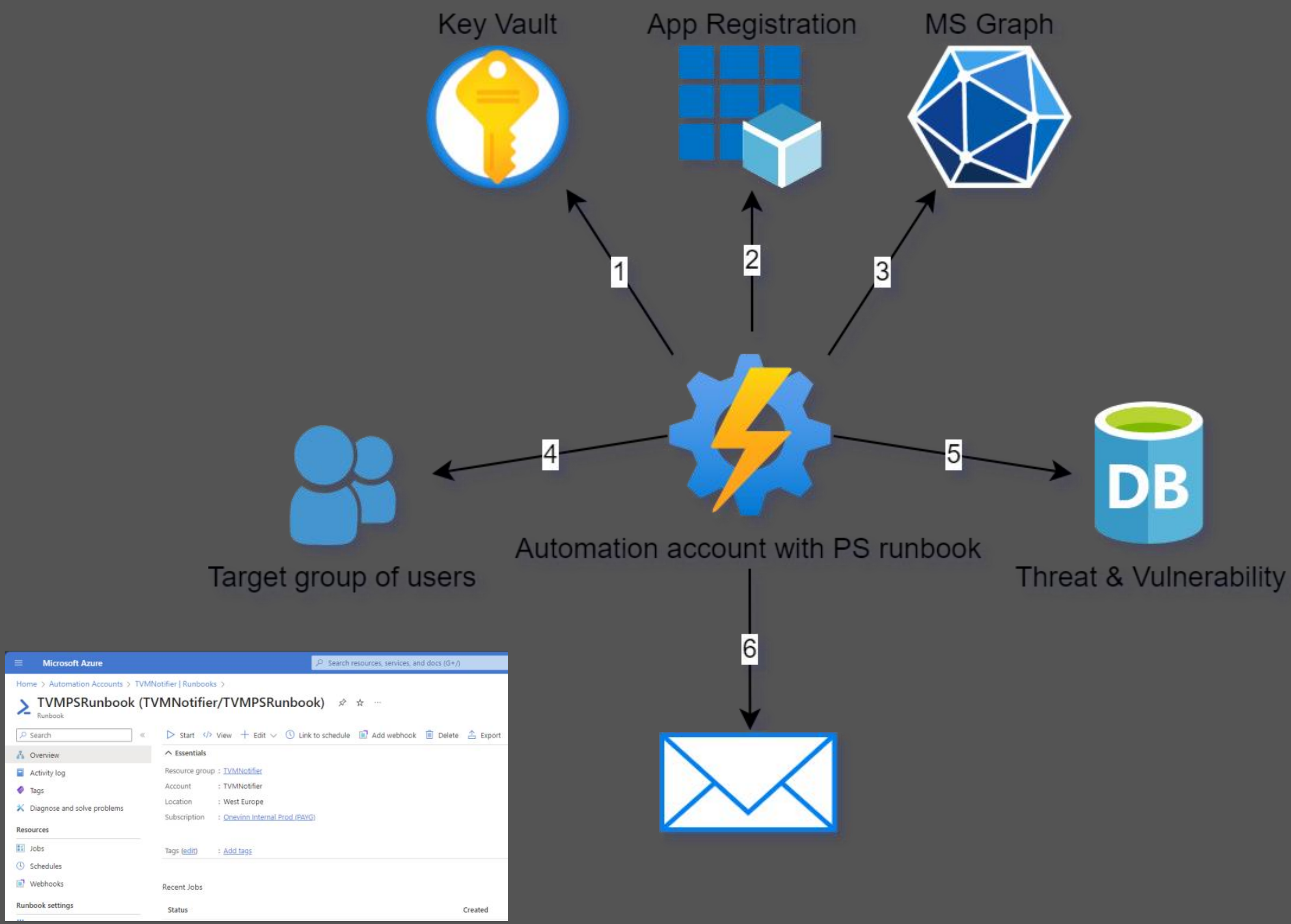
Username: jorgen.nilsson

UTC Timestamp: 2023-10-15 18:13:20

Please update the Software(s) mentioned in the table below.

DeviceName	Vendor	Software	Version	Count of Vulnerabilities	Detection Path
jorgen-x1x	openssl	openssl	3.0.9.0	2	c:\program files\windowsapps\microsoft.microsoftpowerbidesktop_2.121.942.0_x64__8wekyb3d8bbwe\bin\odbc drivers\simba sp x64.dll,c:\program files\windowsapps\microsoft.microsoftpowerbidesktop_2.121.942.0_x64__8wekyb3d8bbwe\bin\odbc drivers\s x64.dll,c:\program files\windowsapps\microsoft.microsoftpowerbidesktop_2.121.942.0_x64__8wekyb3d8bbwe\bin\odbc drivers\s files\windowsapps\microsoft.microsoftpowerbidesktop_2.121.942.0_x64__8wekyb3d8bbwe\bin\odbc drivers\simba spark odbc d files\windowsapps\microsoft.microsoftpowerbidesktop_2.121.942.0_x64__8wekyb3d8bbwe\bin\odbc drivers\simba trino odbc dri files\windowsapps\microsoft.microsoftpowerbidesktop_2.121.942.0_x64__8wekyb3d8bbwe\bin\odbc drivers\simba trino odbc dri files\windowsapps\microsoft.microsoftpowerbidesktop_2.121.942.0_x64__8wekyb3d8bbwe\bin\odbc drivers\simba trino odbc dri files\windowsapps\microsoft.microsoftpowerbidesktop_2.121.942.0_x64__8wekyb3d8bbwe\bin\odbc drivers\simba trino odbc dri
jorgen-x1x	openssl	openssl	3.1.1.0	2	c:\program files\zoom\bin\libcrypto-3-zm.dll,c:\program files\zoom\bin\libssl-3-zm.dll
jorgen-x1x	microsoft	office	16.0.16626.20208	2	SOFTWARE\Microsoft\Office\ClickToRun\Configuration\VersionToReport

TVM Notifier



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Automation Accounts > TVMNotifier | Runbooks >

TVMPSRunbook (TVMNotifier/TVMPSRunbook)

Runbook

Search

Overview

Activity log

Tags

Diagnose and solve problems

Resources

Jobs

Schedules

Webhooks

Runbook settings

Start · View · Edit · Link to schedule · Add webhook · Delete · Export

Essentials

Resource group : TVMNotifier

Account : TVMNotifier

Location : West Europe

Subscription : Onevinn Internal Prod (PAYG)

Tags (edit) : Add tags

Recent Jobs

Status · Created

Call to Action

- Visibility = Accountability
- Shorten time before you Patch
- Patch, Patch Patch
- Use TVM for help with Prioritization of 3rd party apps