ALSID

ANSSI

SATURDAY, 29TH JULY 2017

WSUSpendu

USE WSUS TO HANG ITS CLIENTS

YVES LE PROVOST & ROMAIN COLTEL

Who we are, what we do...

- Yves Le Provost
  - Security auditor for more than 10 years
  - Currently works for French cyber defense Agency (ANSSI)
  - Specializes in SCADA and database assessments, but masters any other field ;-)

- Romain Coltel
  - Former security auditor
  - Currently works for a disruptive startup
  - Developing next-gen Active Directory security product

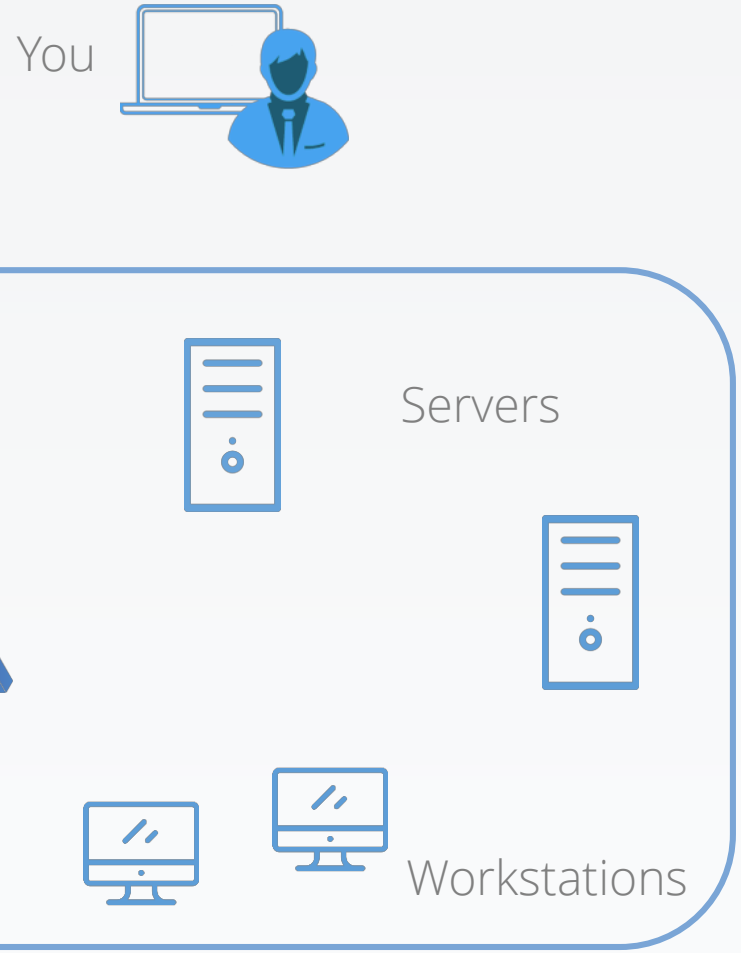
The problem

Sometimes, compromising a network is not that easy.

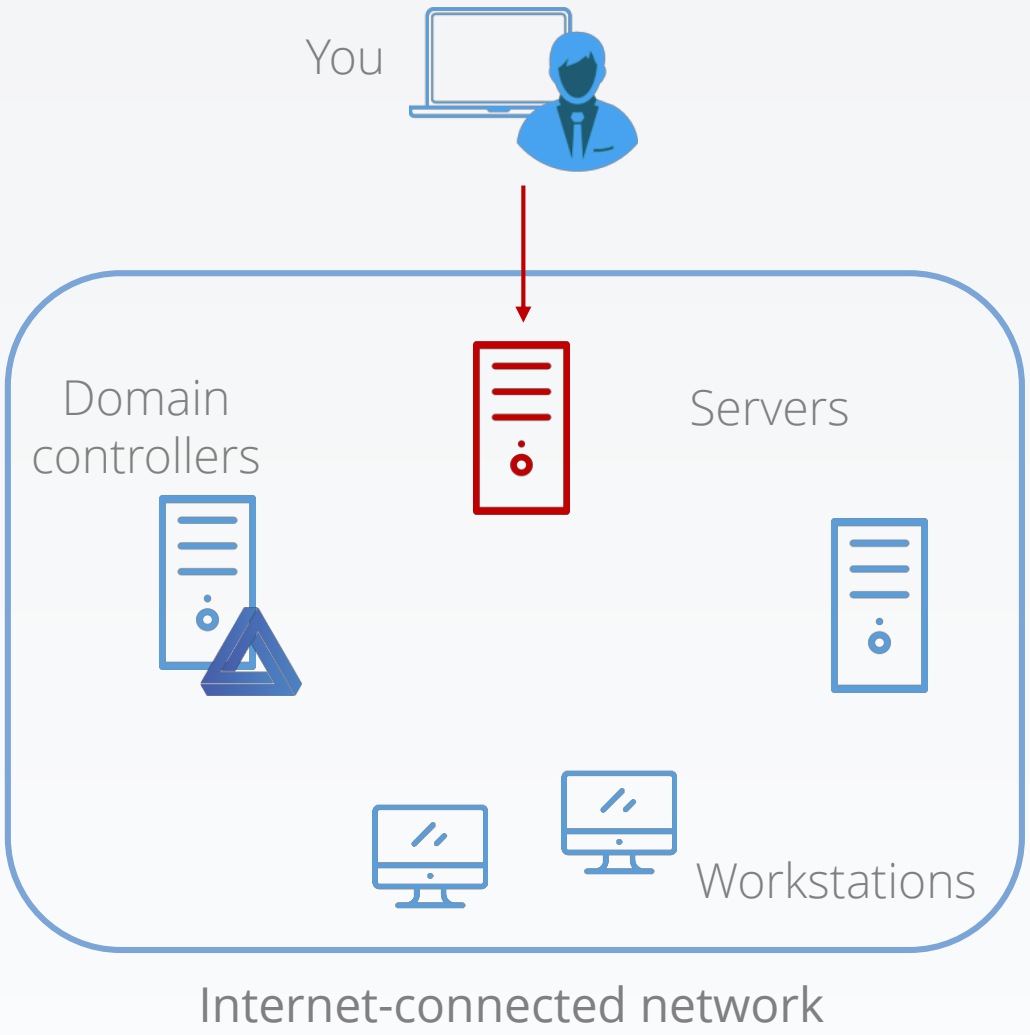
Compromise scenario

You 

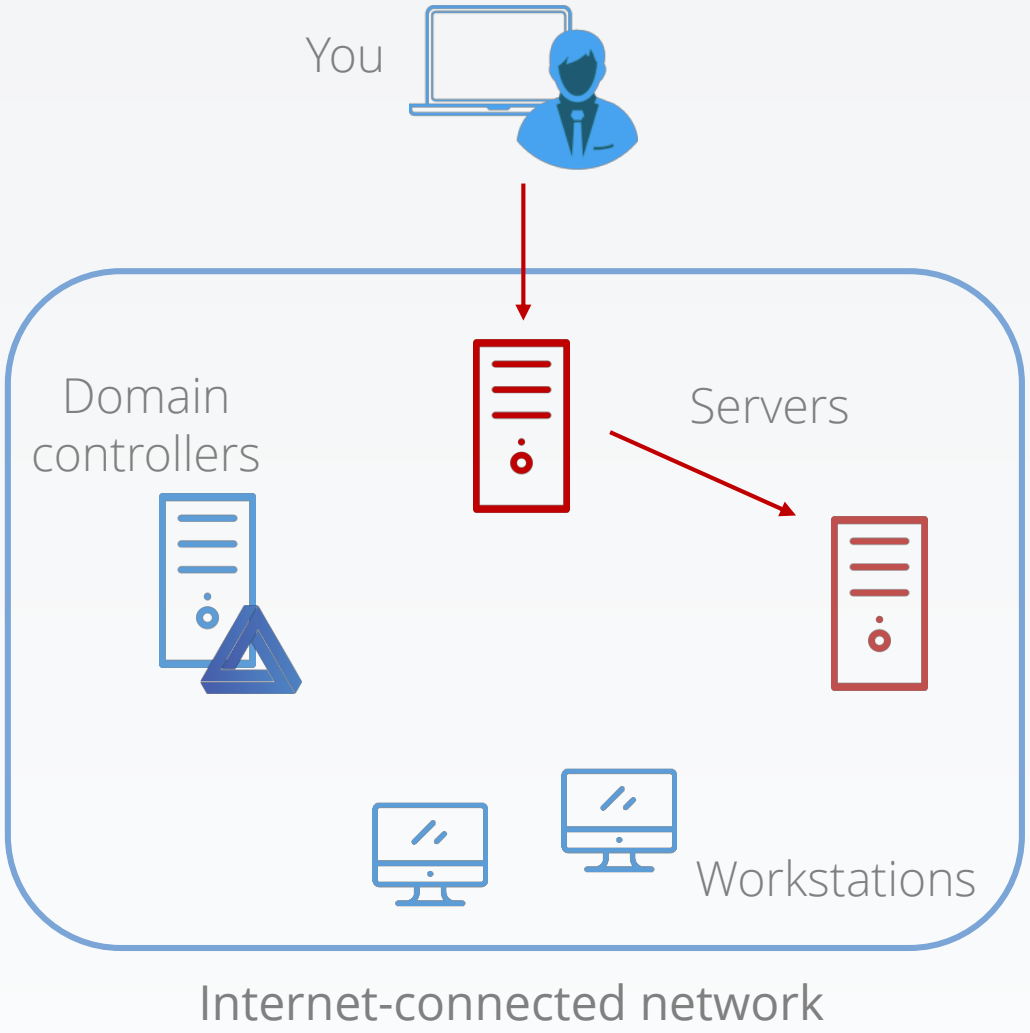
Compromise scenario



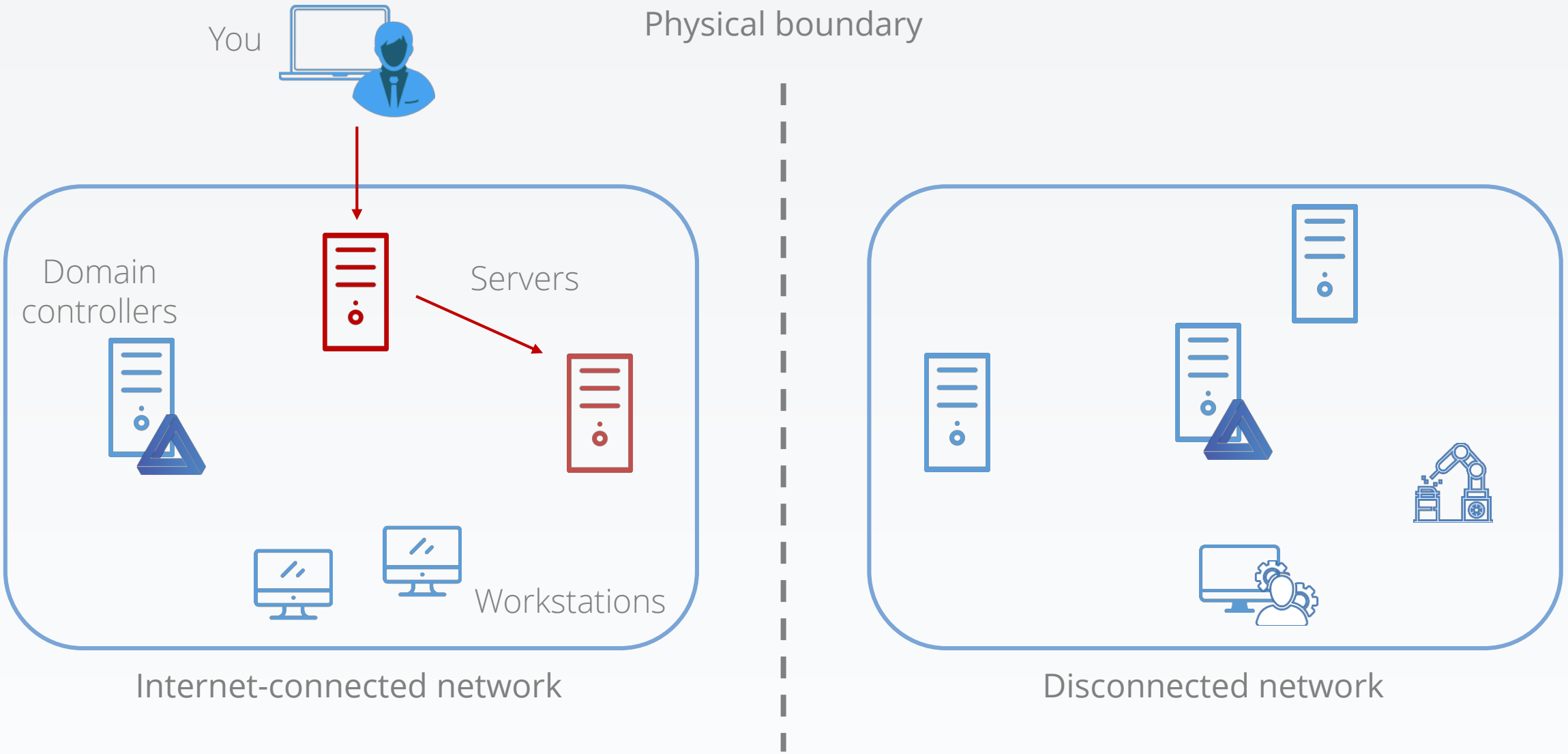
Compromise scenario



Compromise scenario



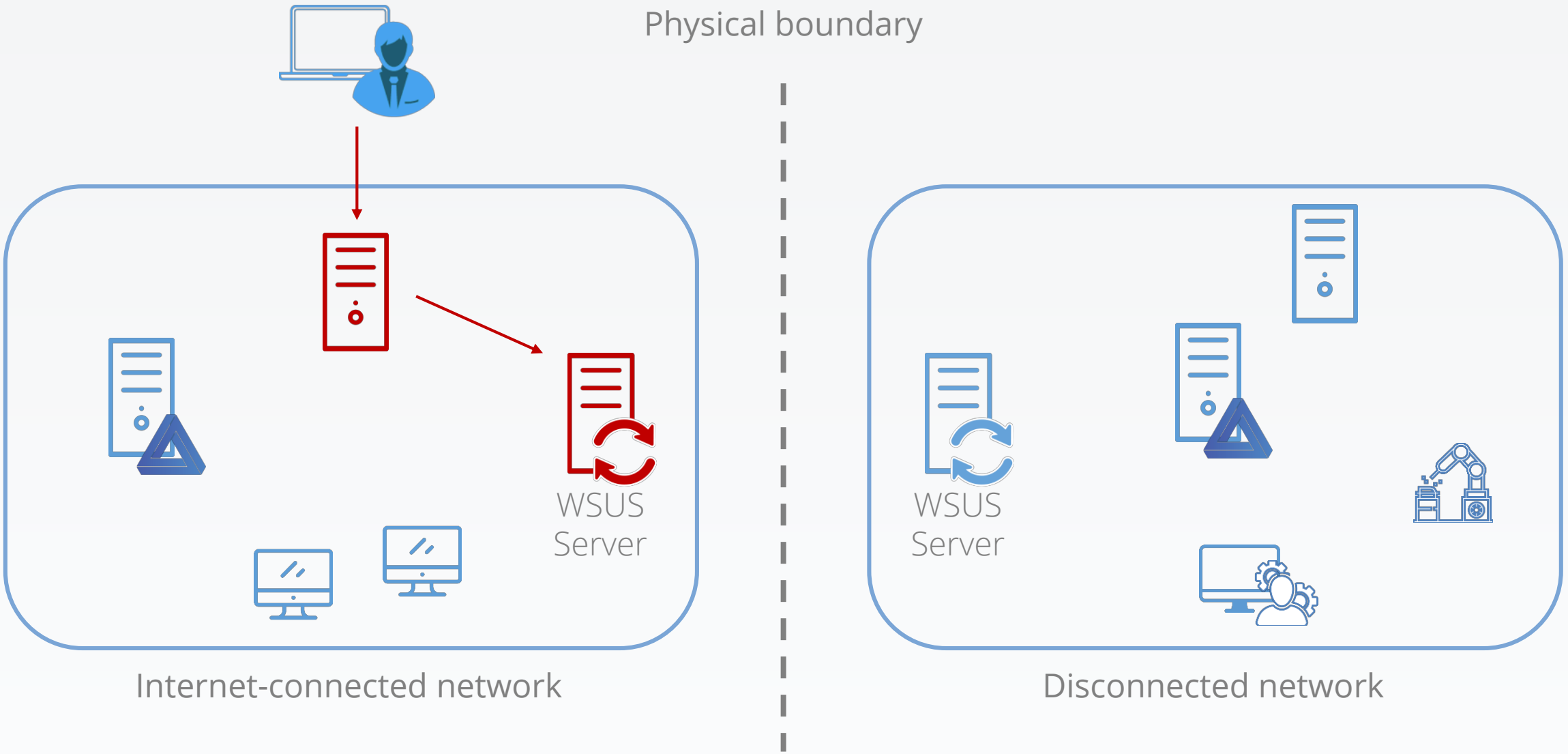
Compromise scenario



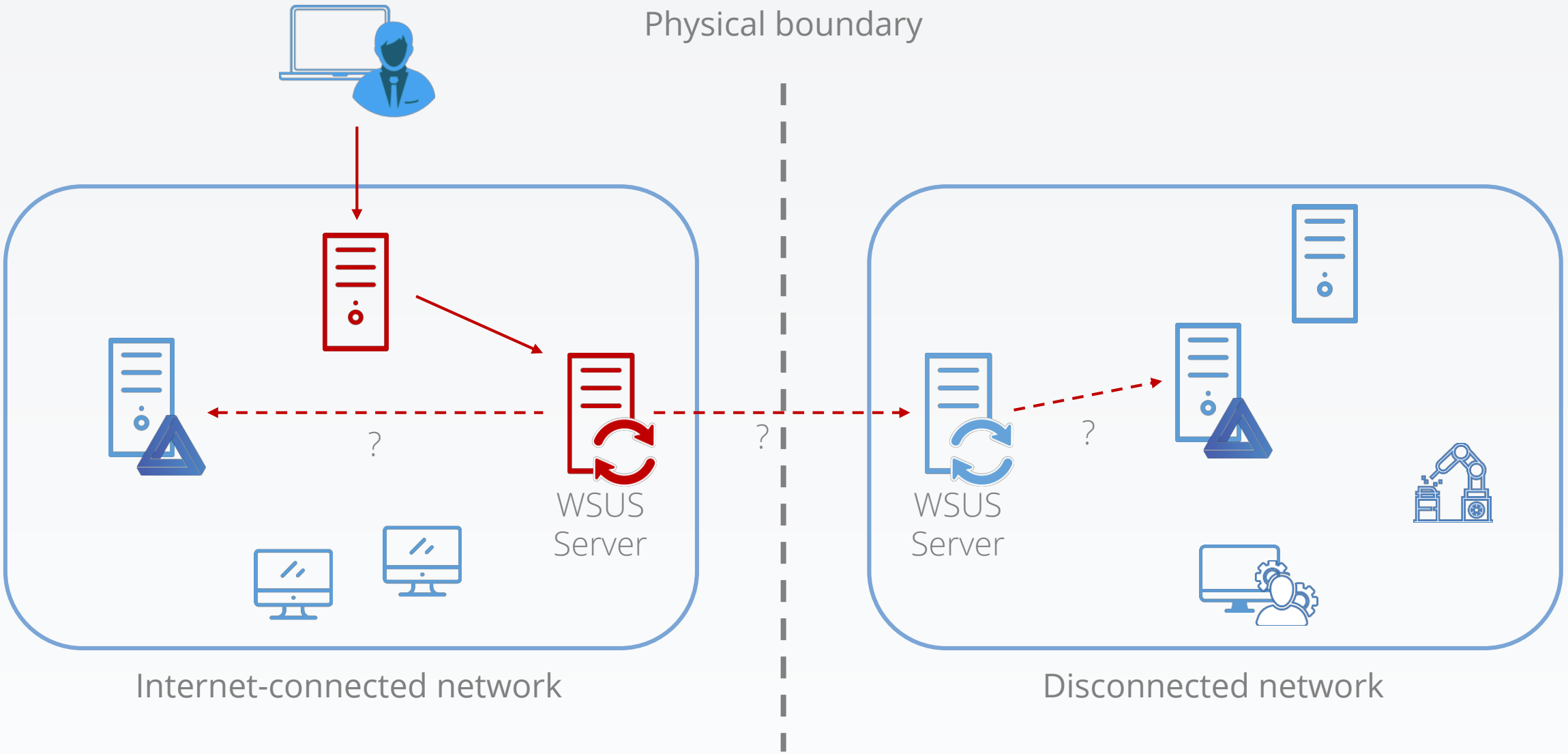
The solution?

Sometimes, compromising a network might not be as far as we think.

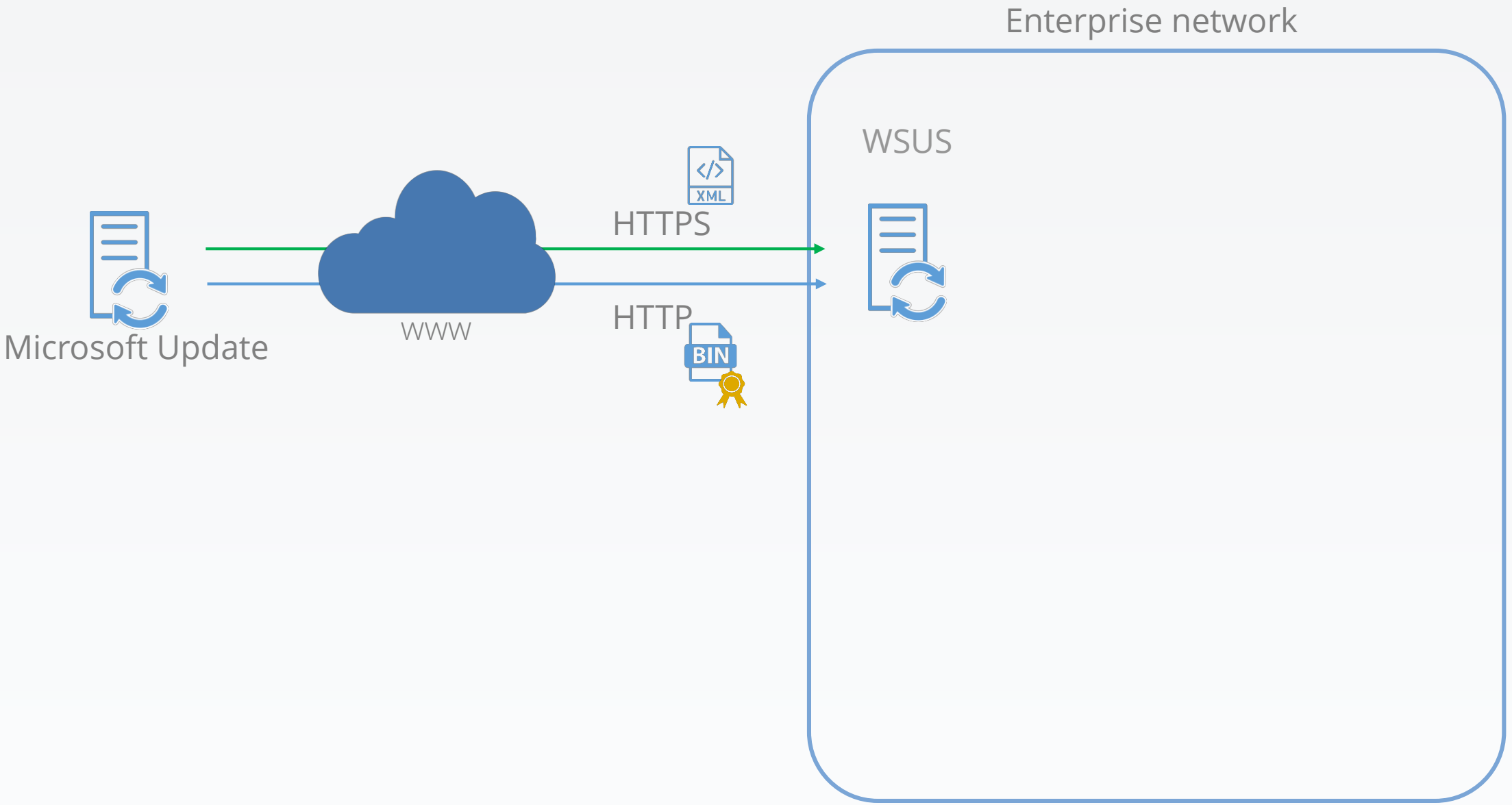
Potential compromise scenario



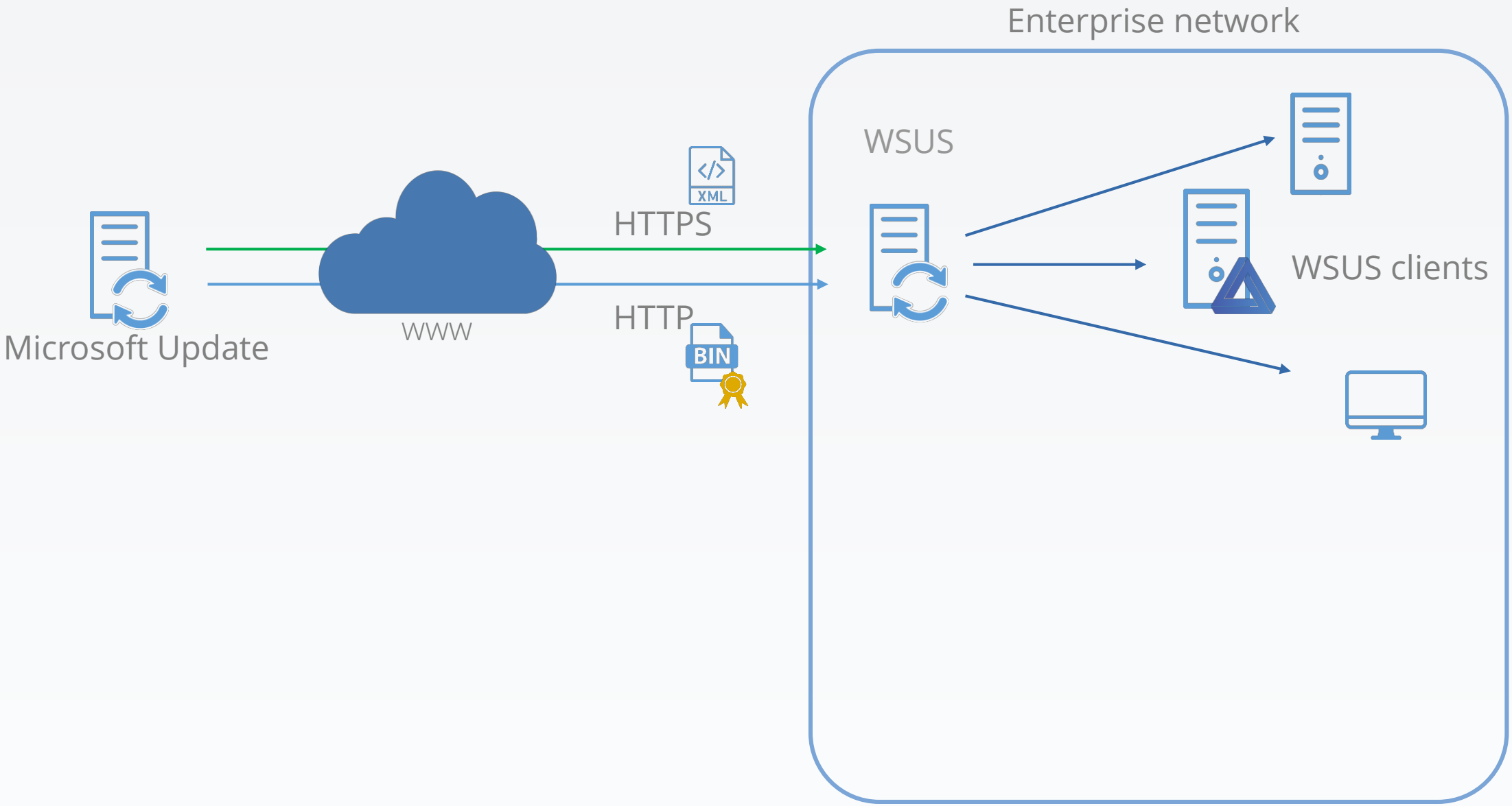
Potential compromise scenario



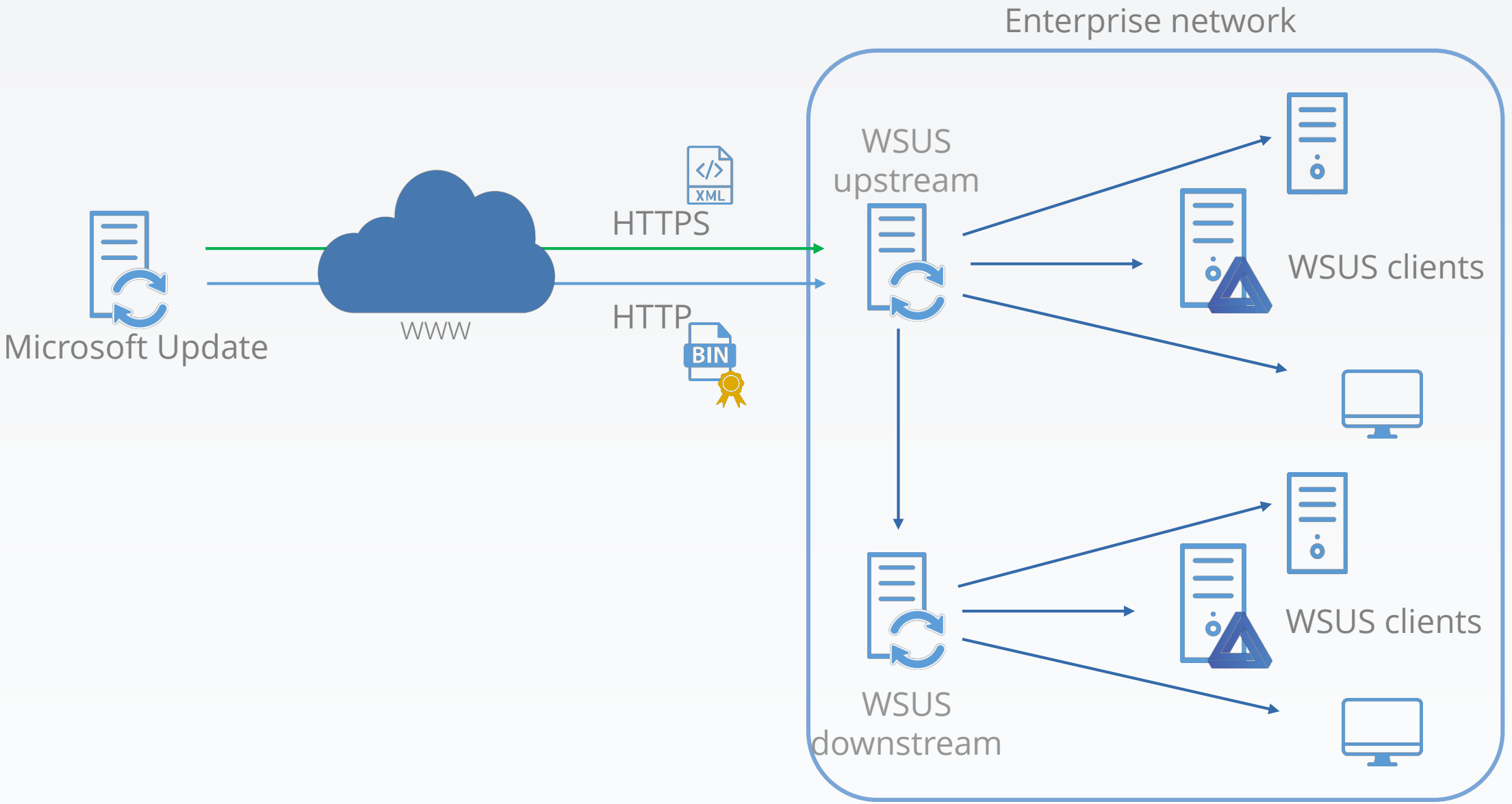
Windows Server Update Services (WSUS)



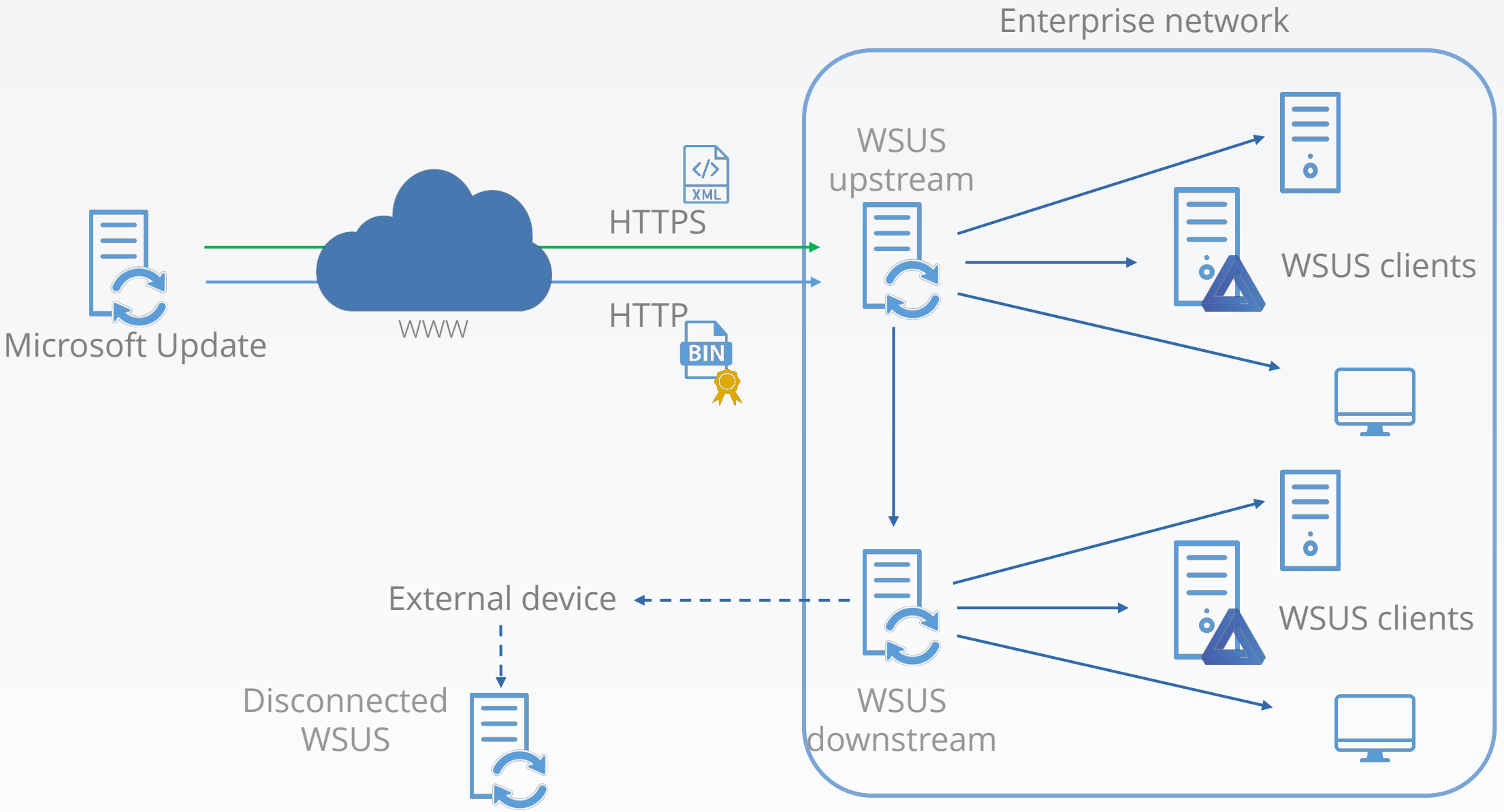
Windows Server Update Services (WSUS)



Windows Server Update Services (WSUS)

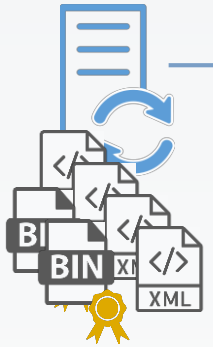


Windows Server Update Services (WSUS)



Updates journey within a WSUS server

Microsoft Update



Windows service

Web service

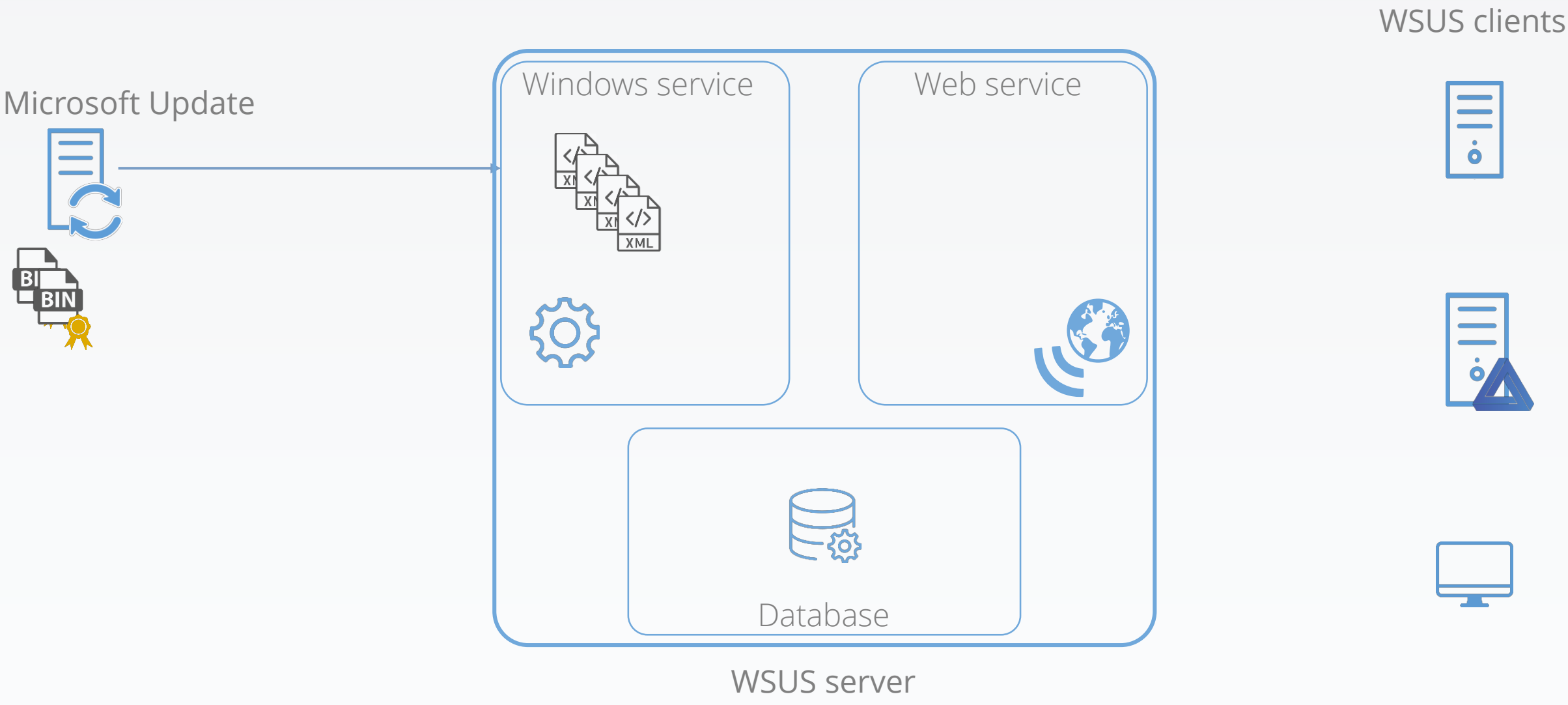
Database

WSUS server

WSUS clients

Updates journey within a WSUS server

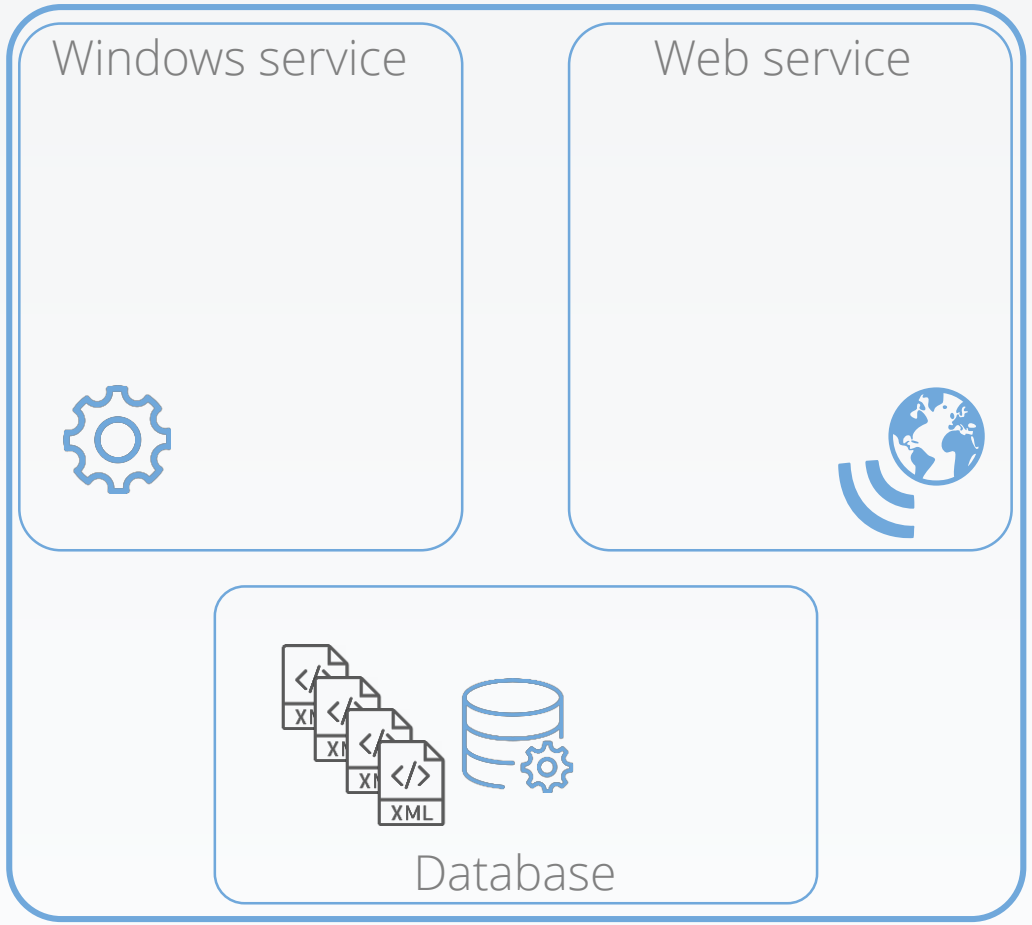
1. Windows service downloads update metadata (binaries size, download URL, command-line arguments, ...)



Updates journey within a WSUS server

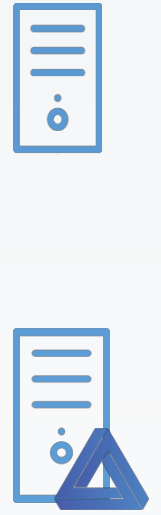
2. Windows service transmits the metadata to the database

Microsoft Update



WSUS server

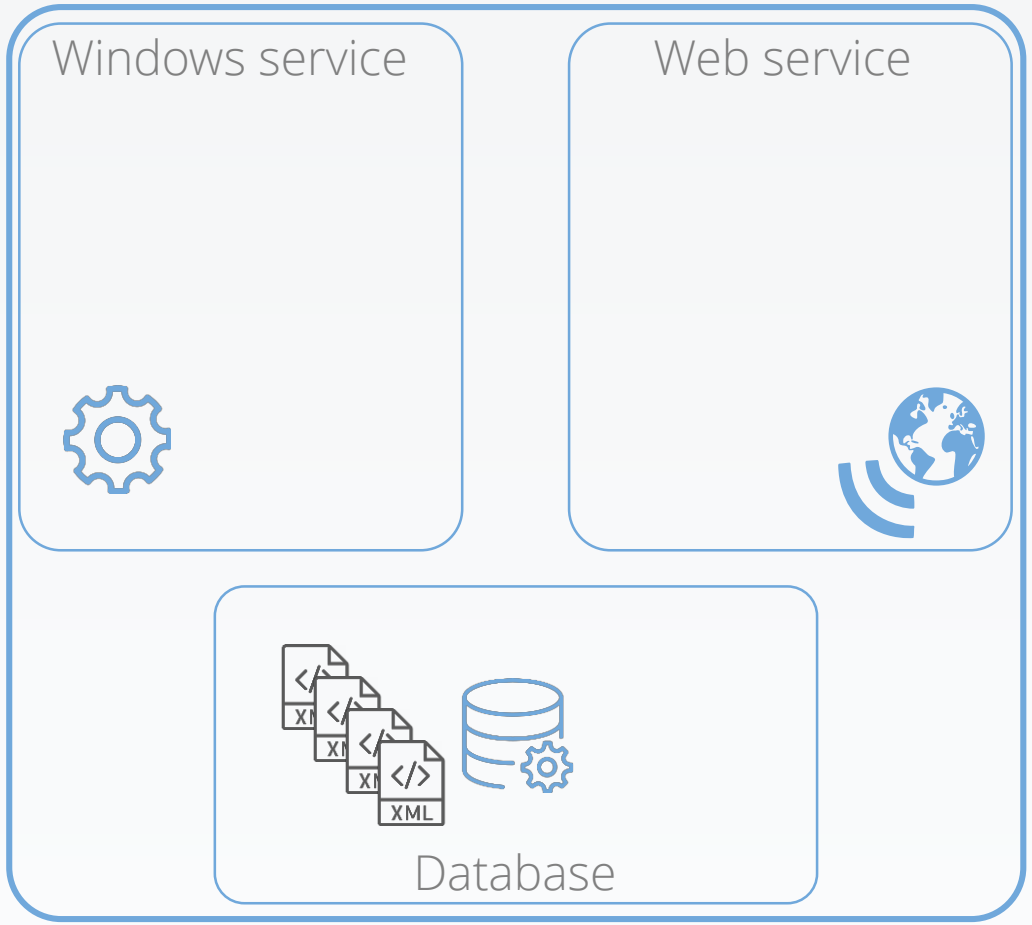
WSUS clients



Updates journey within a WSUS server

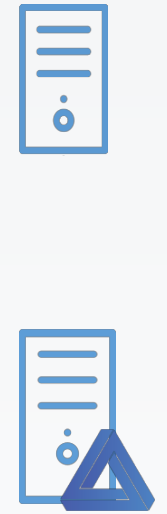
3. The database uses functions to parse metadata inputs, incorporates them into its tables

Microsoft Update



WSUS server

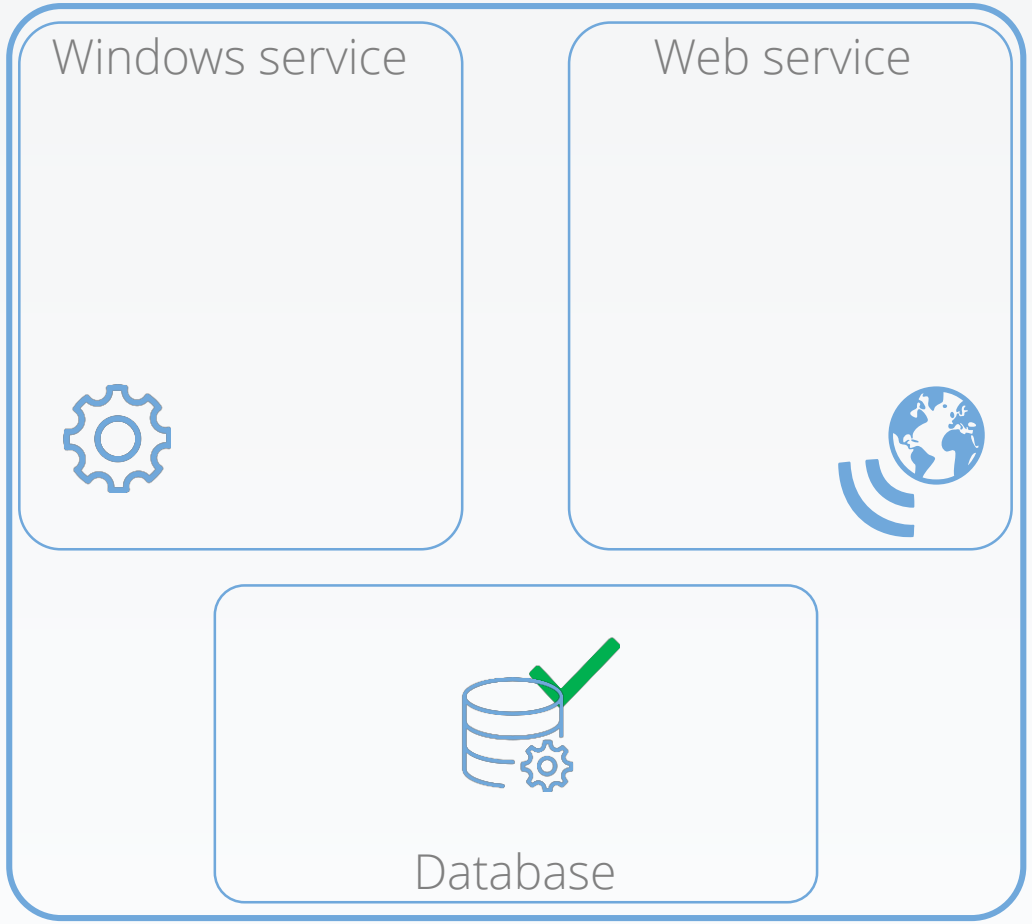
WSUS clients



Updates journey within a WSUS server

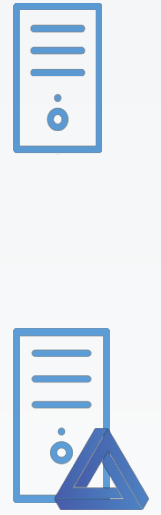
4. Updates are approved, either by an admin or by automatic approval rules

Microsoft Update



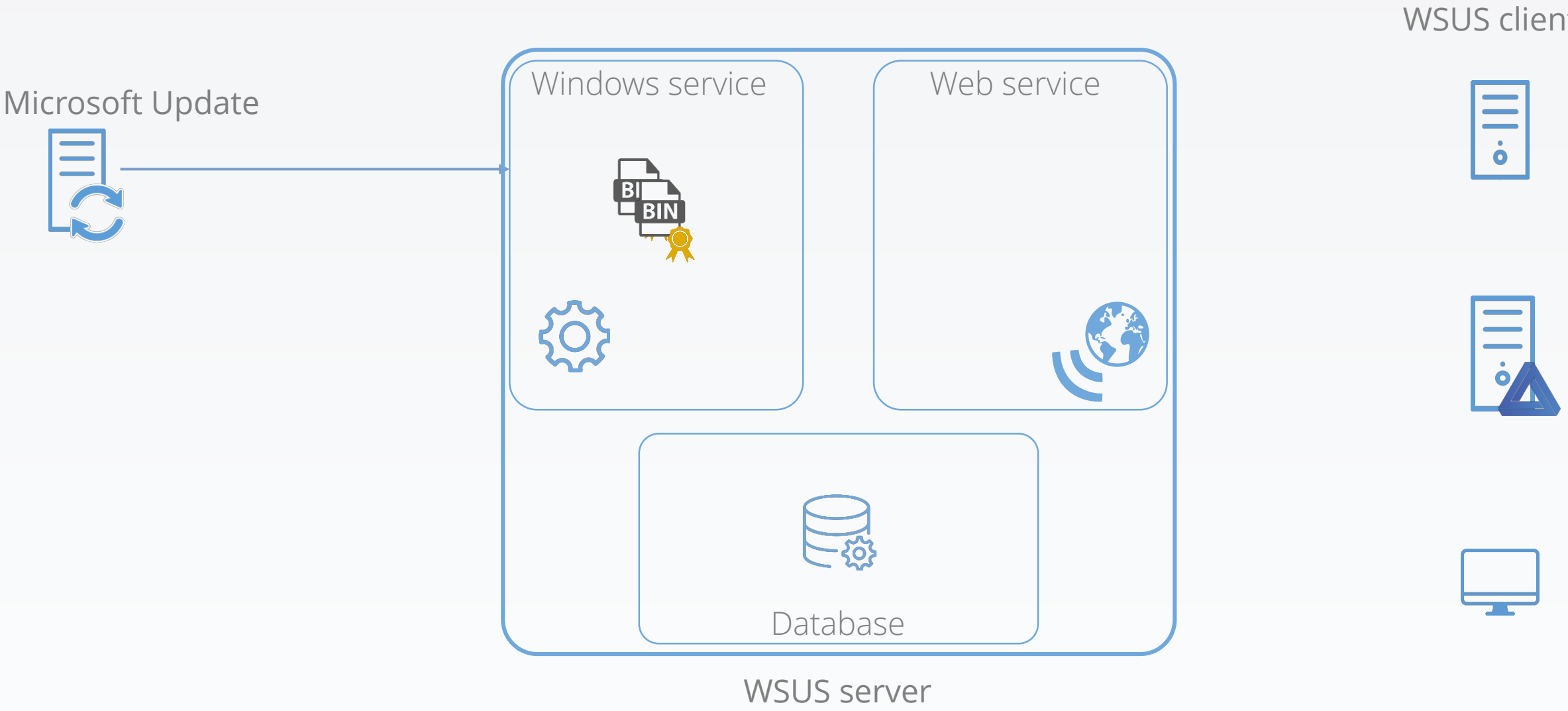
WSUS server

WSUS clients



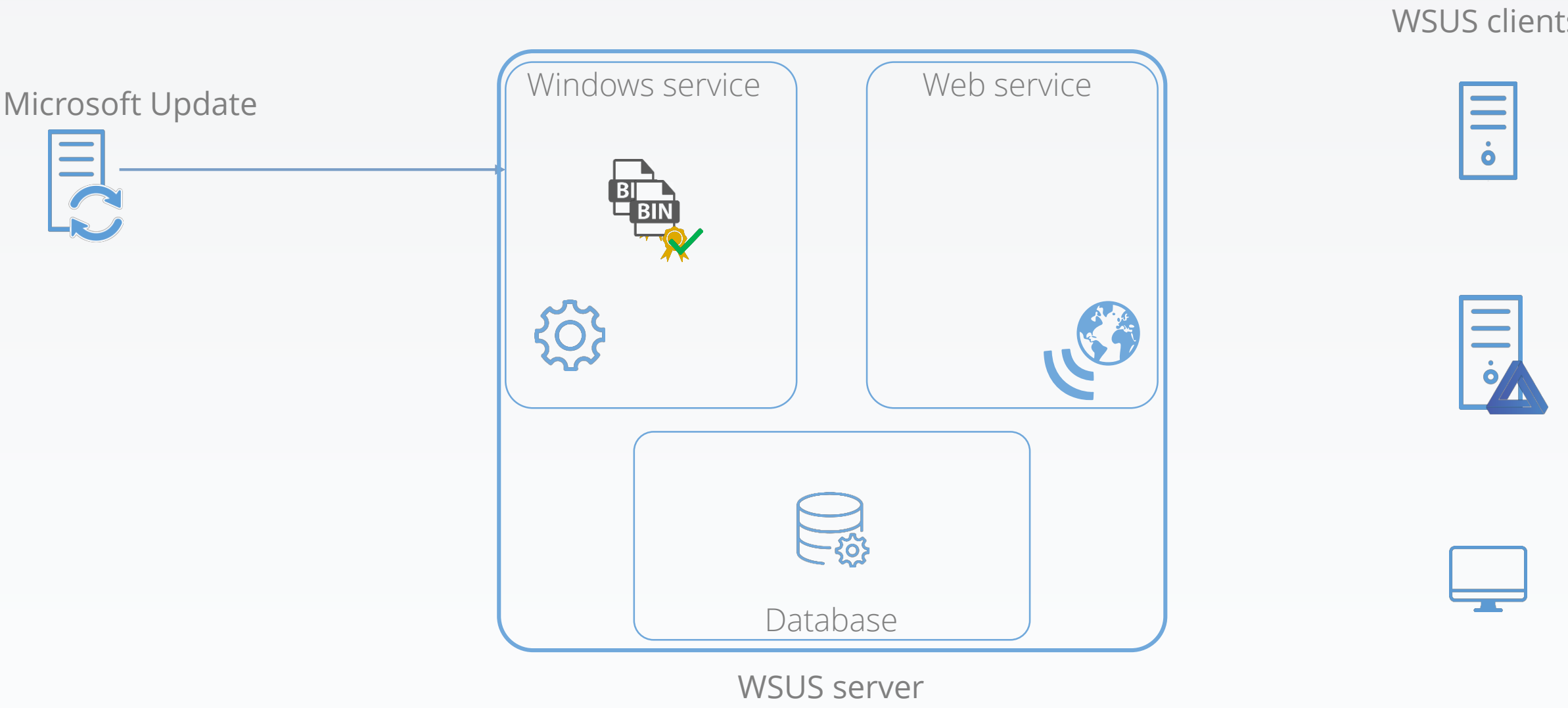
Updates journey within a WSUS server

5. Approved updates binaries (psf, cab, exe, ...) are downloaded



Updates journey within a WSUS server

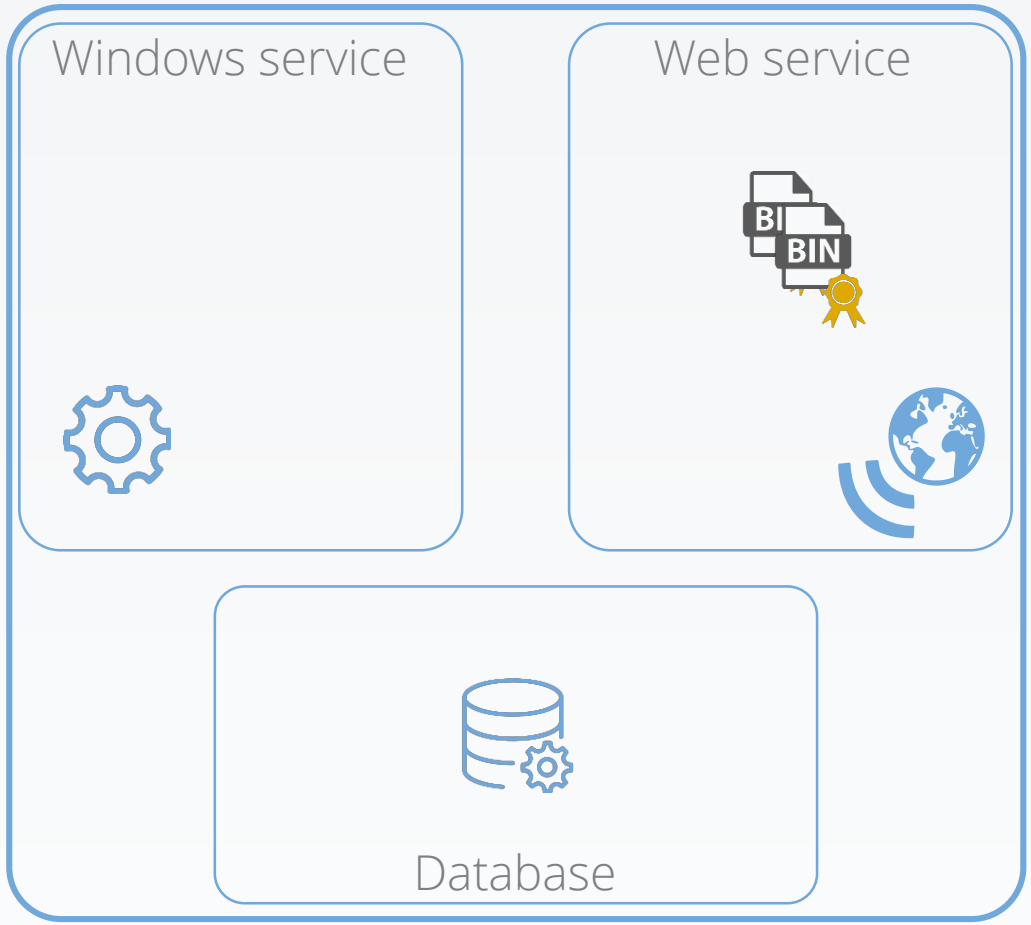
6. Each binary signature is checked



Updates journey within a WSUS server

7. Each binary is stored for the Web service to be able to get them

Microsoft Update

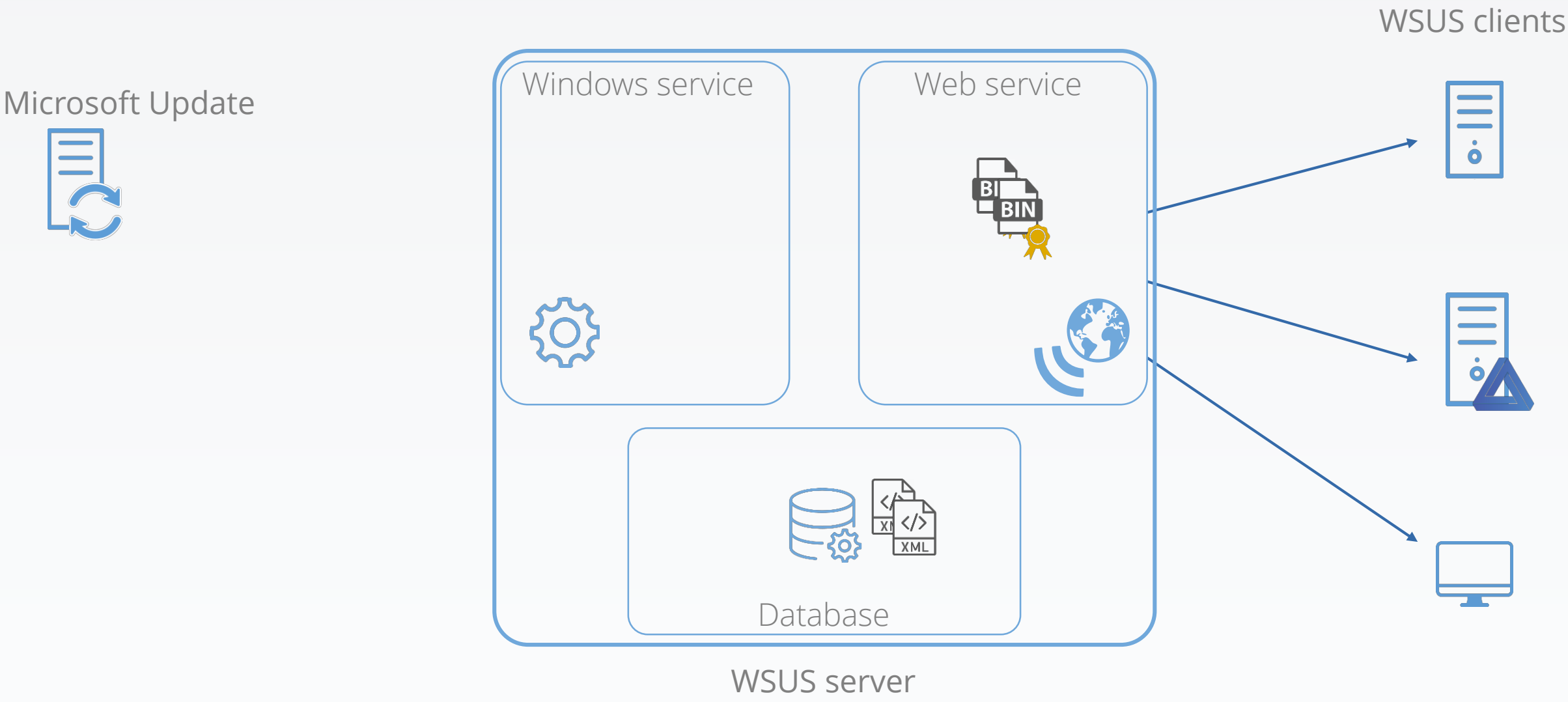


WSUS server

WSUS clients

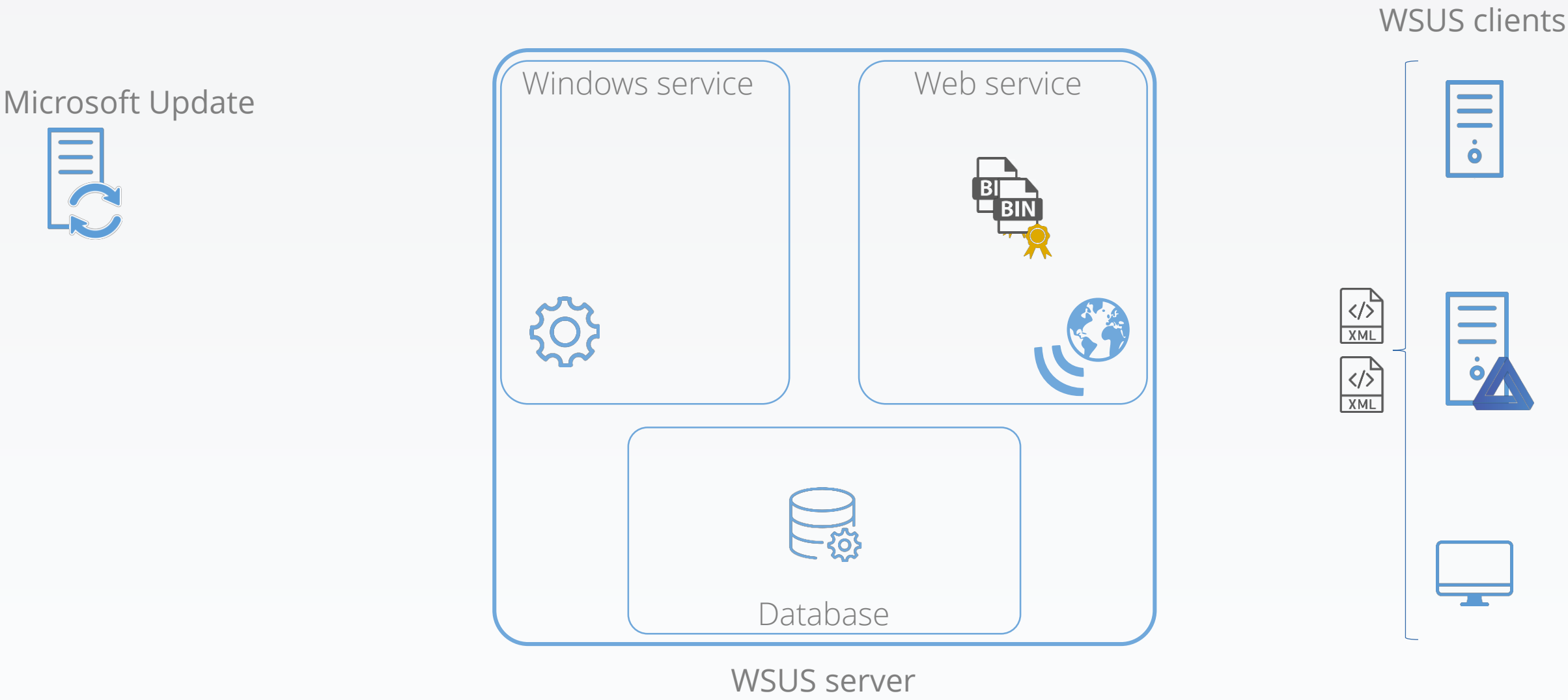
Updates journey within a WSUS server

8. Clients are looking for new updates ; Web service gets approved updates metadata from the database



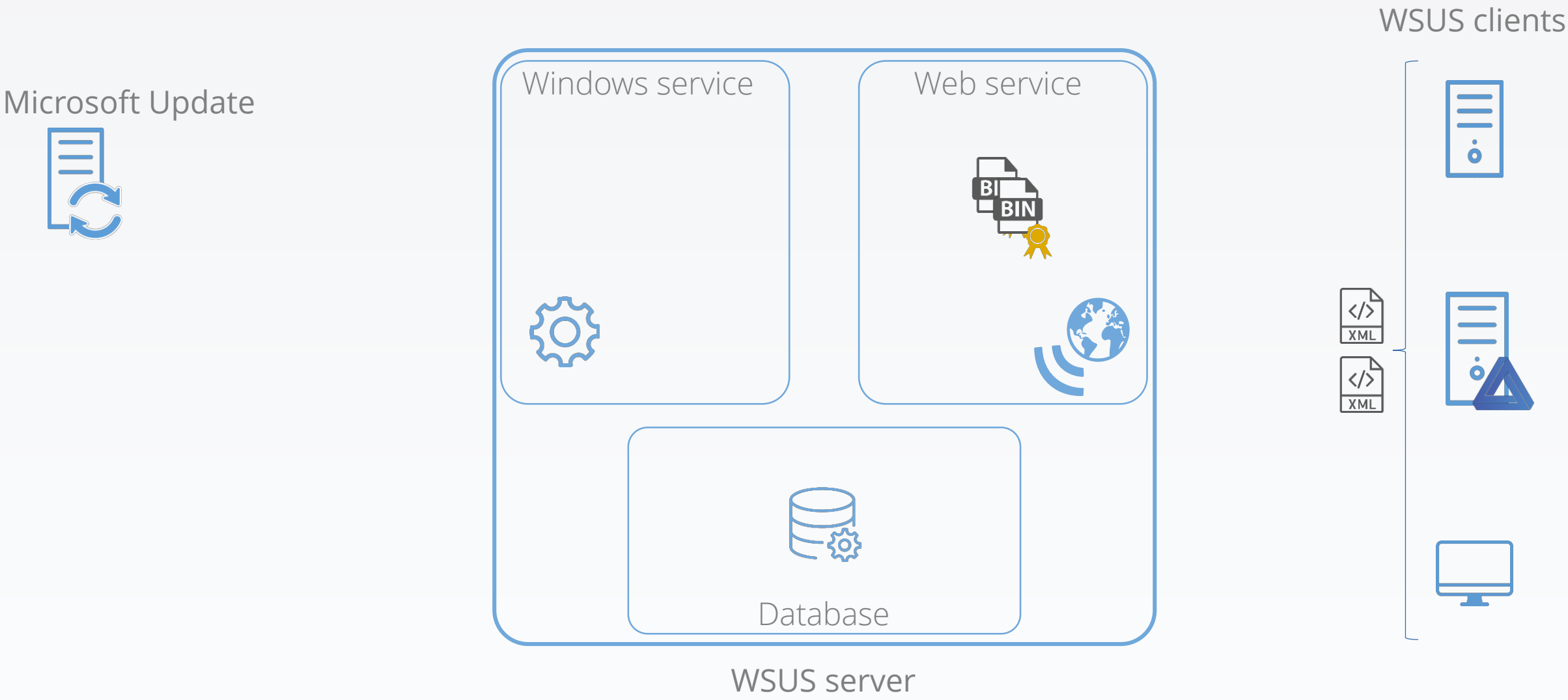
Updates journey within a WSUS server

9. Web service transmits the metadata to the WSUS clients



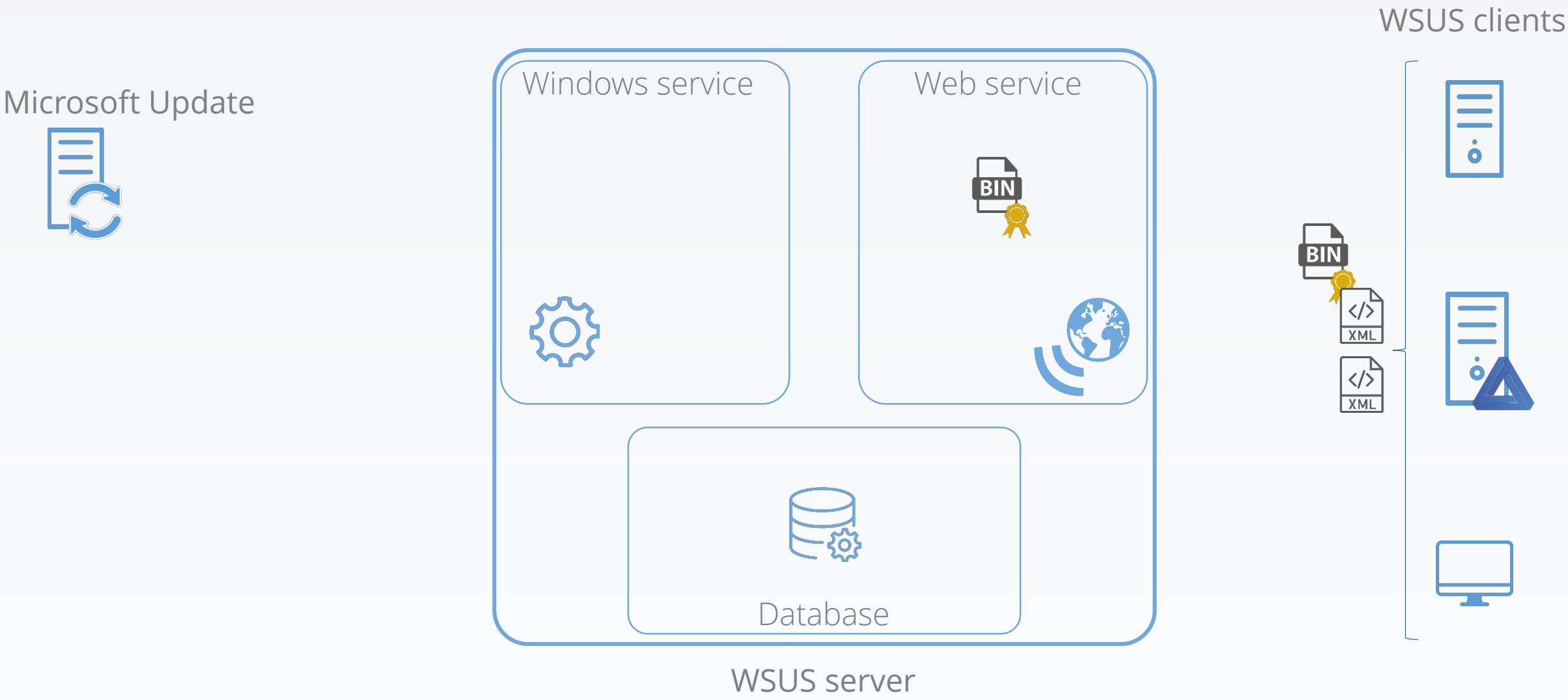
Updates journey within a WSUS server

10. Each client evaluates if the updates is installable



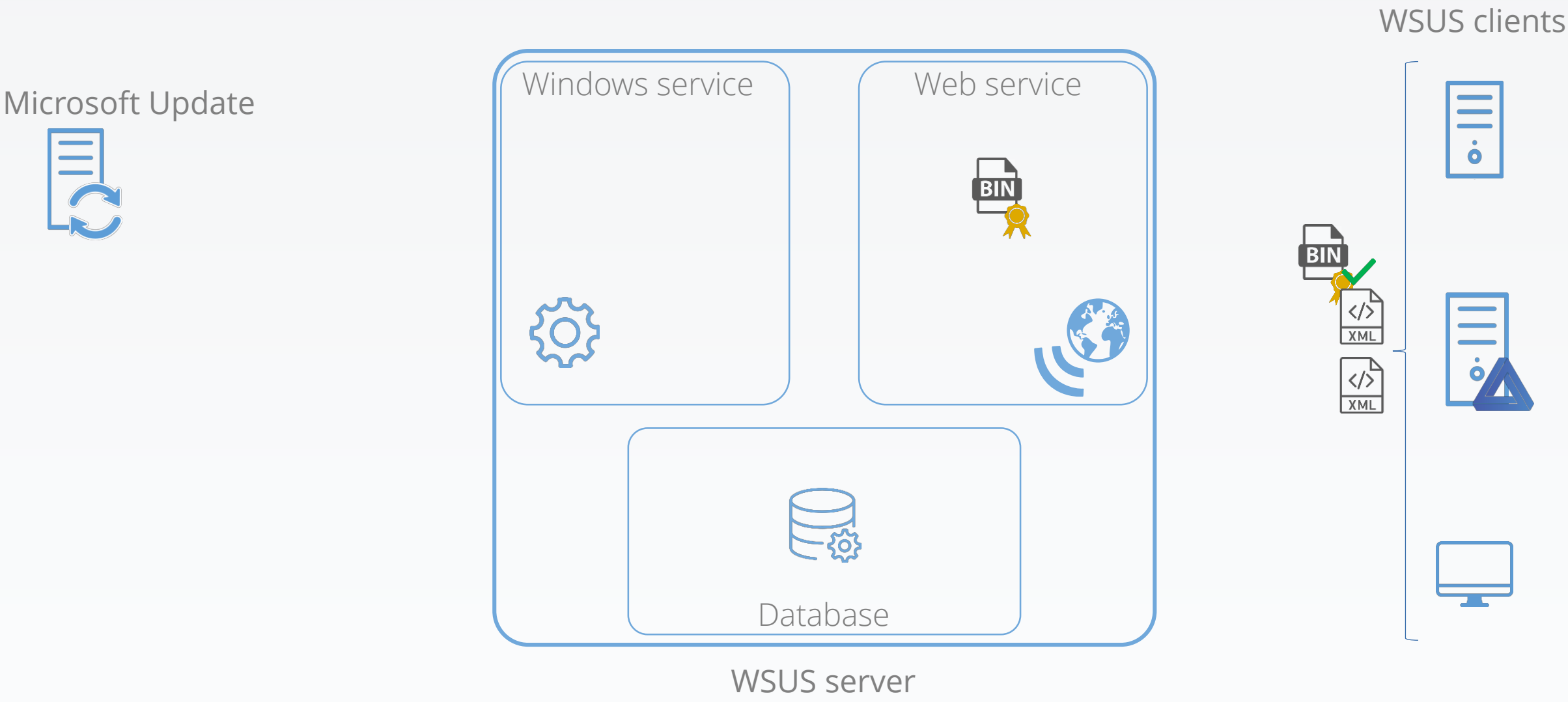
Updates journey within a WSUS server

11. If an update is installable on a client, the associated binary is downloaded



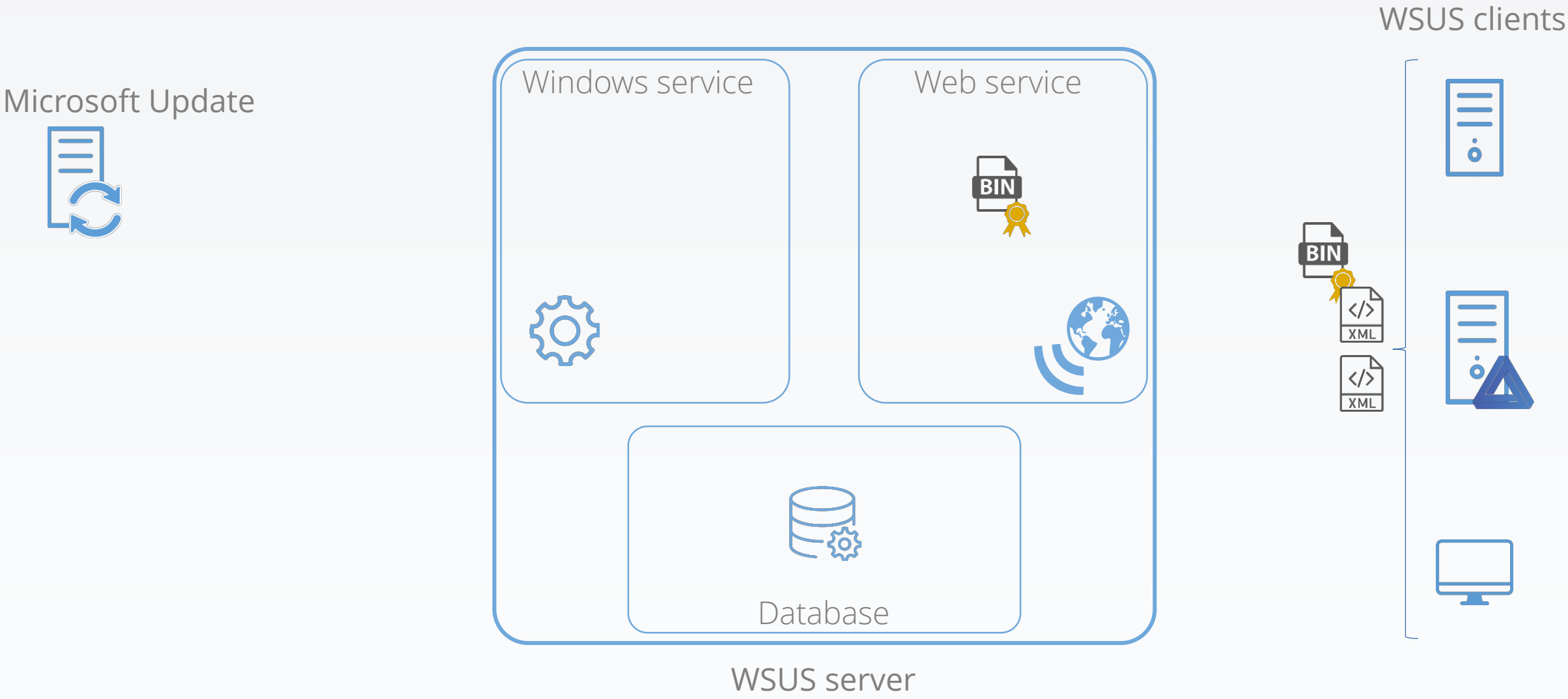
Updates journey within a WSUS server

12. Each downloaded binary's signature is checked

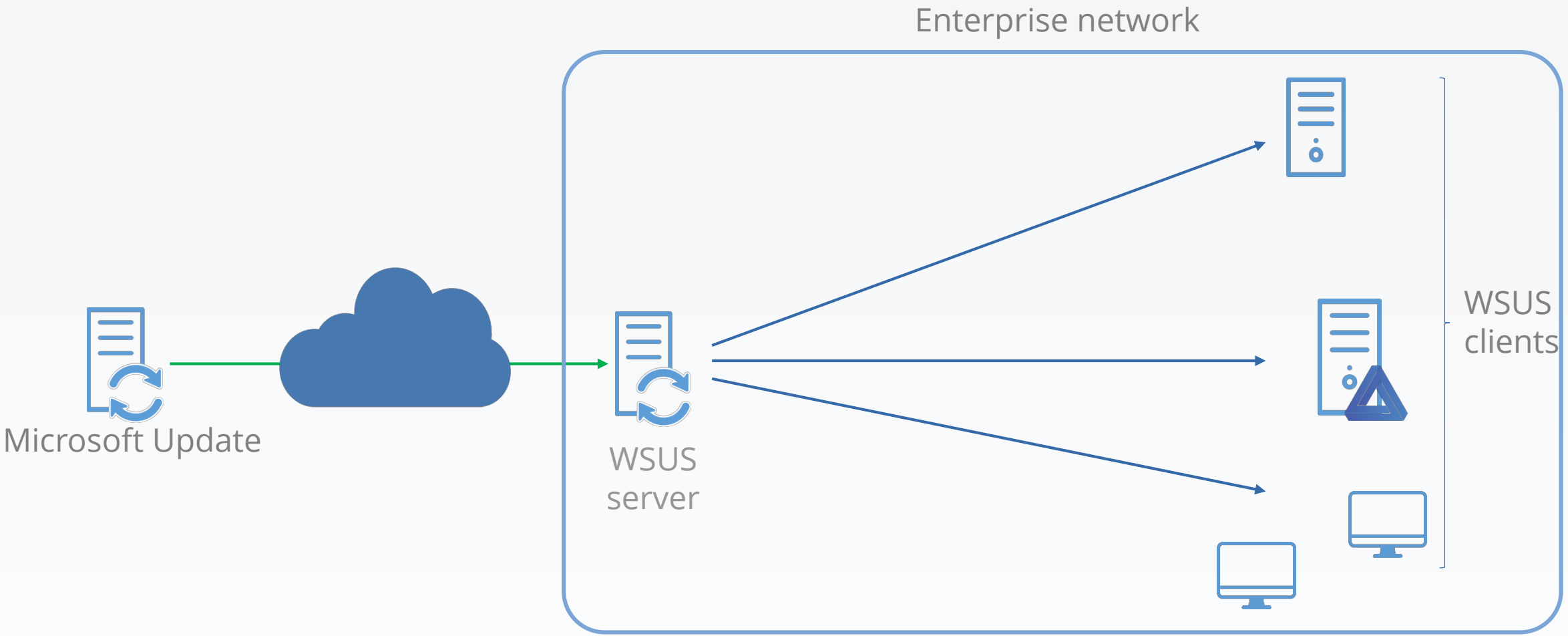


Updates journey within a WSUS server

13. Each binary is executed, with SYSTEM privileges, with possible command line parameters from the metadata

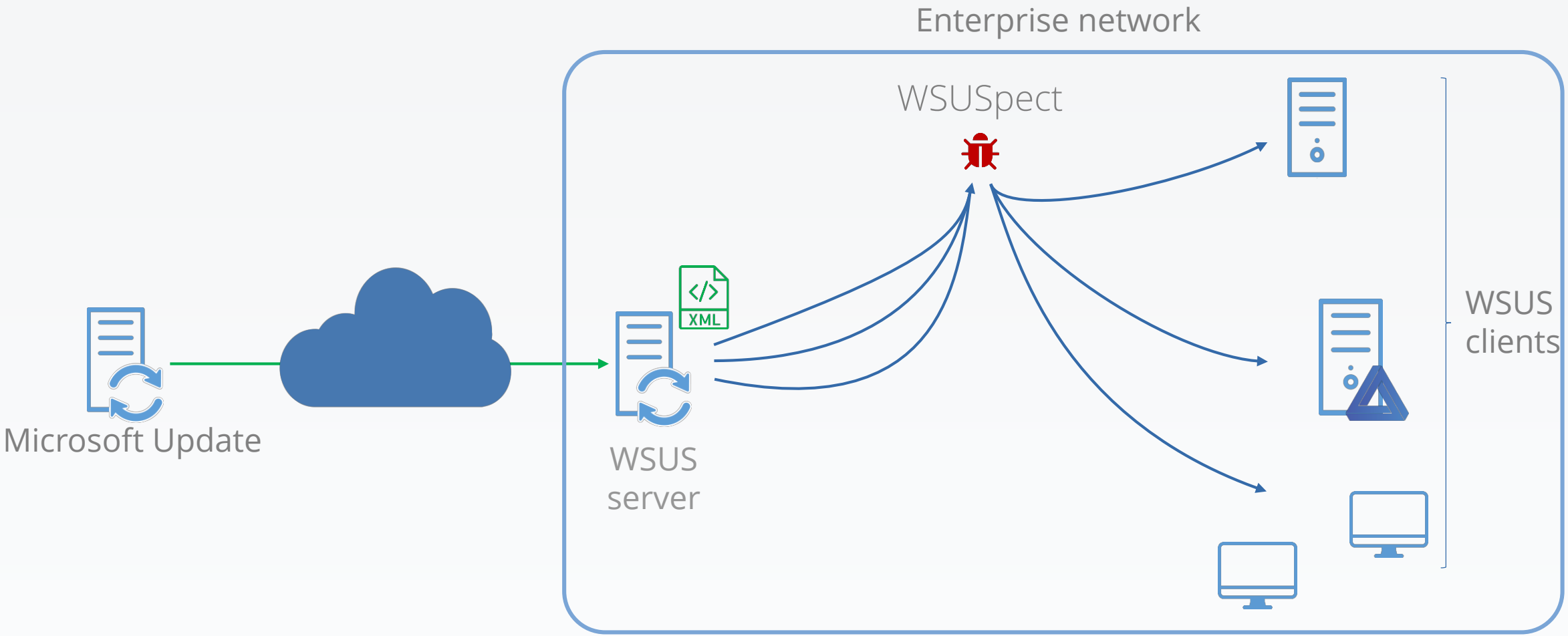


WSUS attacks: Black Hat USA 2015, WSUSpect



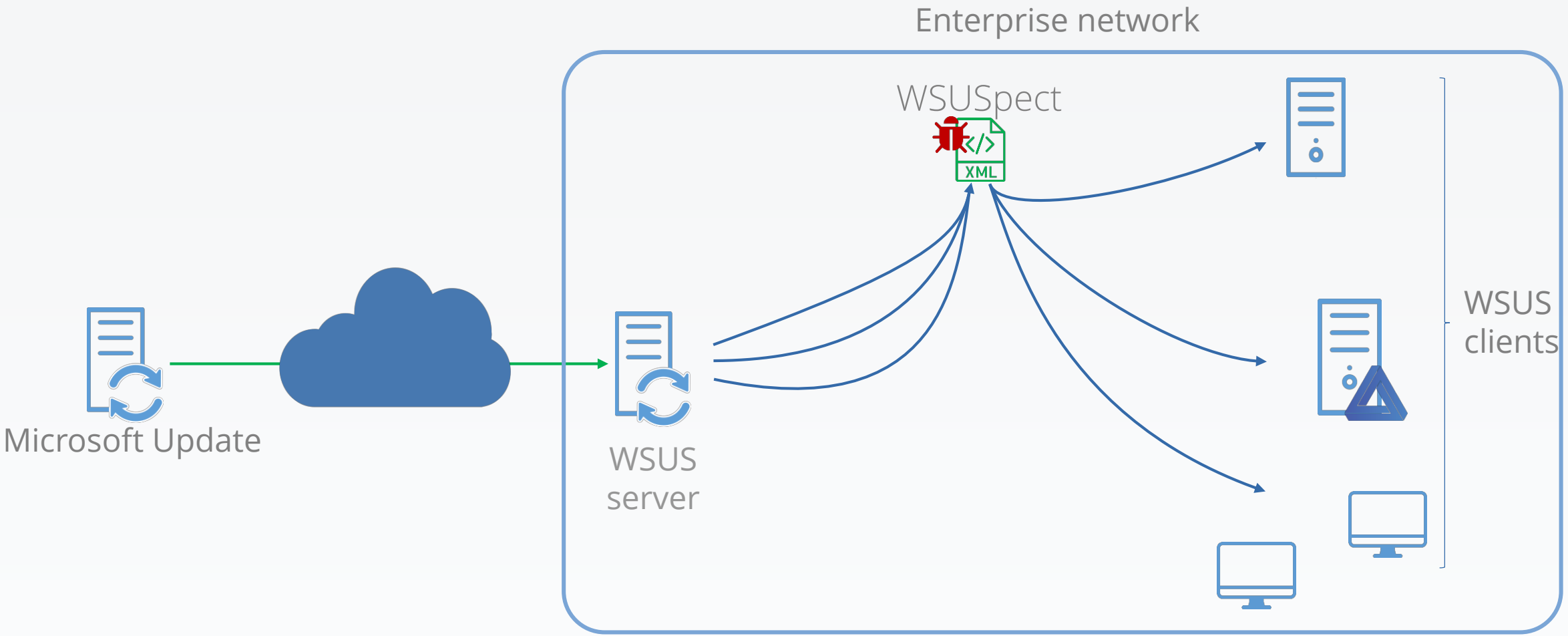
State-of-the-art

1. Get a mitm position



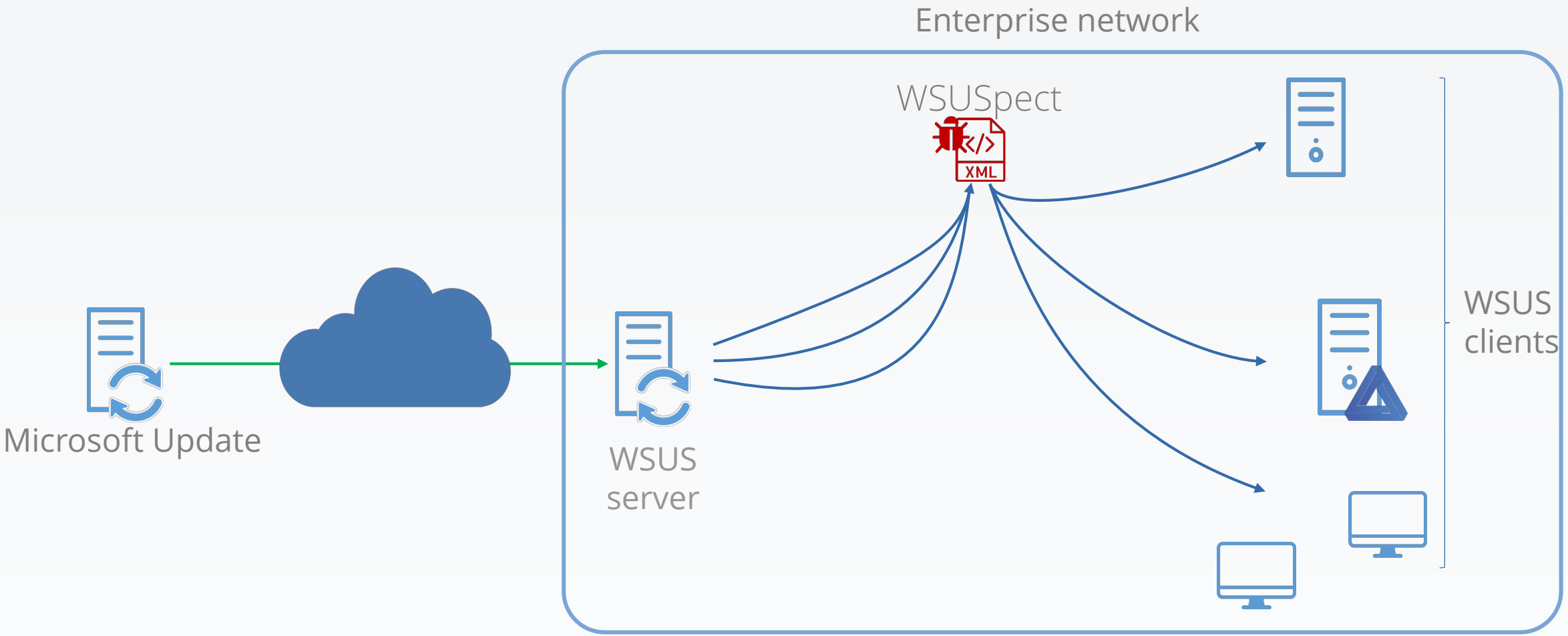
State-of-the-art

2. Intercepts new update queries



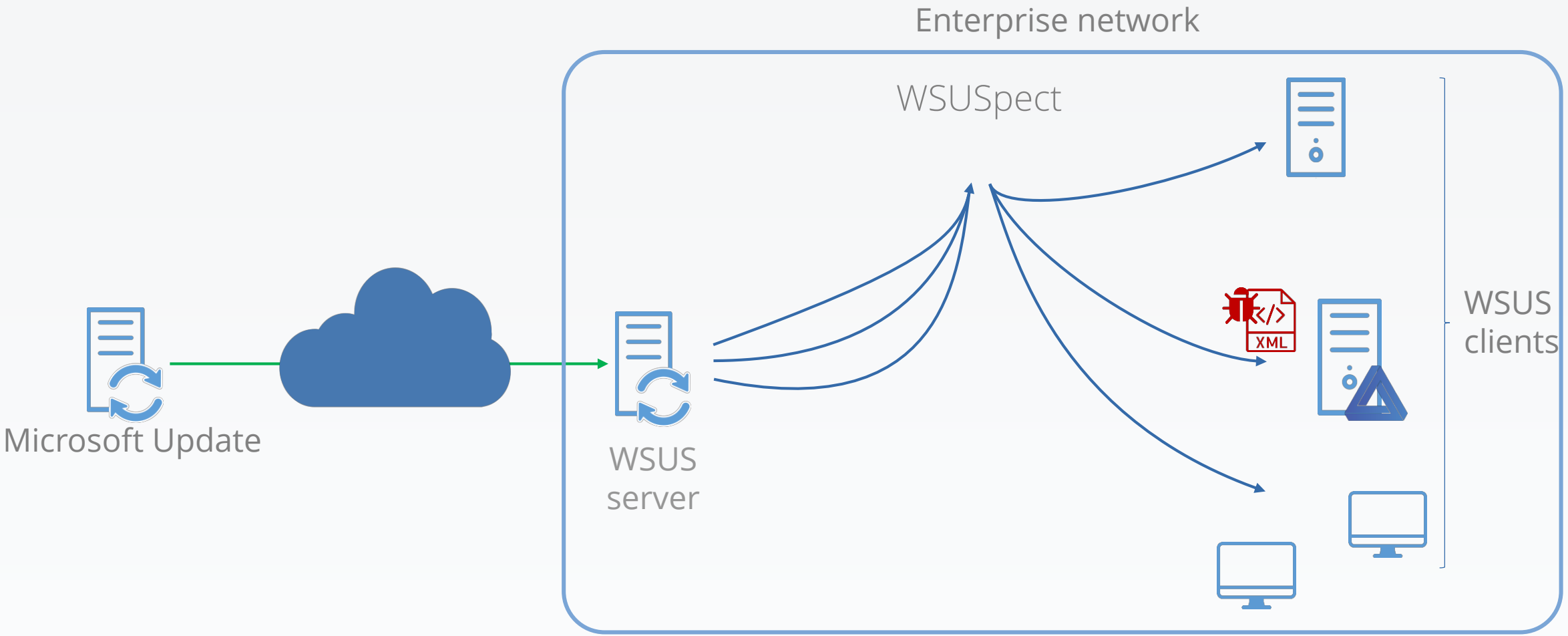
State-of-the-art

3. Infects the on-network metadata with a new, malicious update



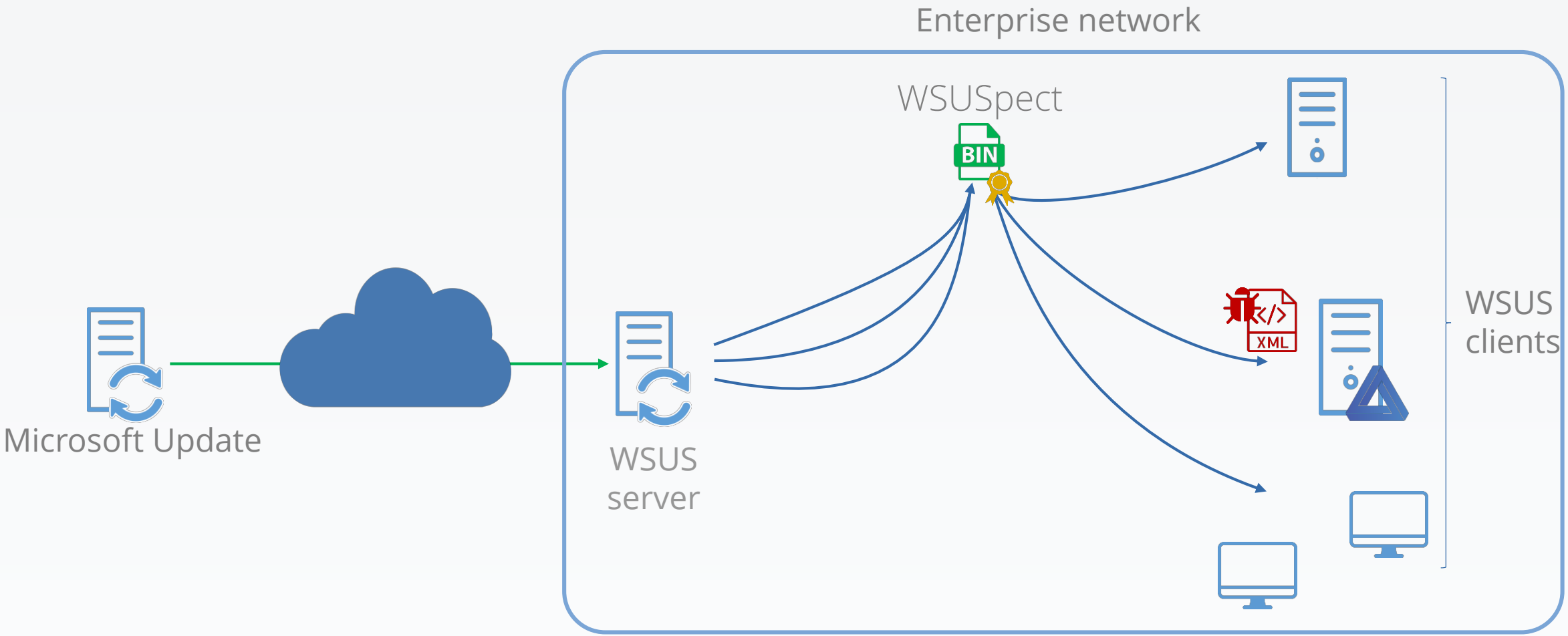
State-of-the-art

4. The client sees a new available and installable update



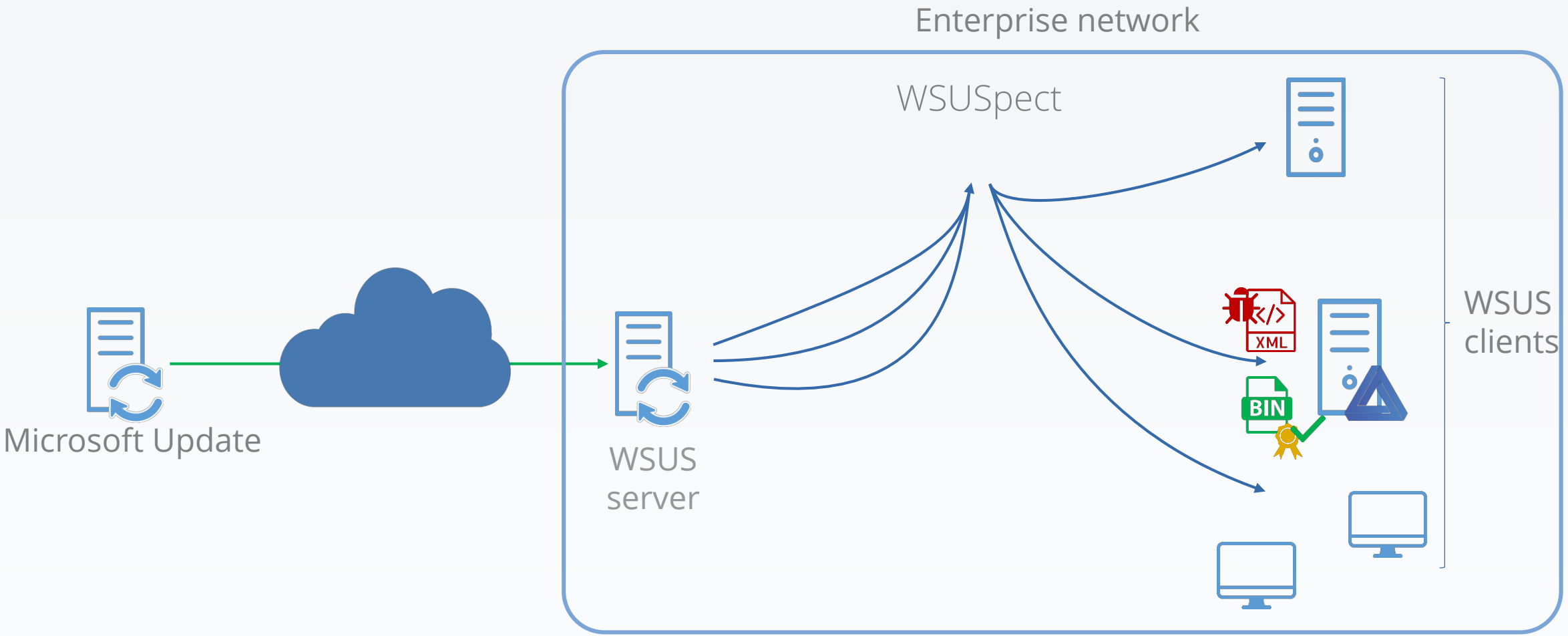
State-of-the-art

5. Fetches the related binary

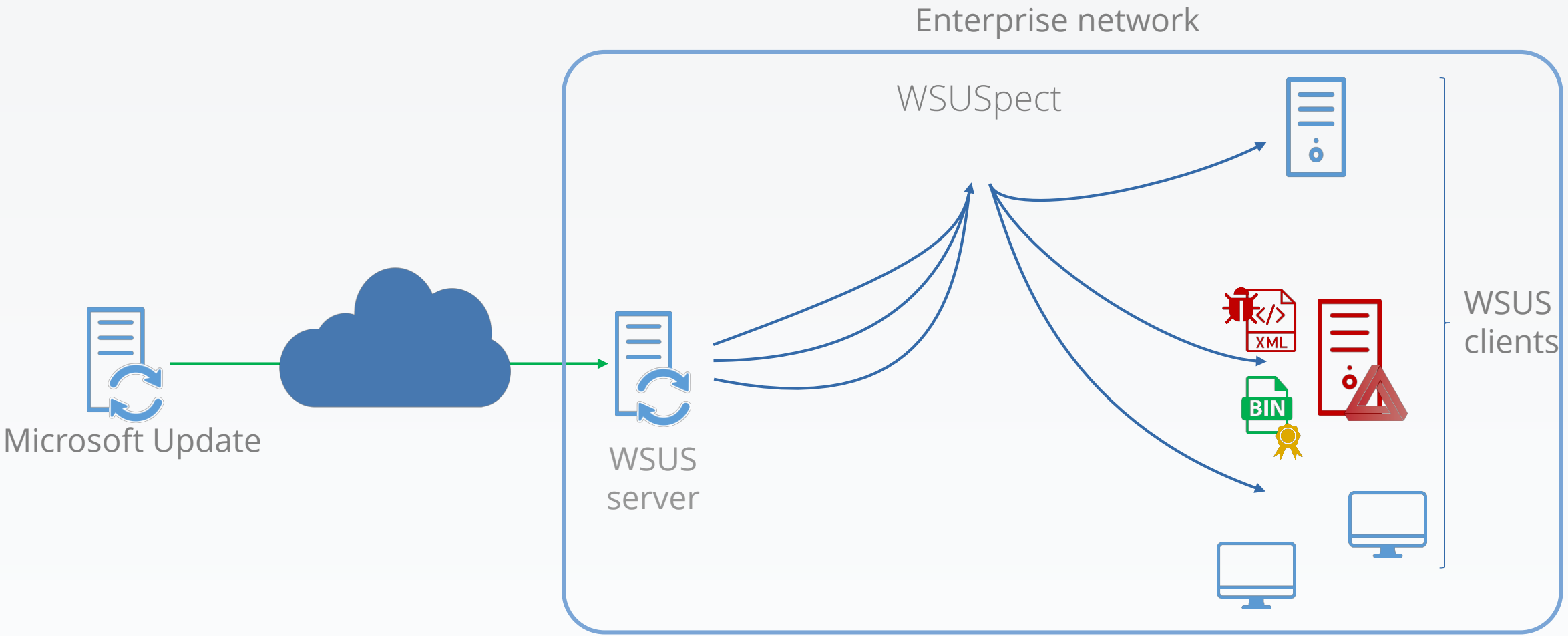


State-of-the-art

6. Checks if binary signature is okay: it is.



7. Installs the binary, with SYSTEM privileges, with metadata command-line arguments



WSUS attacks: Black Hat USA 2015, WSUSpect

Awesome attack!

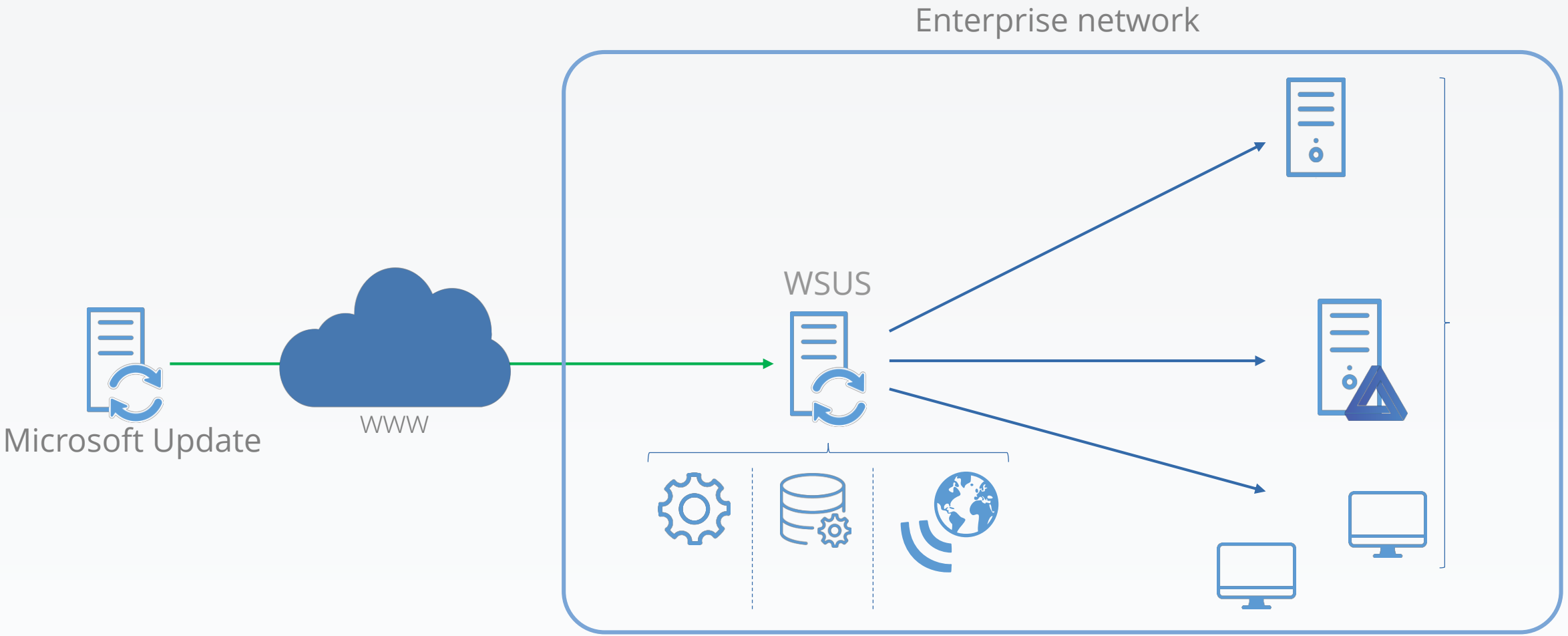
But some limitations:

- Gain a mitm position
  - Meaning no network limitation is in place
- Get a useful one
  - Meaning TLS has to be disabled

➡ Doesn't give us access to the disconnected network ☹

Introducing WSUSpendu[@]

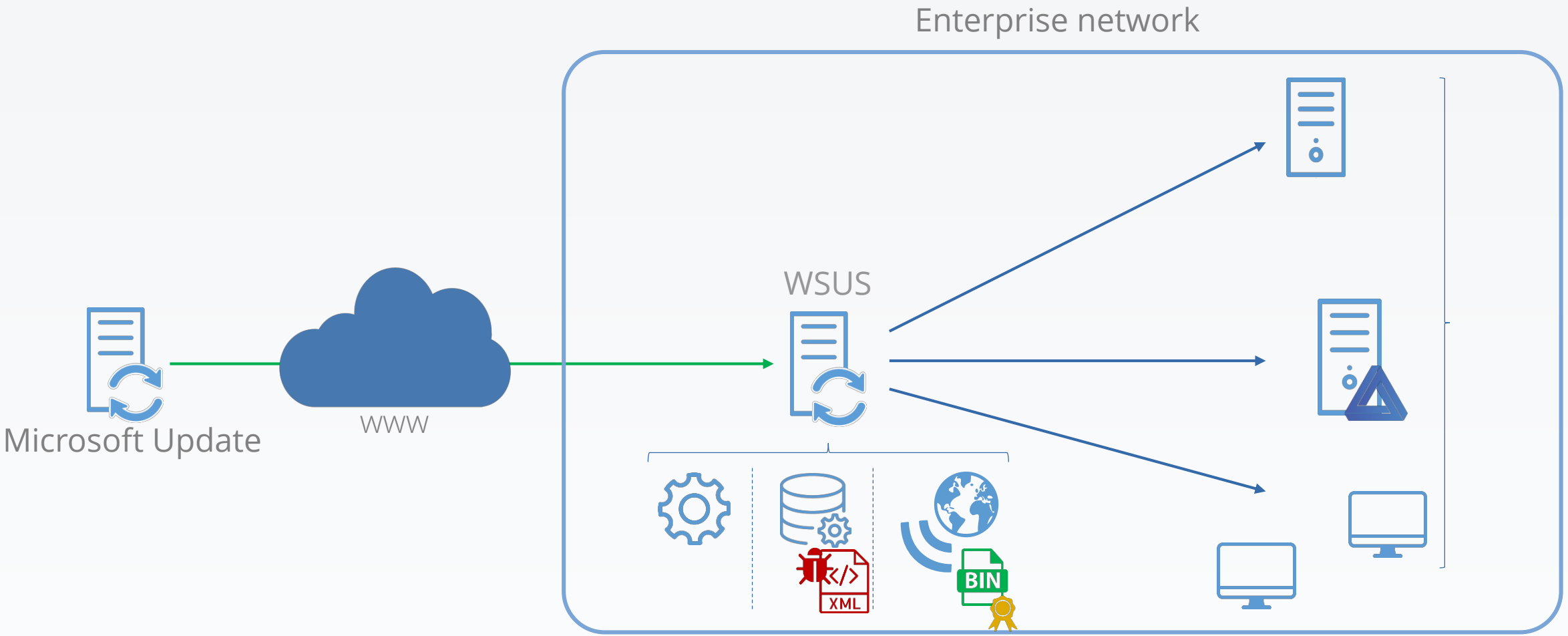
Open-source: https://github.com/AlsidOfficial/WSUSpendu



[@] Thx Maman

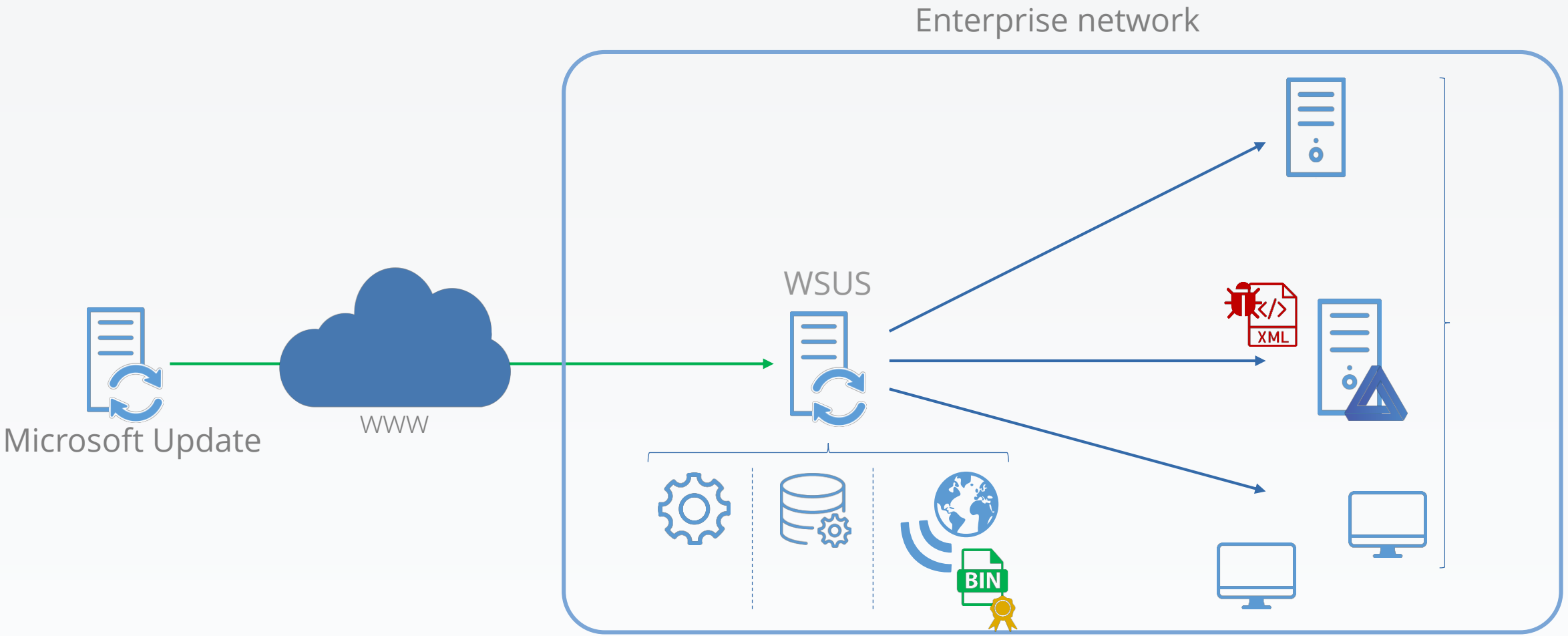
Introducing WSUSpendu

1. Injects update metadata in the database, signed binary in the Web service



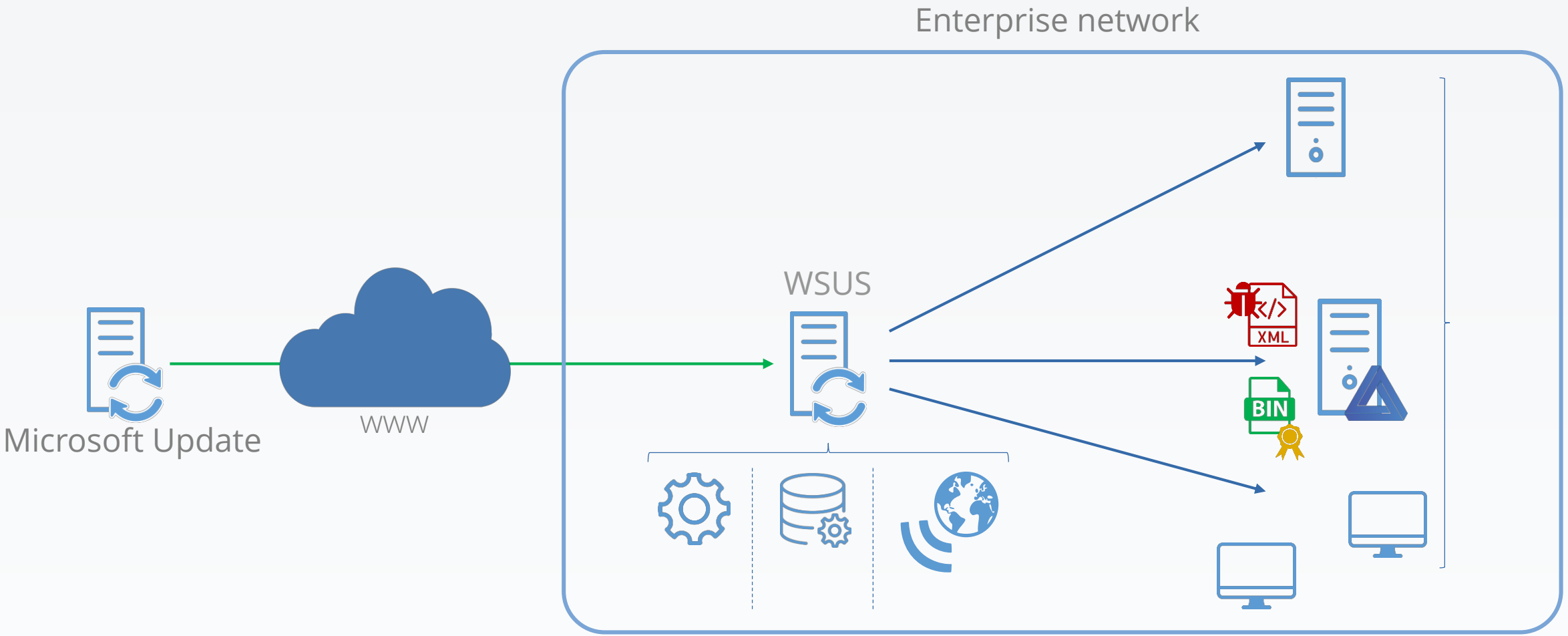
Introducing WSUSpendu

2. The client sees a new available and installable update



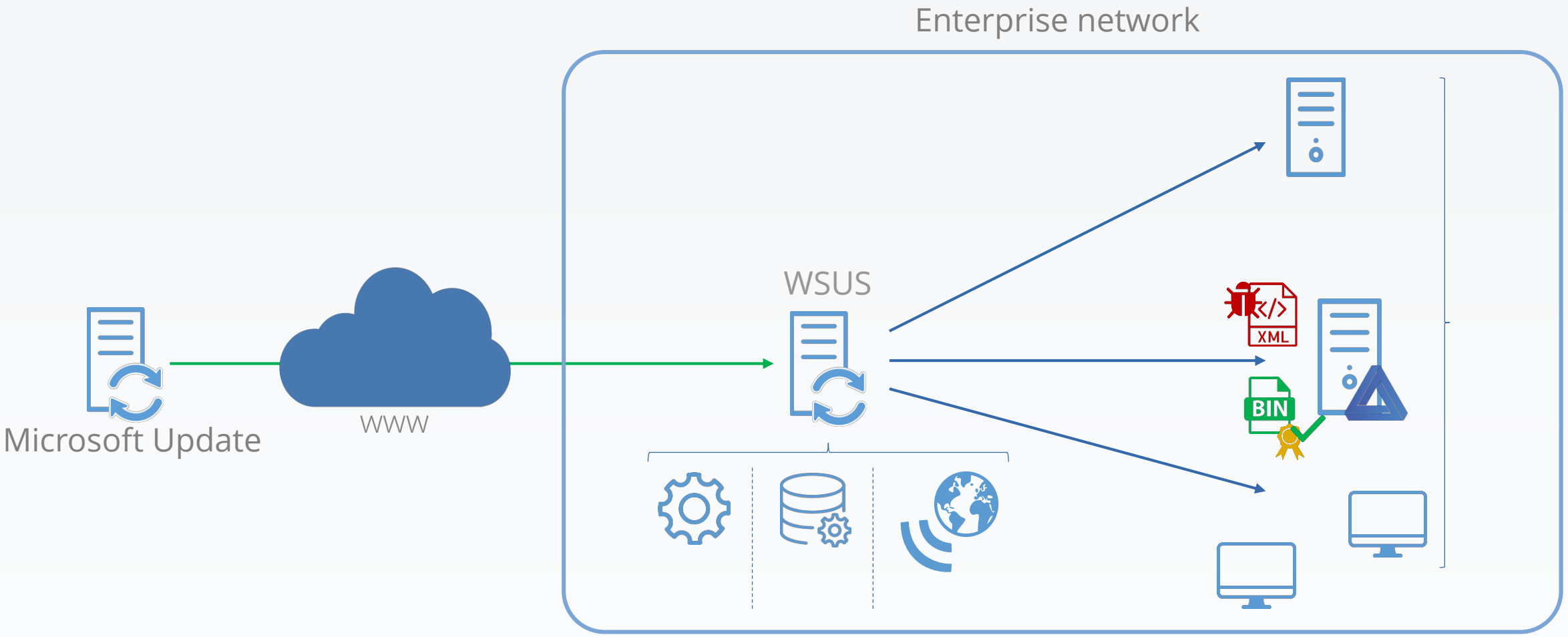
Introducing WSUSpendu

3. Fetches the related binary



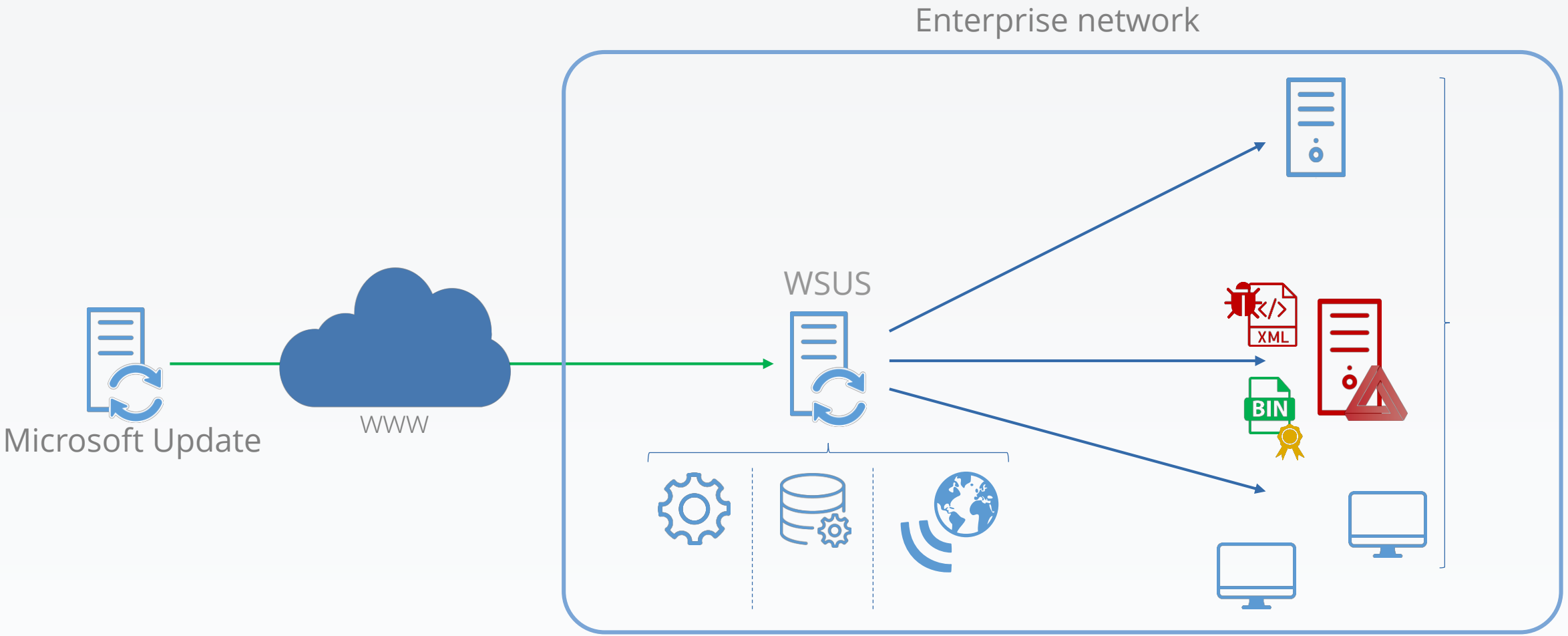
Introducing WSUSpendu

4. Checks if binary signature is okay: it is.



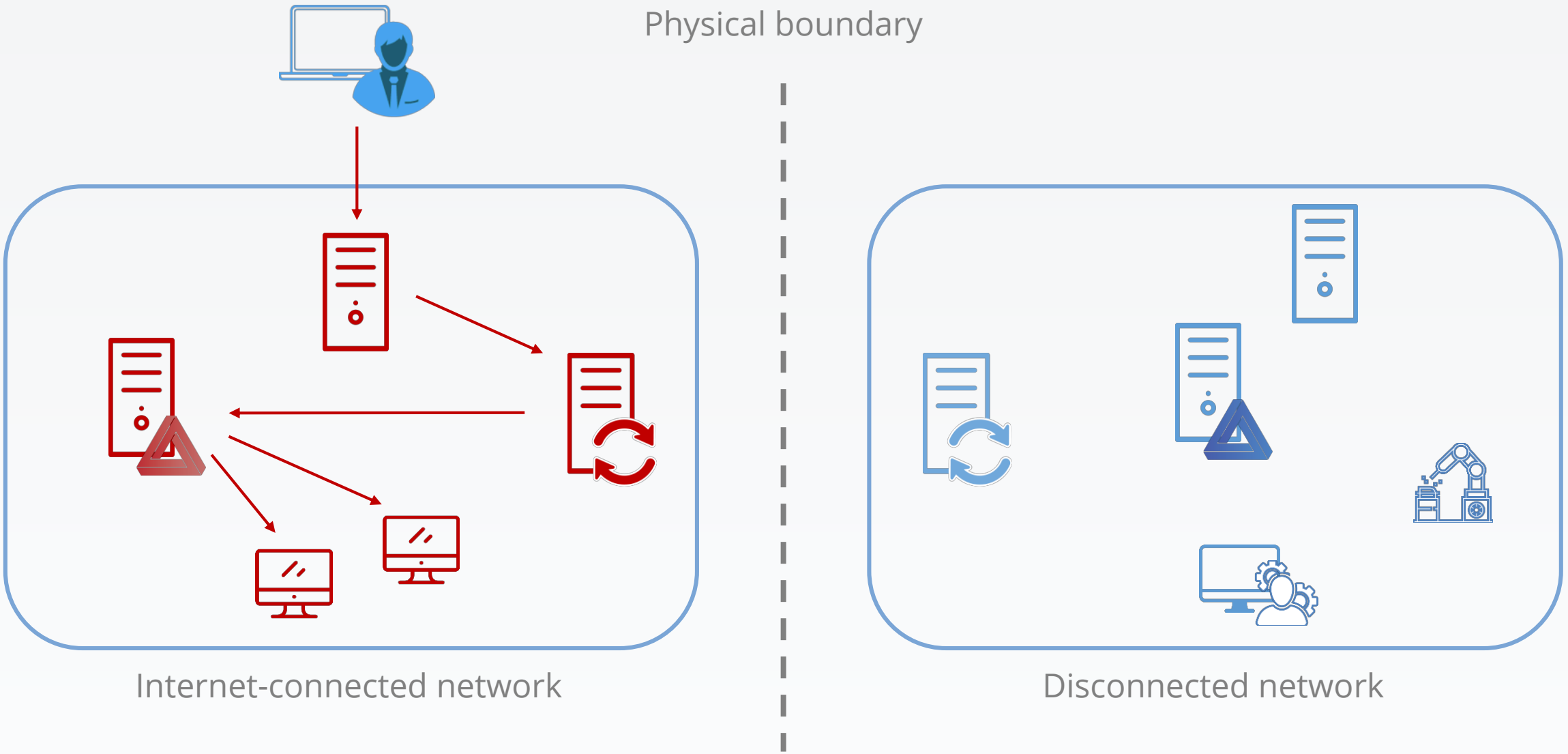
Introducing WSUSpendu

5. Installs the binary, with SYSTEM privileges, with metadata command-line arguments



Demonstration…

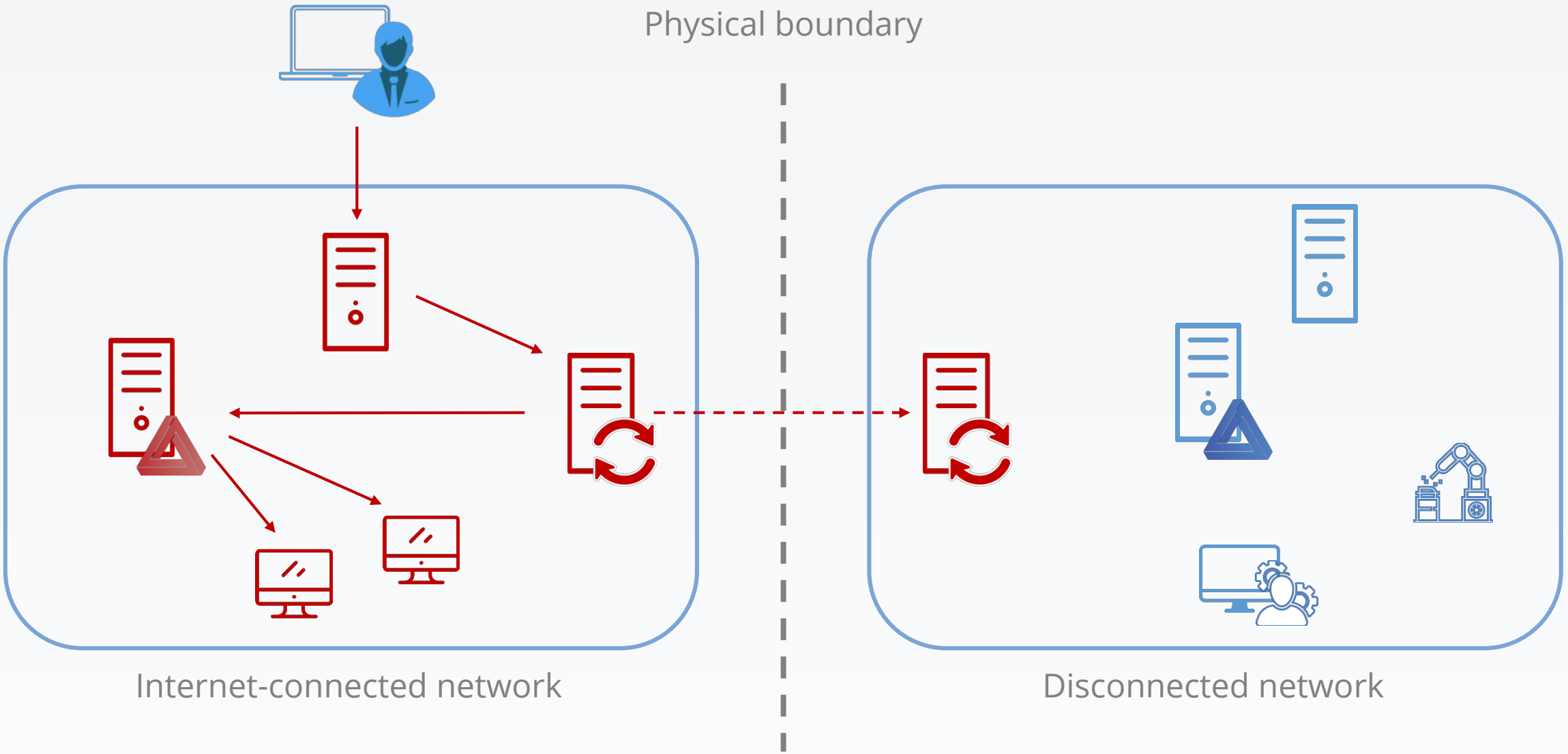
Compromise a connected network



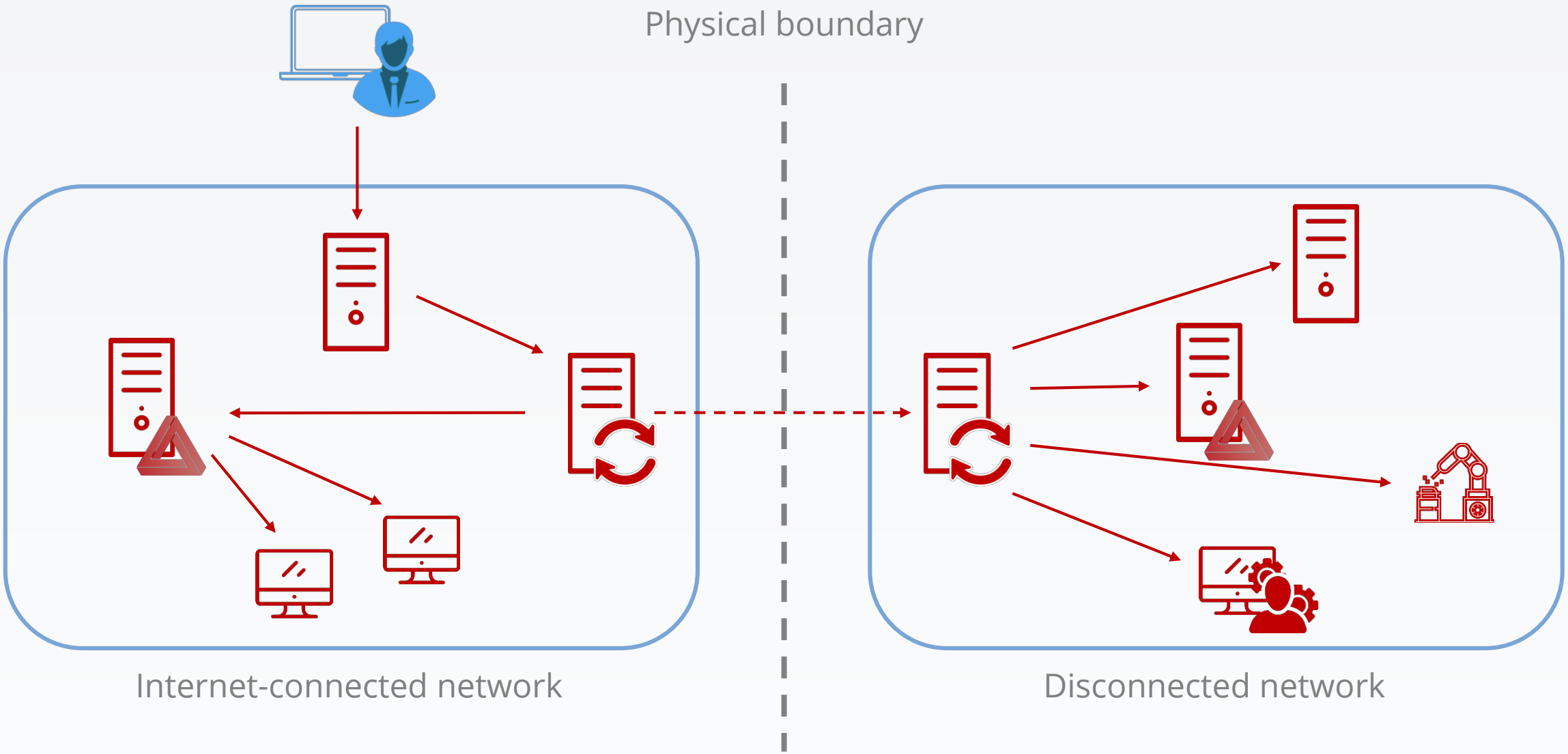
We need to go deeper...

Demonstration…

Compromise a disconnected network



Compromise a disconnected network



Conclusion

~~Stop updating~~ ☺

Control relationship WSUS server → clients

ROMAIN COLTEL

ANSSI

YVES LE PROVOST

Thank you all.