ALSID

ANSSI

Wednesday, 26th 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

How do you compromise an Active Directory domain?

Sample of an Active Directory domain

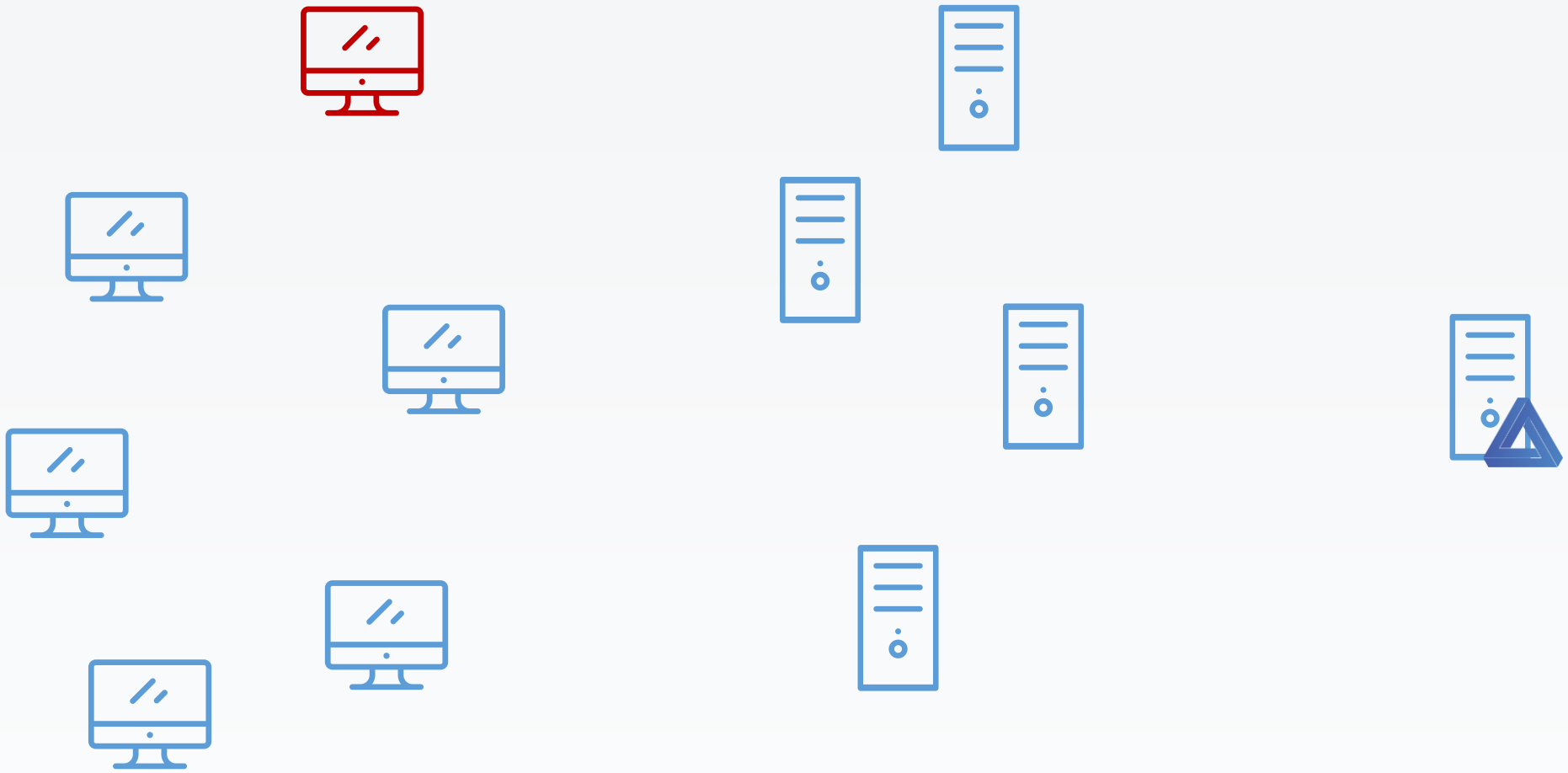
Users workstations

Servers

Domain controllers

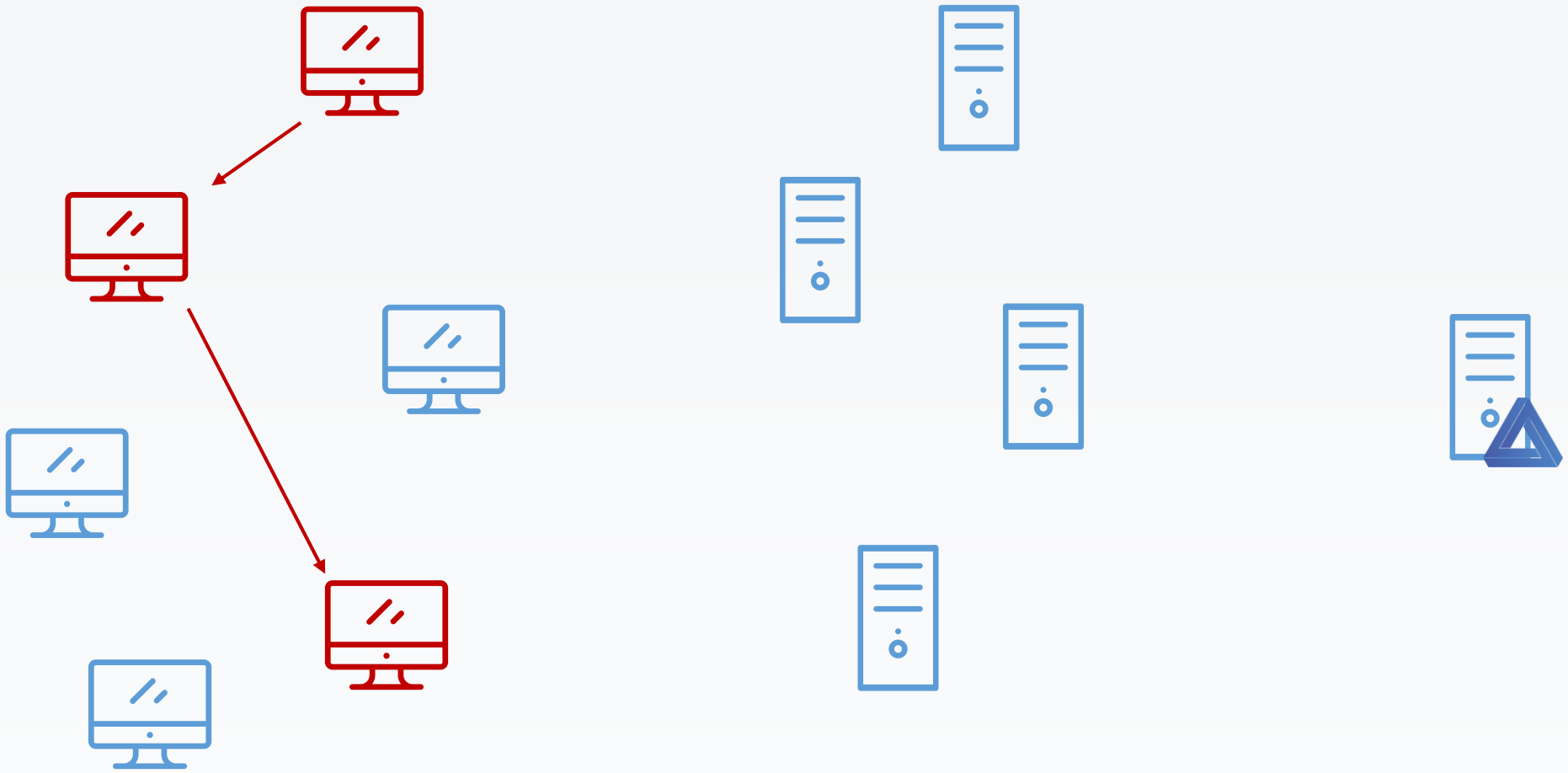
First step

1. Targeted phishing email, with malware: get a foothold in the network



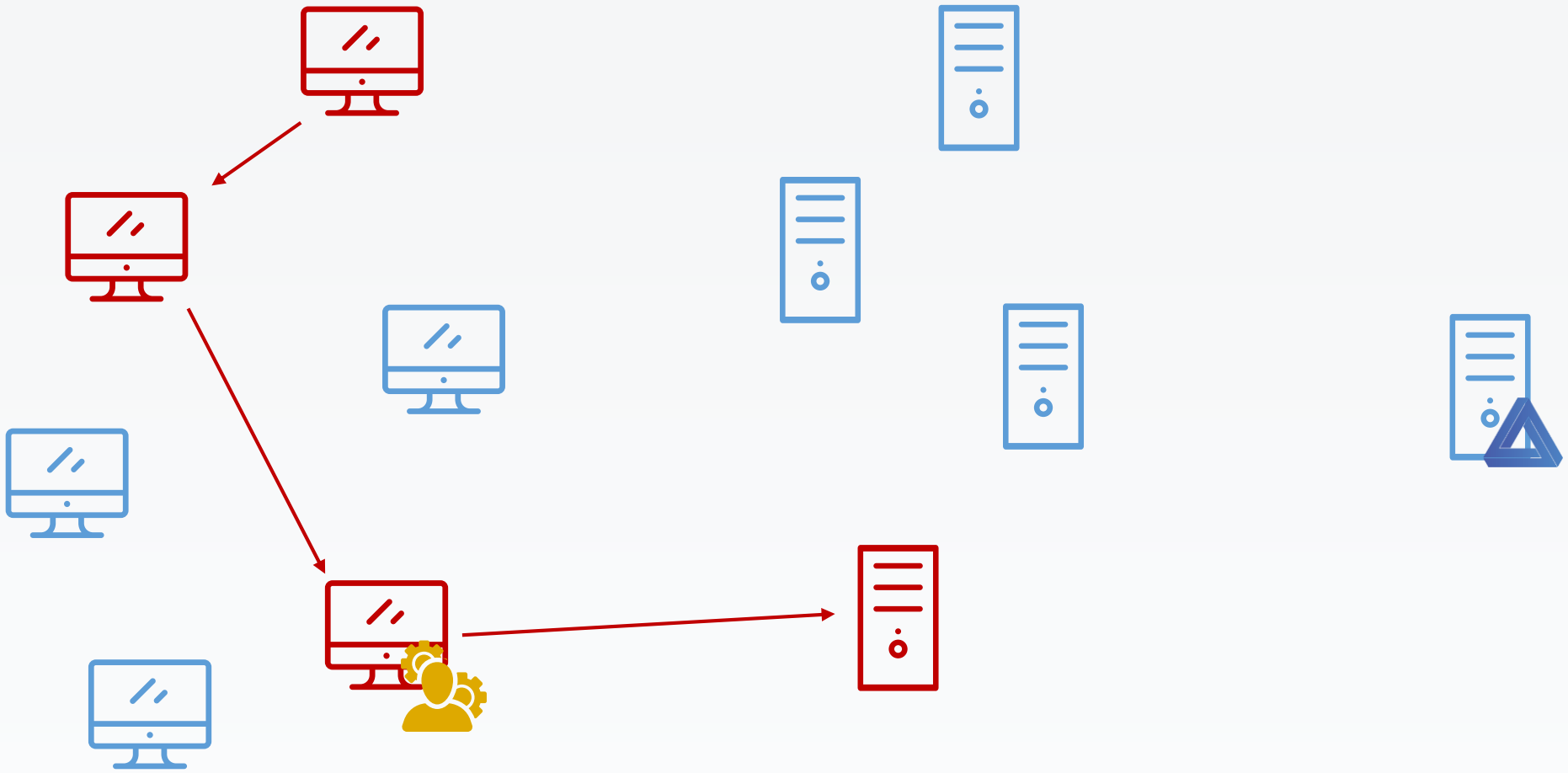
Next step

2. Propagate compromise between workstations until…



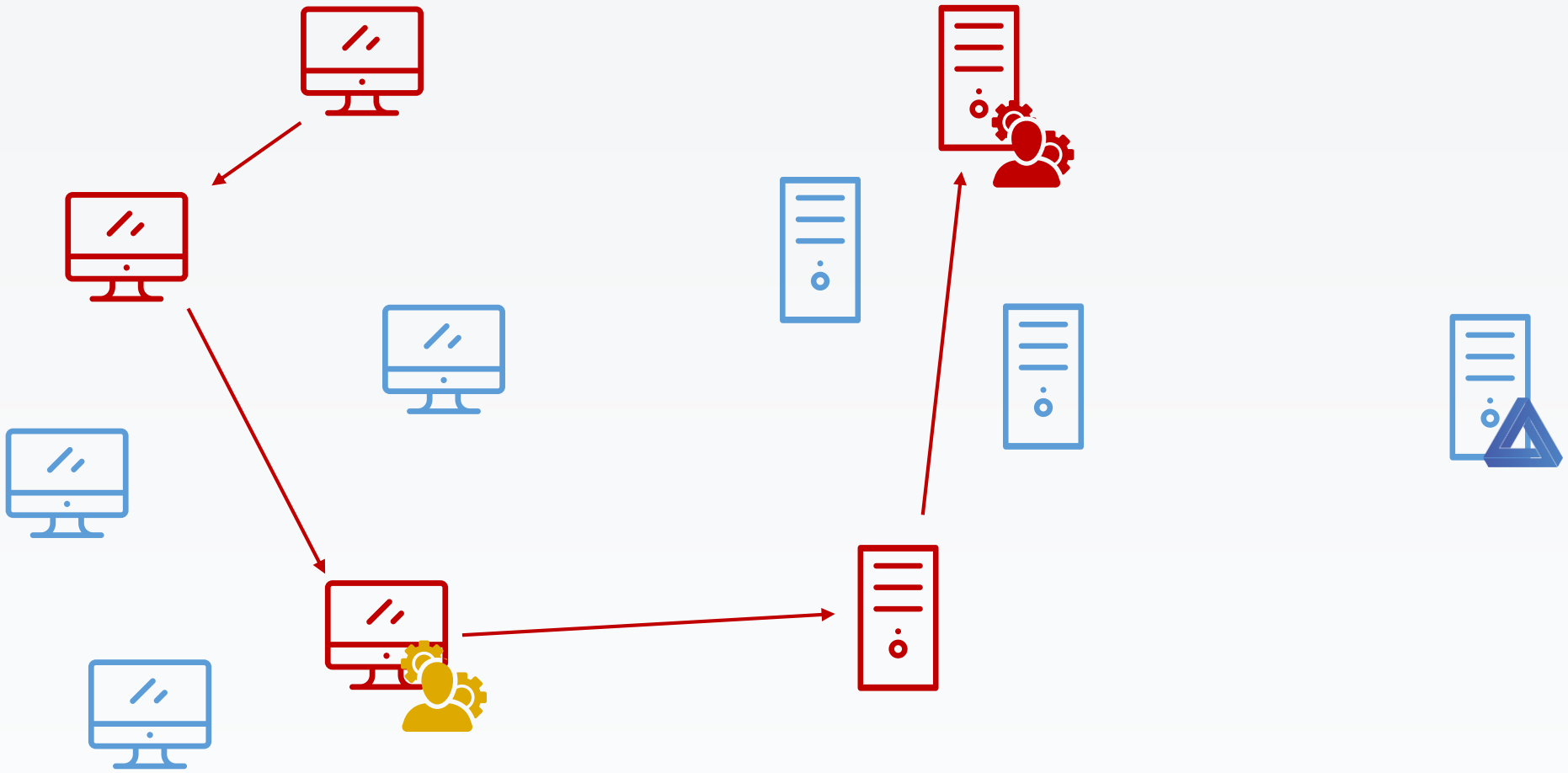
Next step

3. You get a server administrative account, and use it to continue propagation…



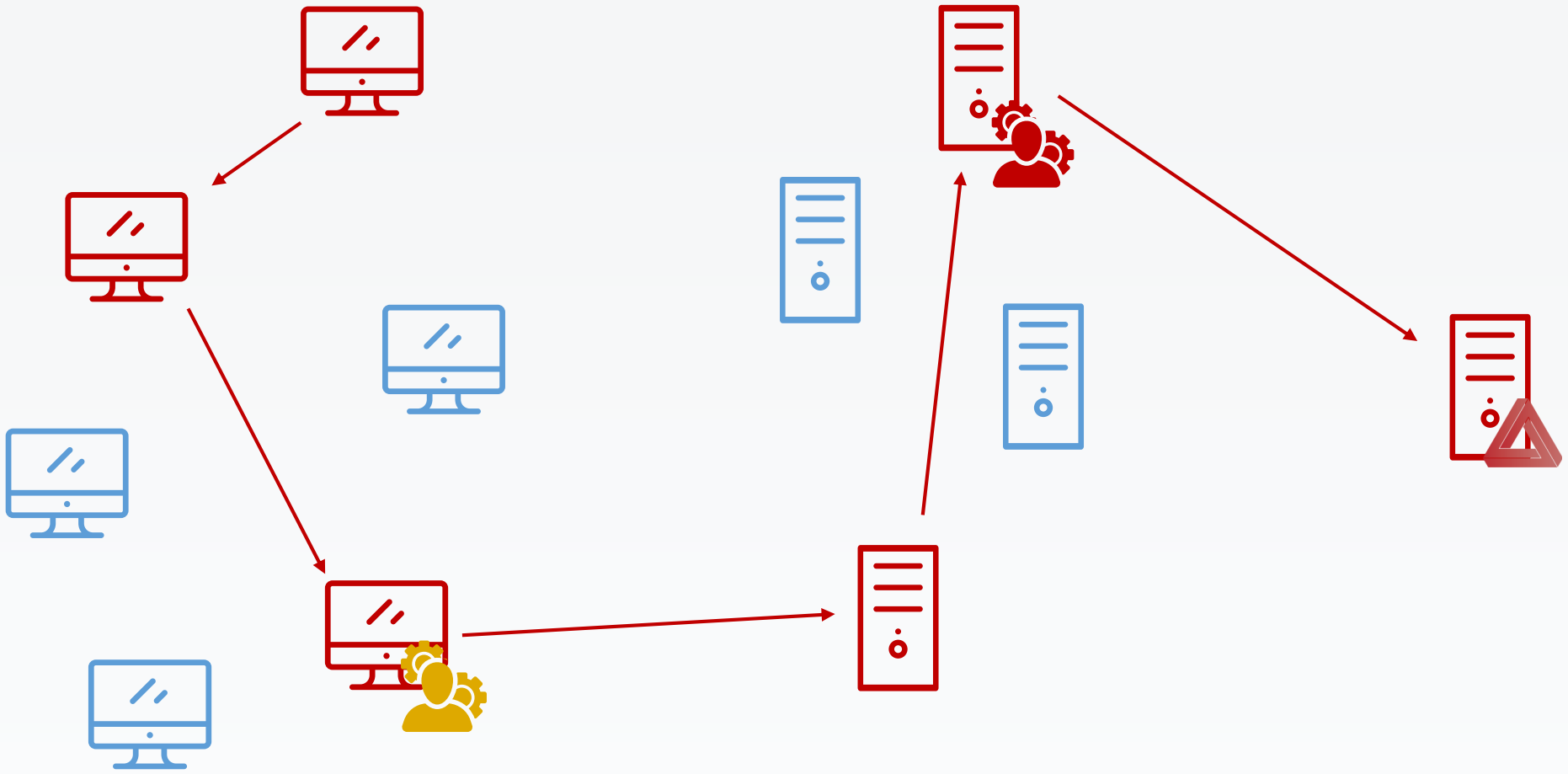
Next step

4. Until you get an Active Directory administrative account



Next step

5. Get domain secrets



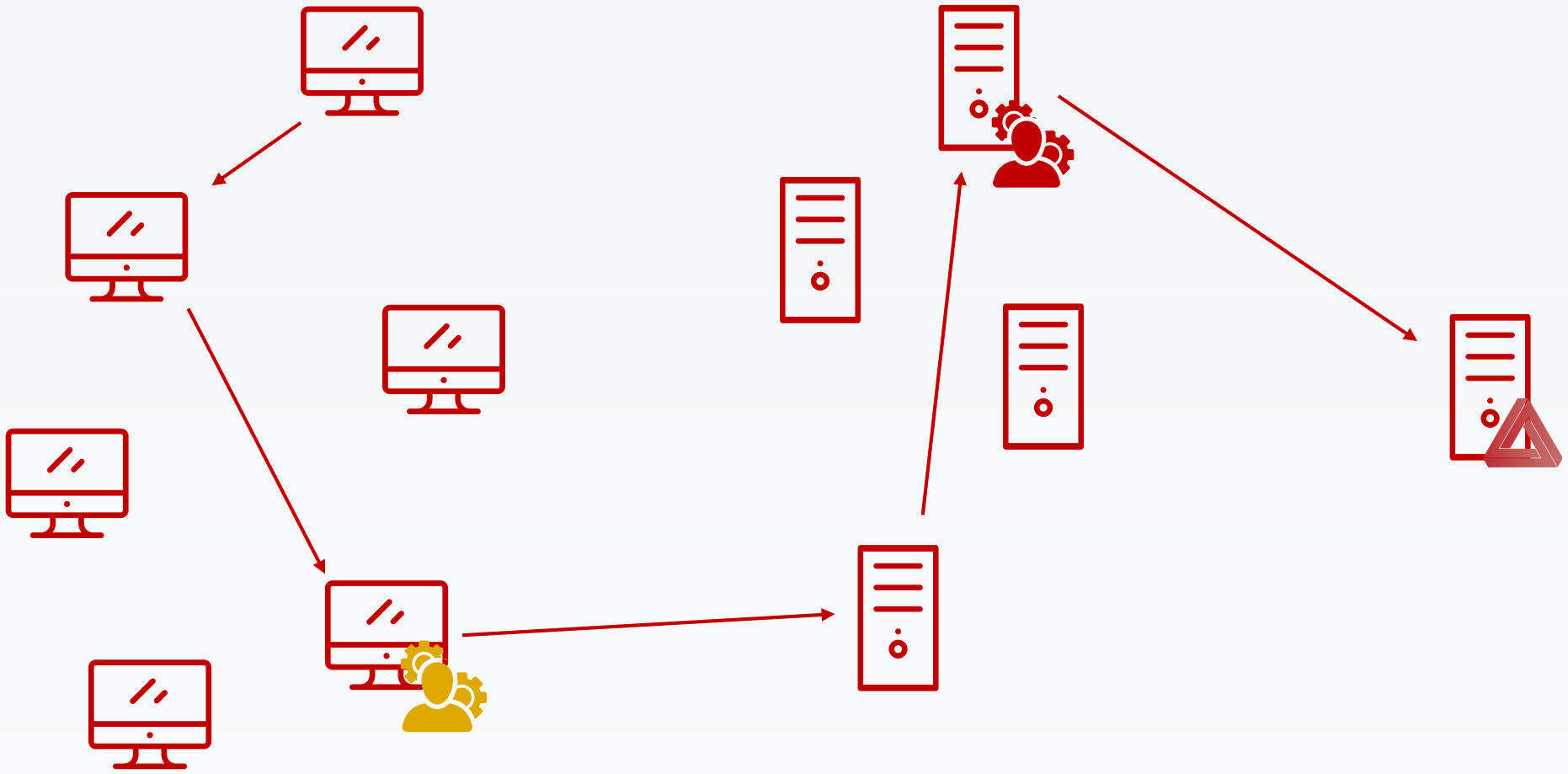
Users workstations

Servers

Domain controllers

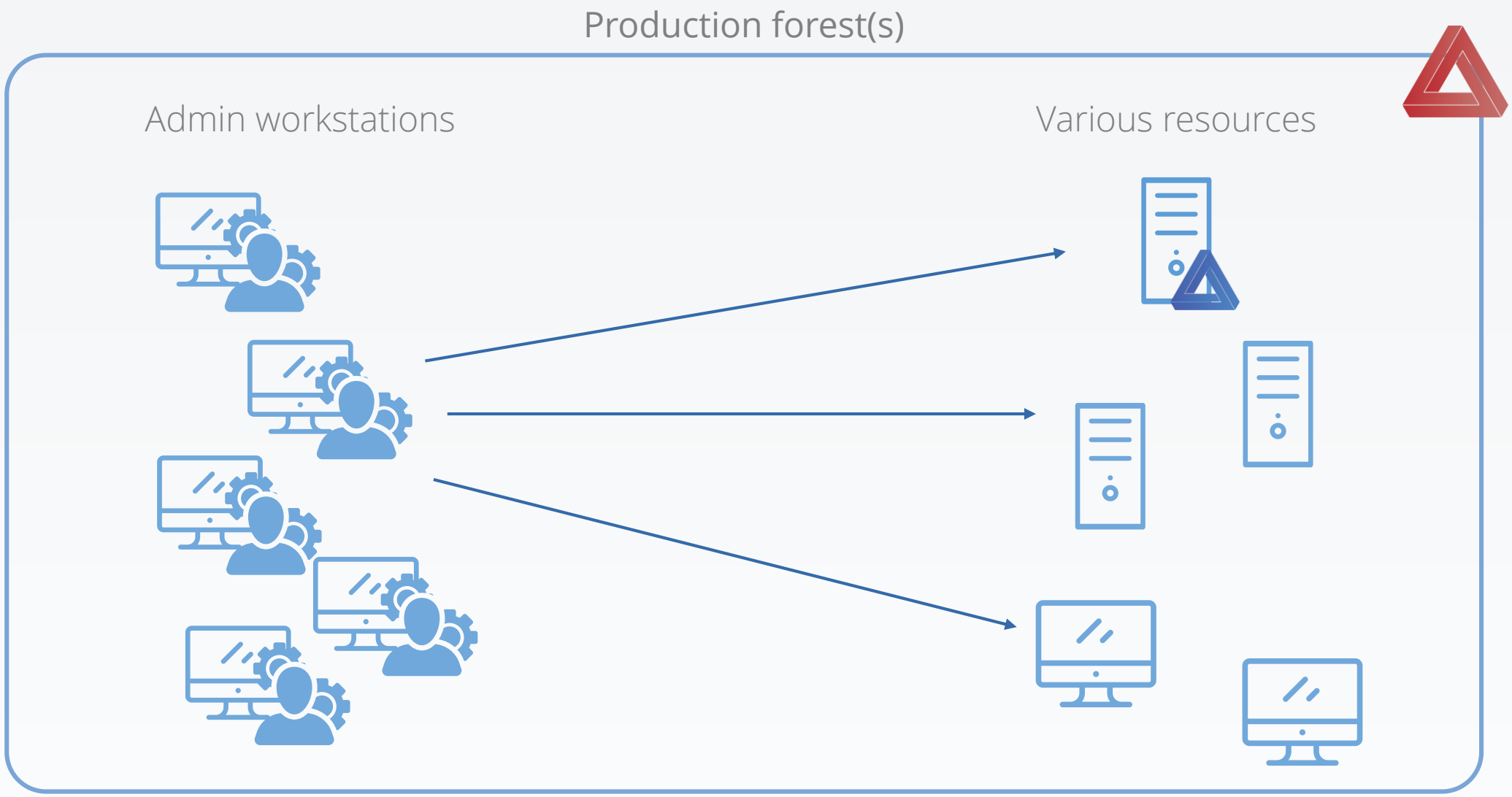
Game over

6. Use secrets to access all data

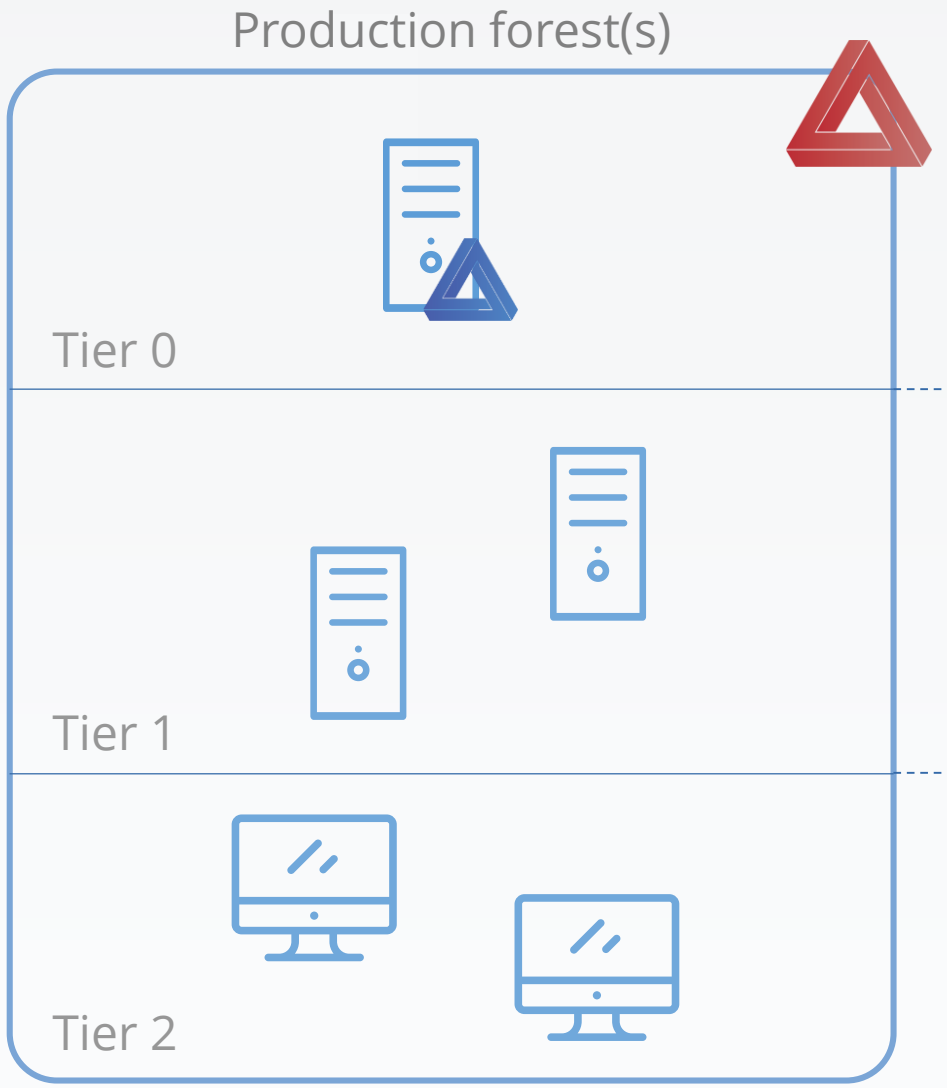


How do you compromise an ESAE-managed forest?

Classic administration



Tier administration model

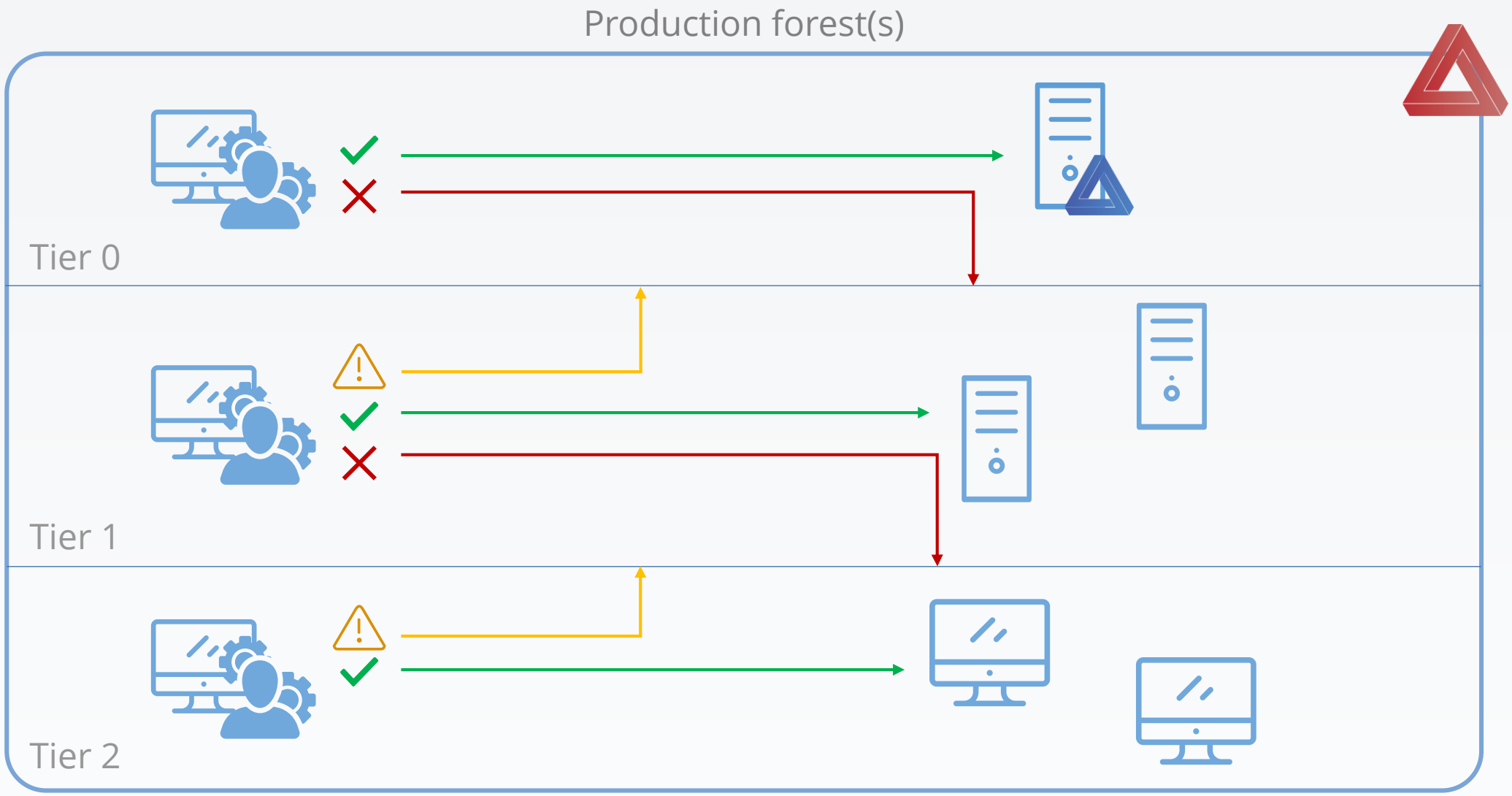


Control of enterprise identities in the environment

Control of enterprise servers and applications

Control of user workstations and devices

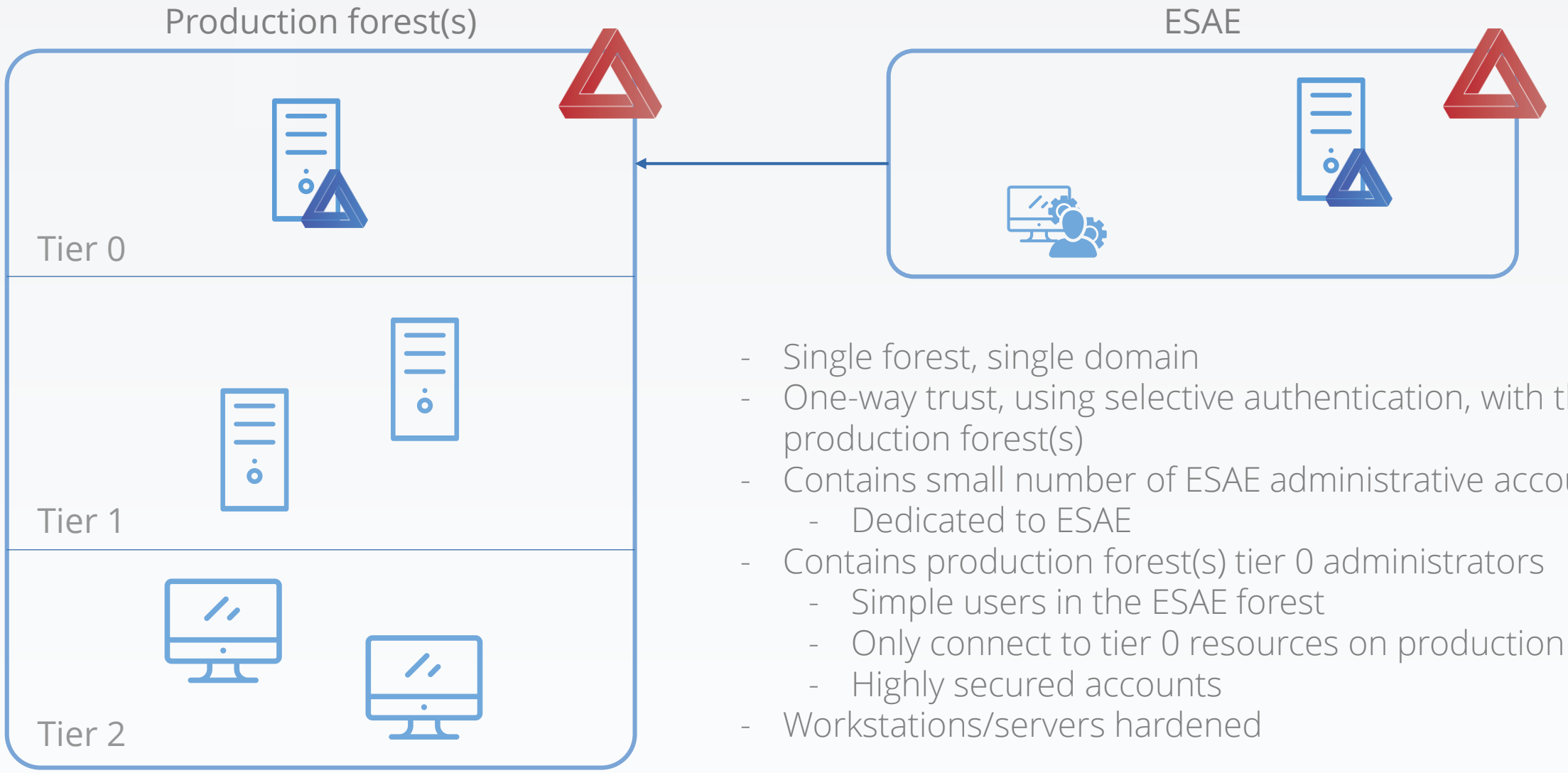
Better administration



Reference: https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

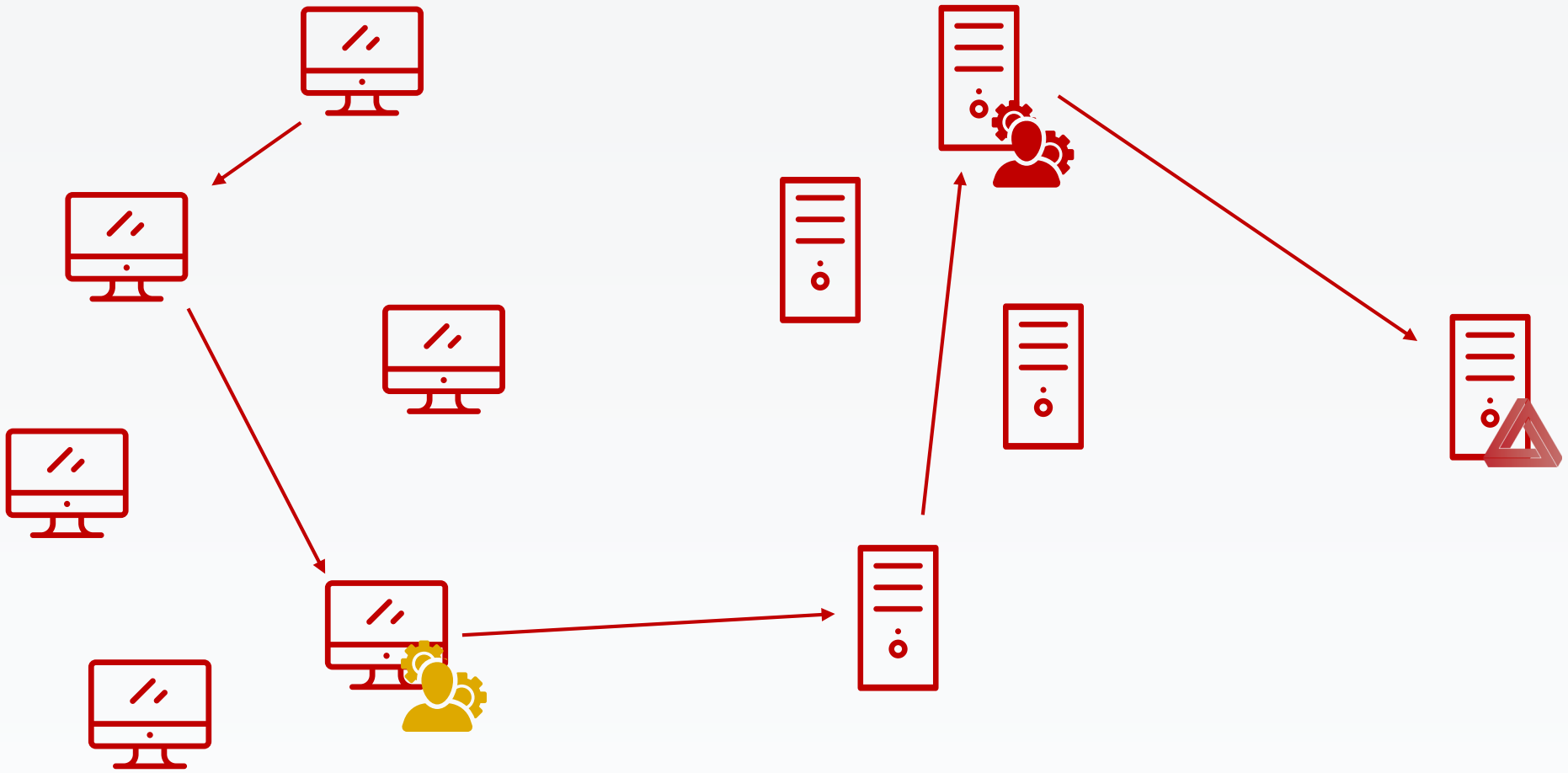
So, what is an ESAE?

Enhanced Security Administrative Environment

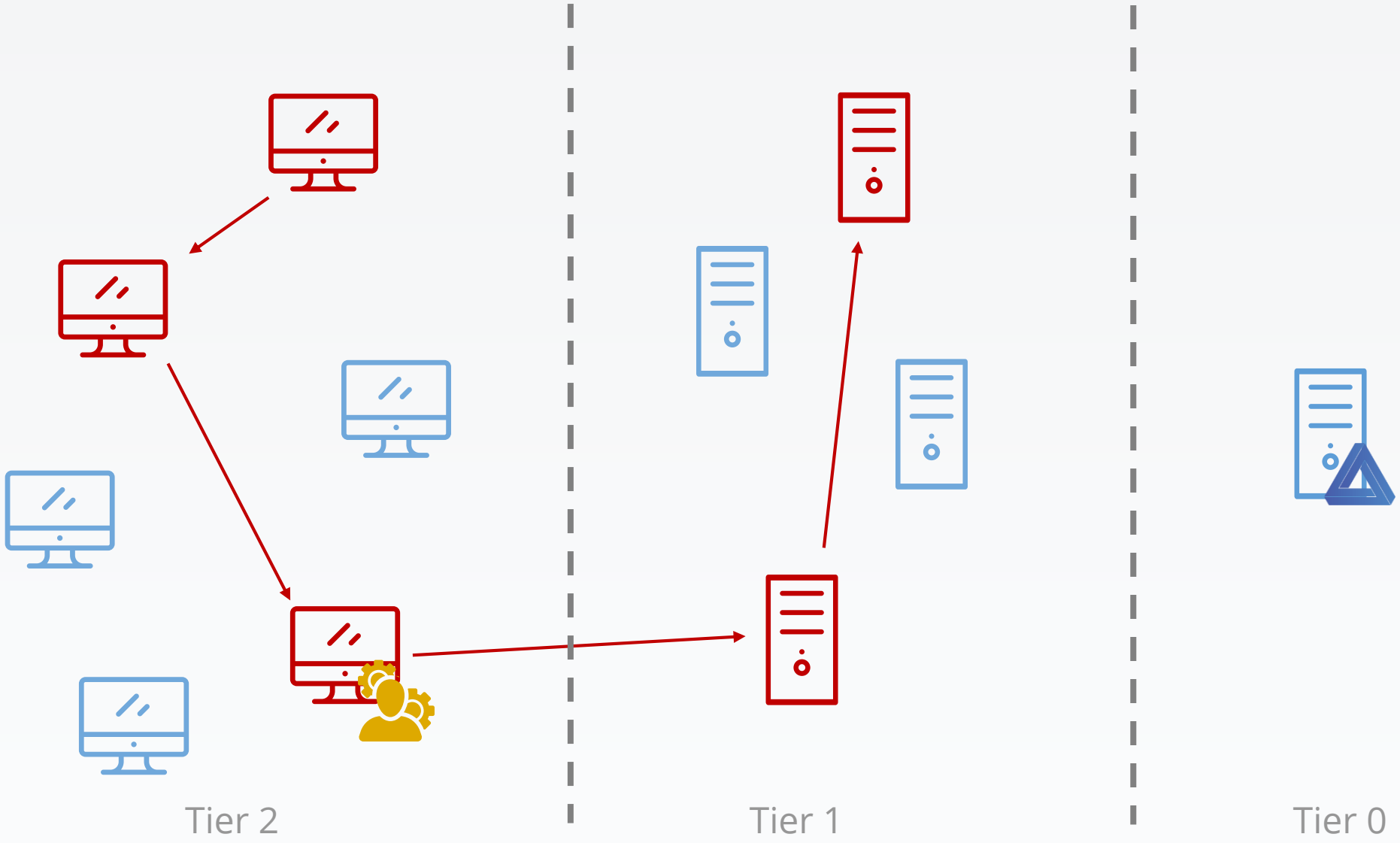


- Single forest, single domain
- One-way trust, using selective authentication, with the production forest(s)
- Contains small number of ESAE administrative accounts
  - Dedicated to ESAE
- Contains production forest(s) tier 0 administrators
  - Simple users in the ESAE forest
  - Only connect to tier 0 resources on production
  - Highly secured accounts
- Workstations/servers hardened

Why use an ESAE?



Why use an ESAE?



Why use an ESAE?

- Helps protect tier 0 resources against compromise
  - Which helps to protect against an overall compromise

Why use an ESAE?

- Helps protect tier 0 resources against compromise
  - Which helps to protect against an overall compromise

- Can use the same Active Directory account to administrate multiple forests
  - In fact, don’t use an ESAE for only one forest…

Why use an ESAE?

- Helps protect tier 0 resources against compromise
  - Which helps to protect against an overall compromise

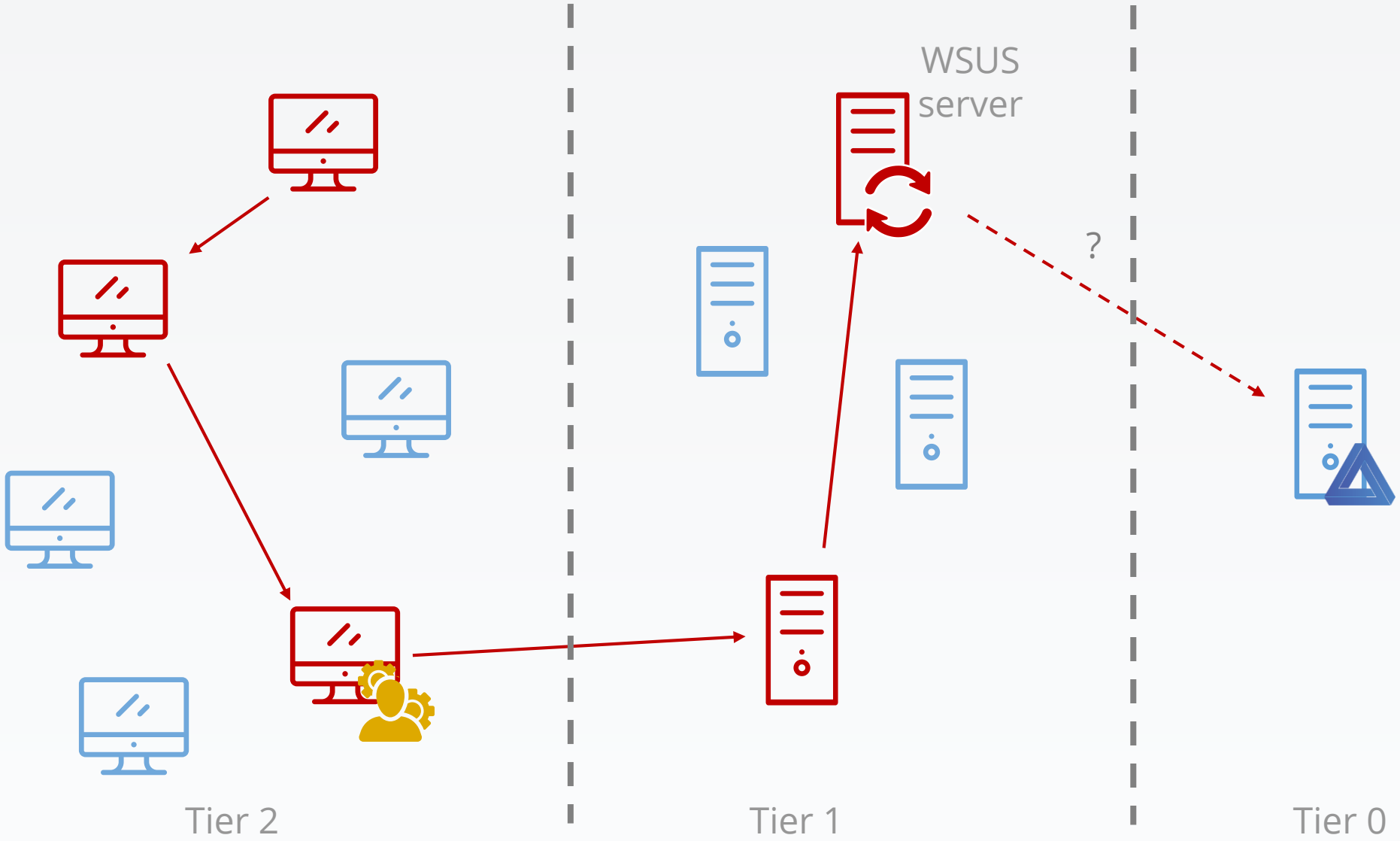
- Can use the same Active Directory account to administrate multiple forests
  - In fact, don’t use an ESAE for only one forest…

- Doesn’t protect enterprise’s assets, but a mandatory step to get to that

How do you compromise an ESAE-managed forest?

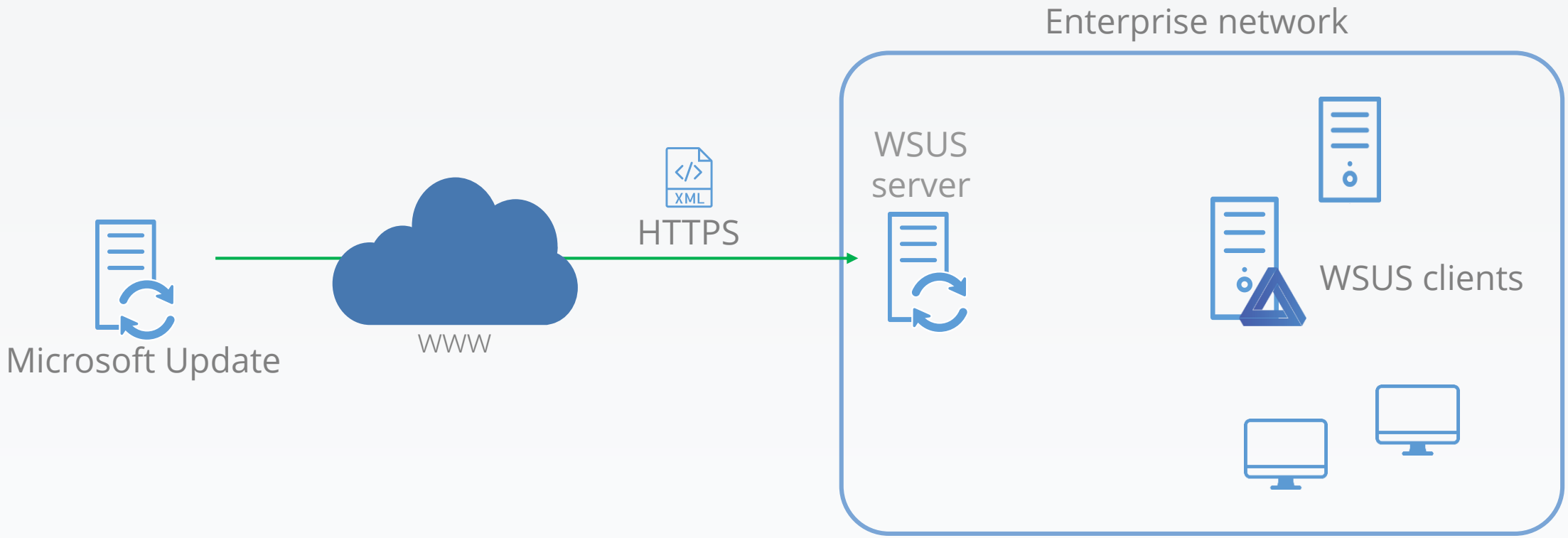
Well, you can’t, that’s the point.

What if a WSUS server serves updates to the DCs?

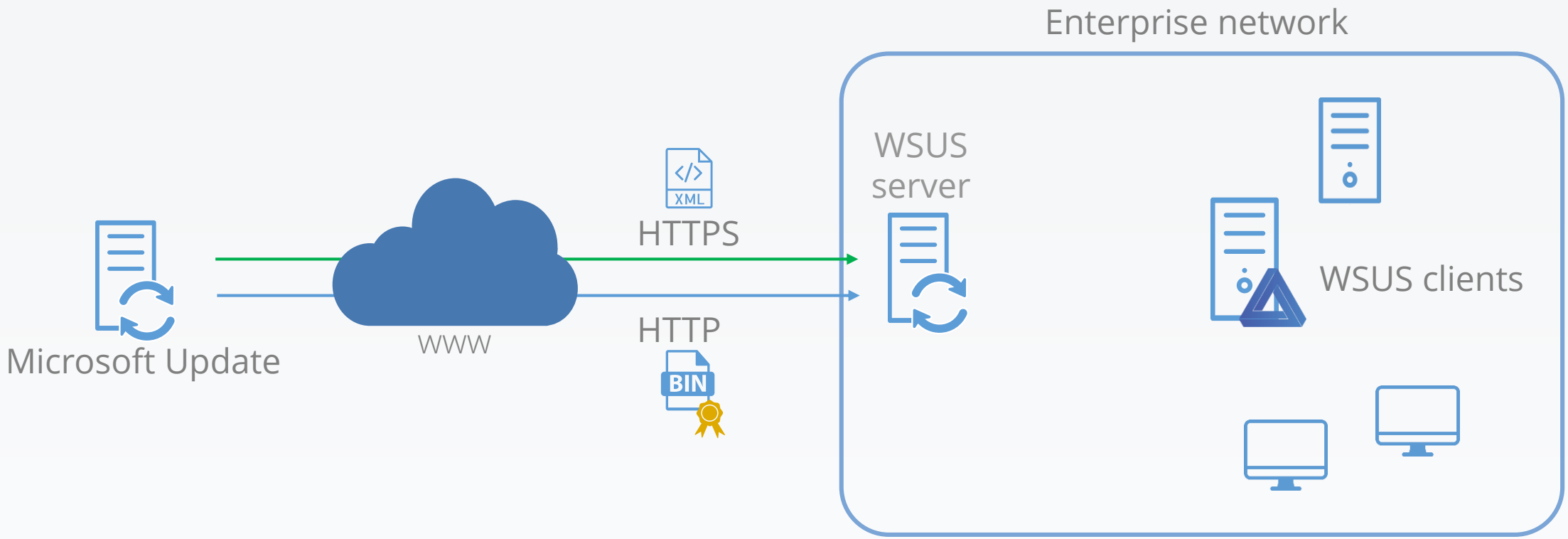


Can you compromise an
ESAE-managed forest using a WSUS server?

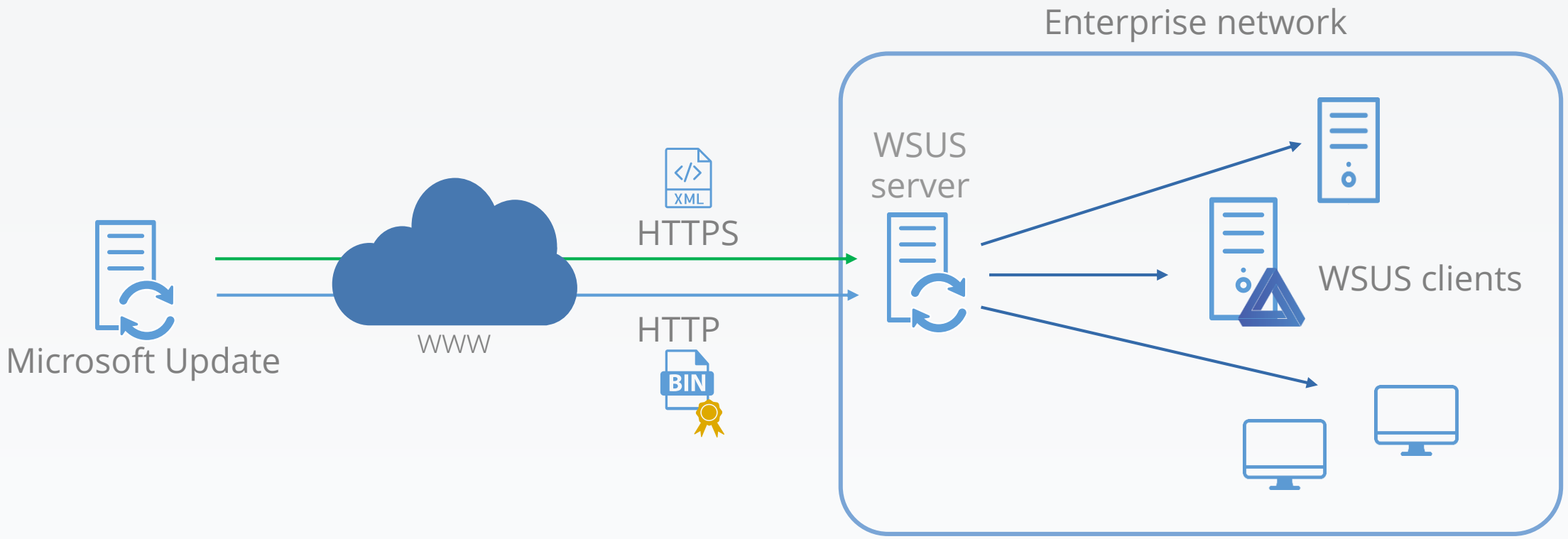
Windows Server Update Services (WSUS) architecture



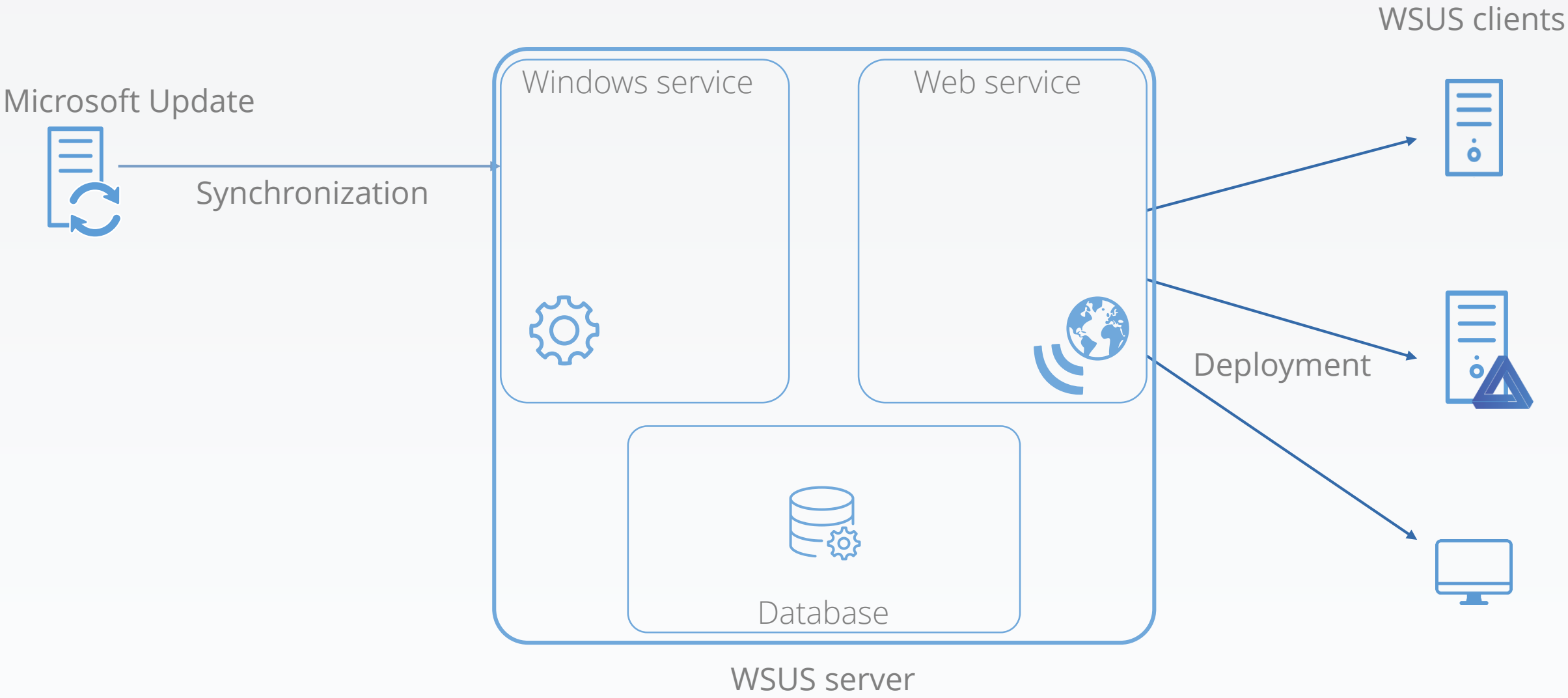
Windows Server Update Services (WSUS) architecture



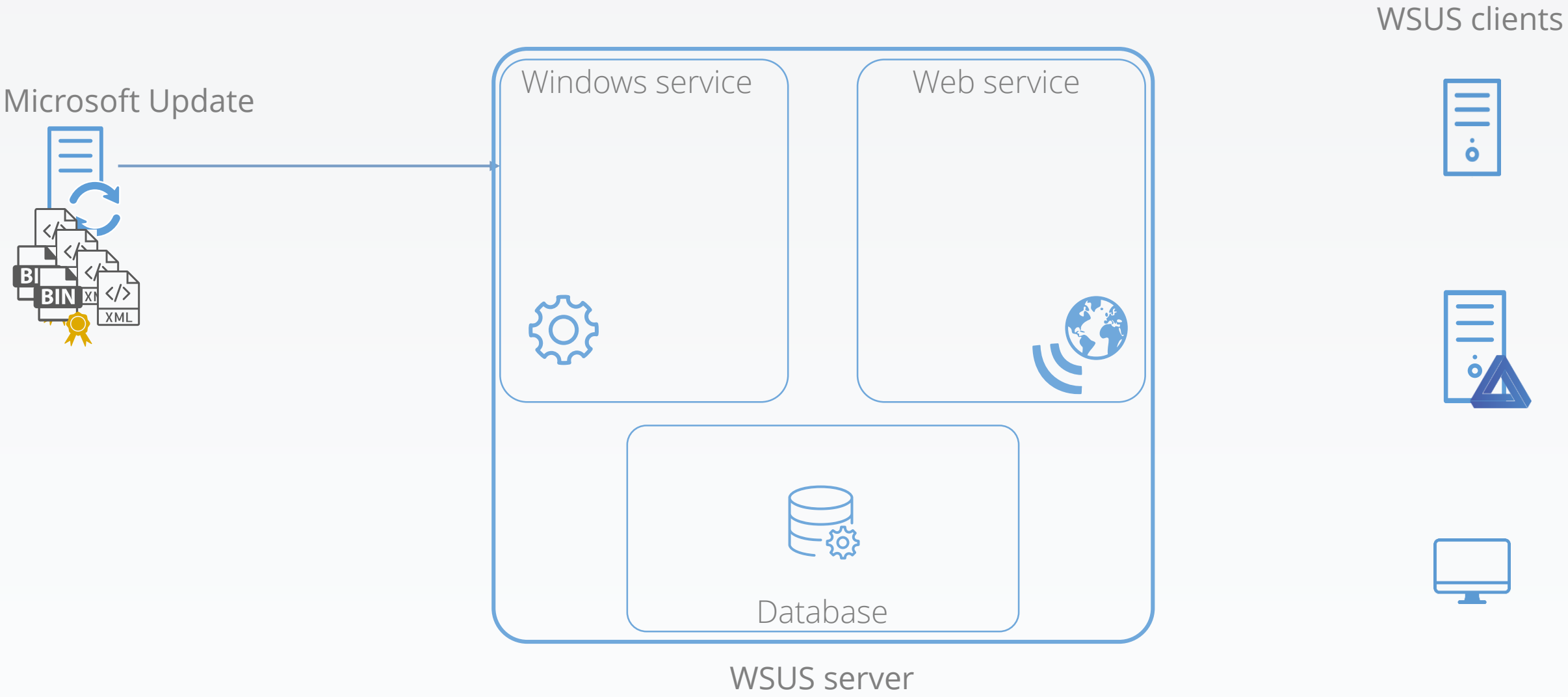
Windows Server Update Services (WSUS) architecture



WSUS server components

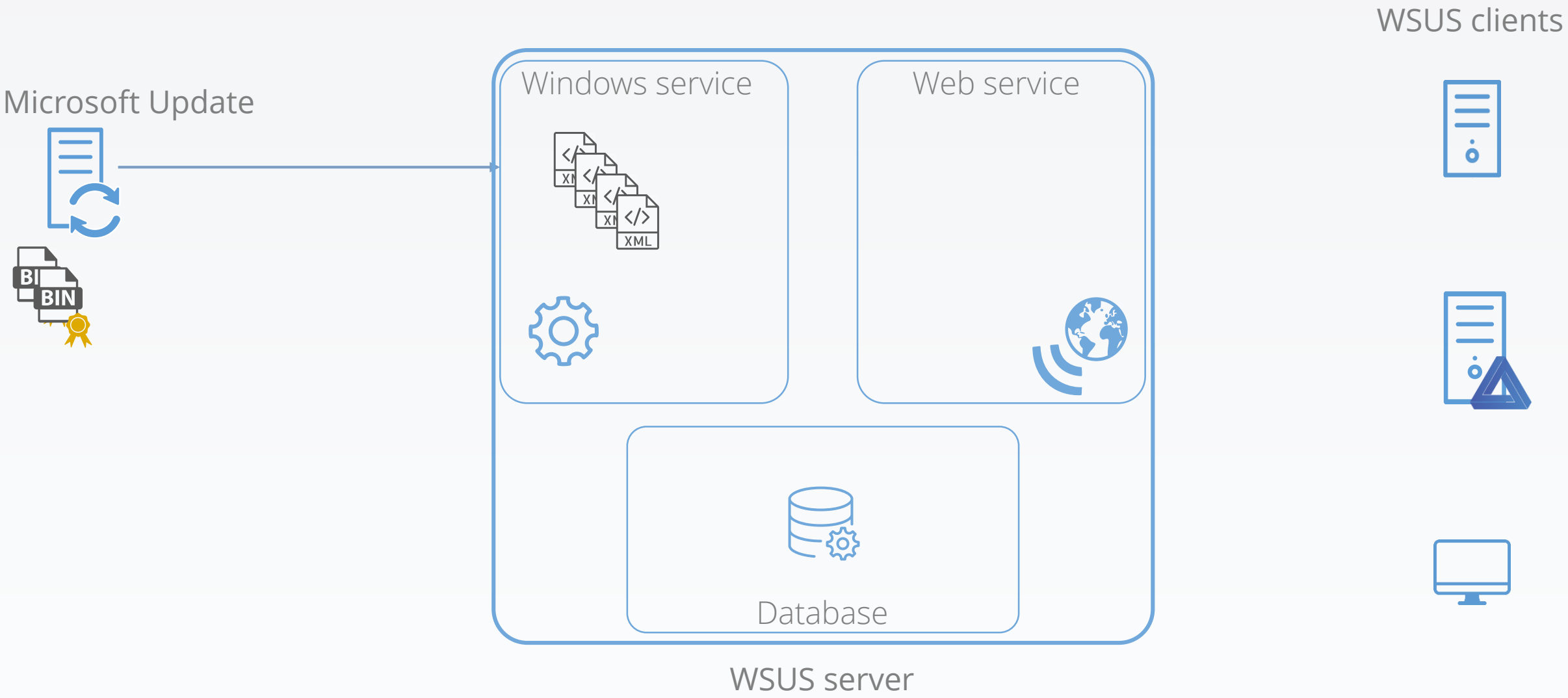


Updates journey within a WSUS server



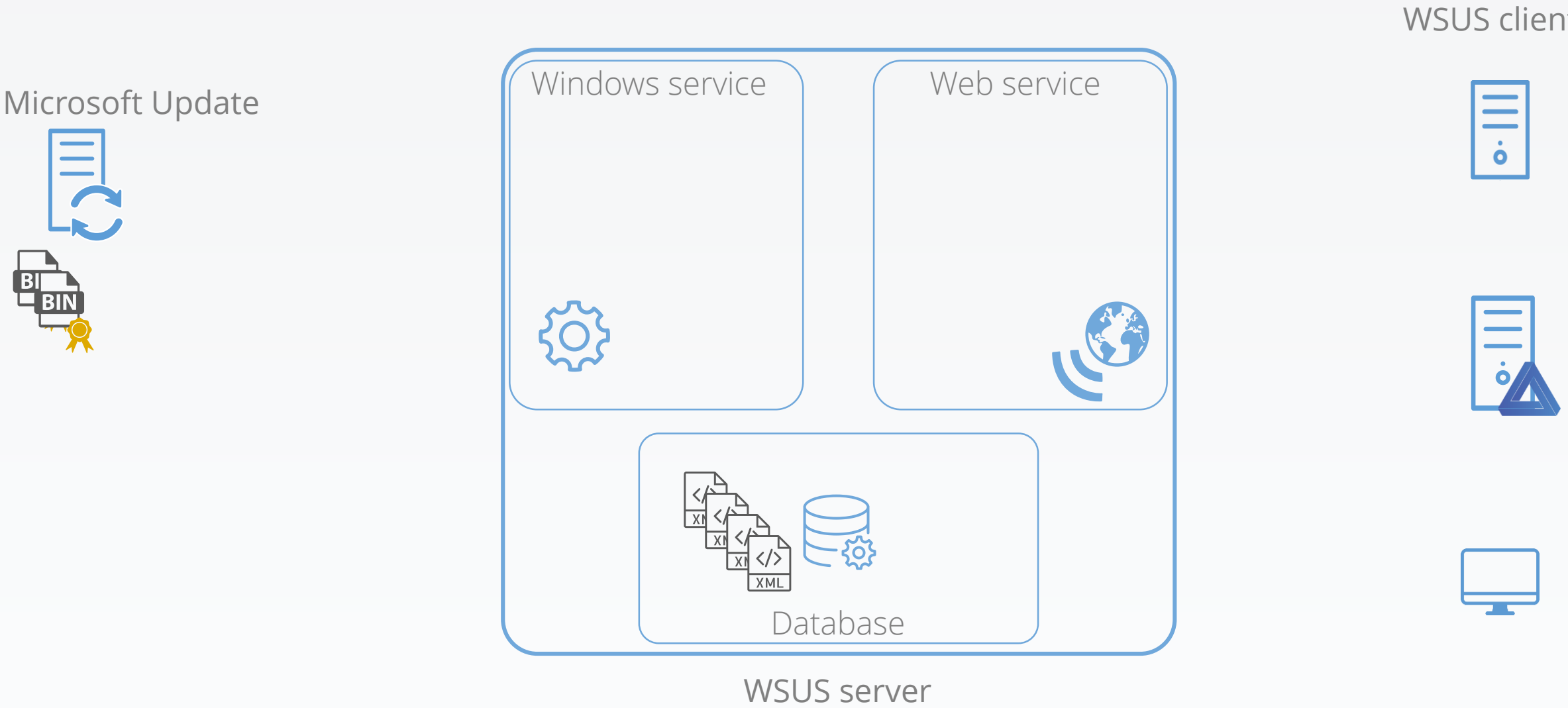
Updates journey within a WSUS server

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



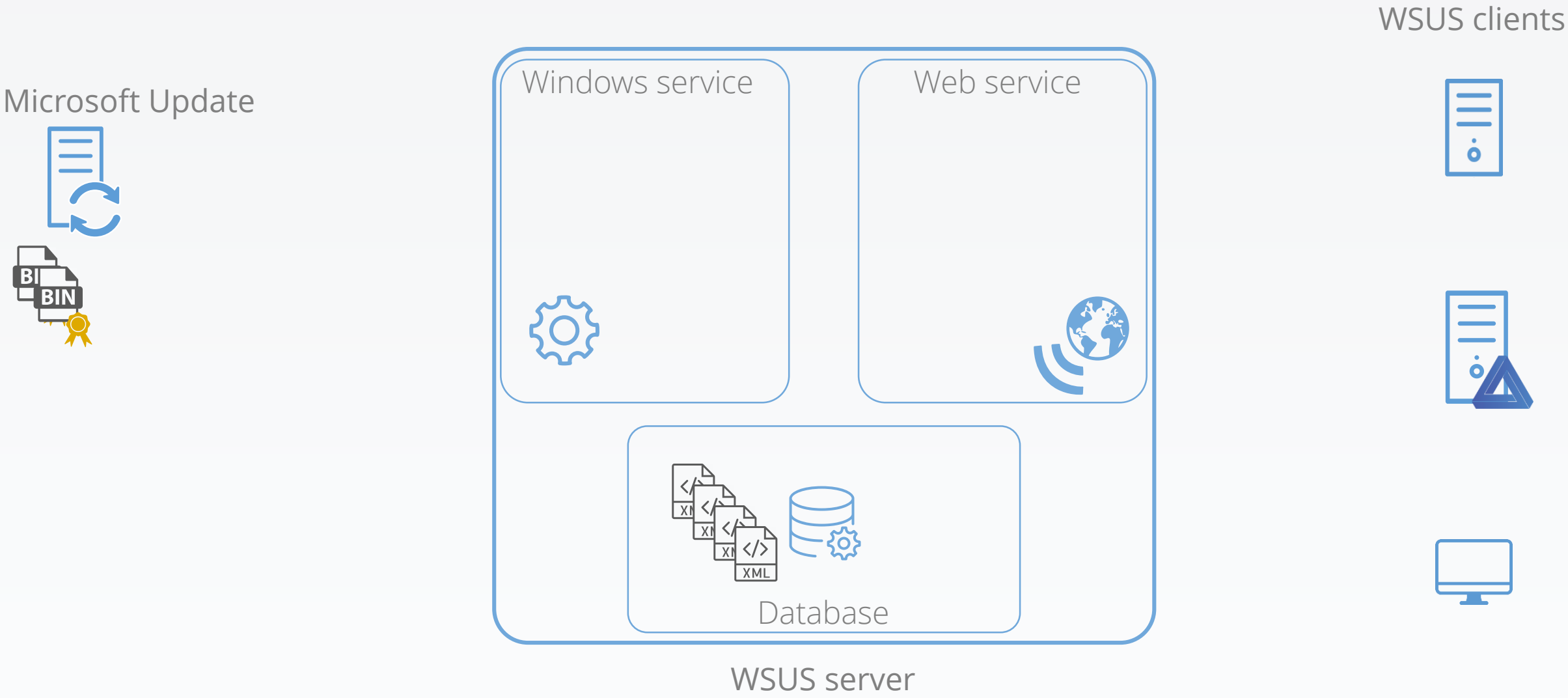
Updates journey within a WSUS server

2. Windows service transmits the metadata to the database



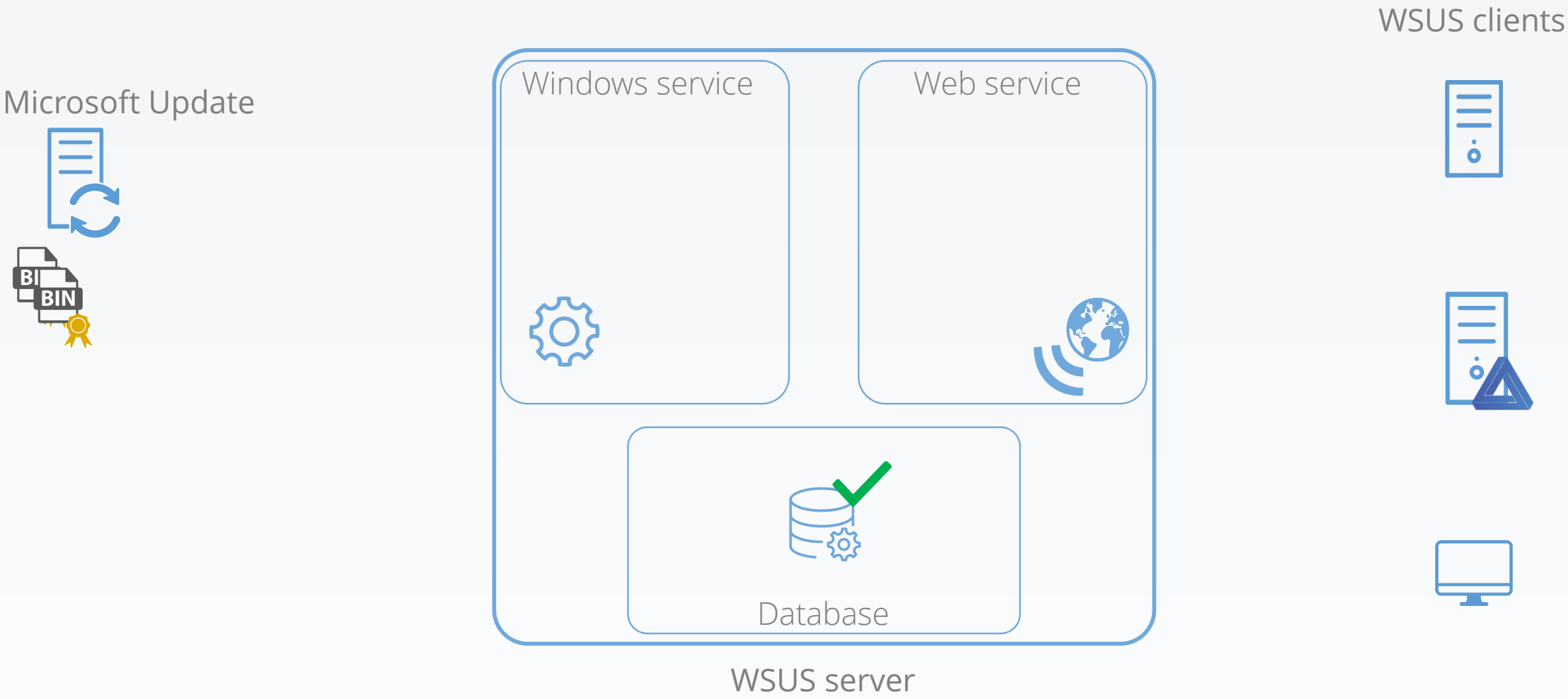
Updates journey within a WSUS server

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



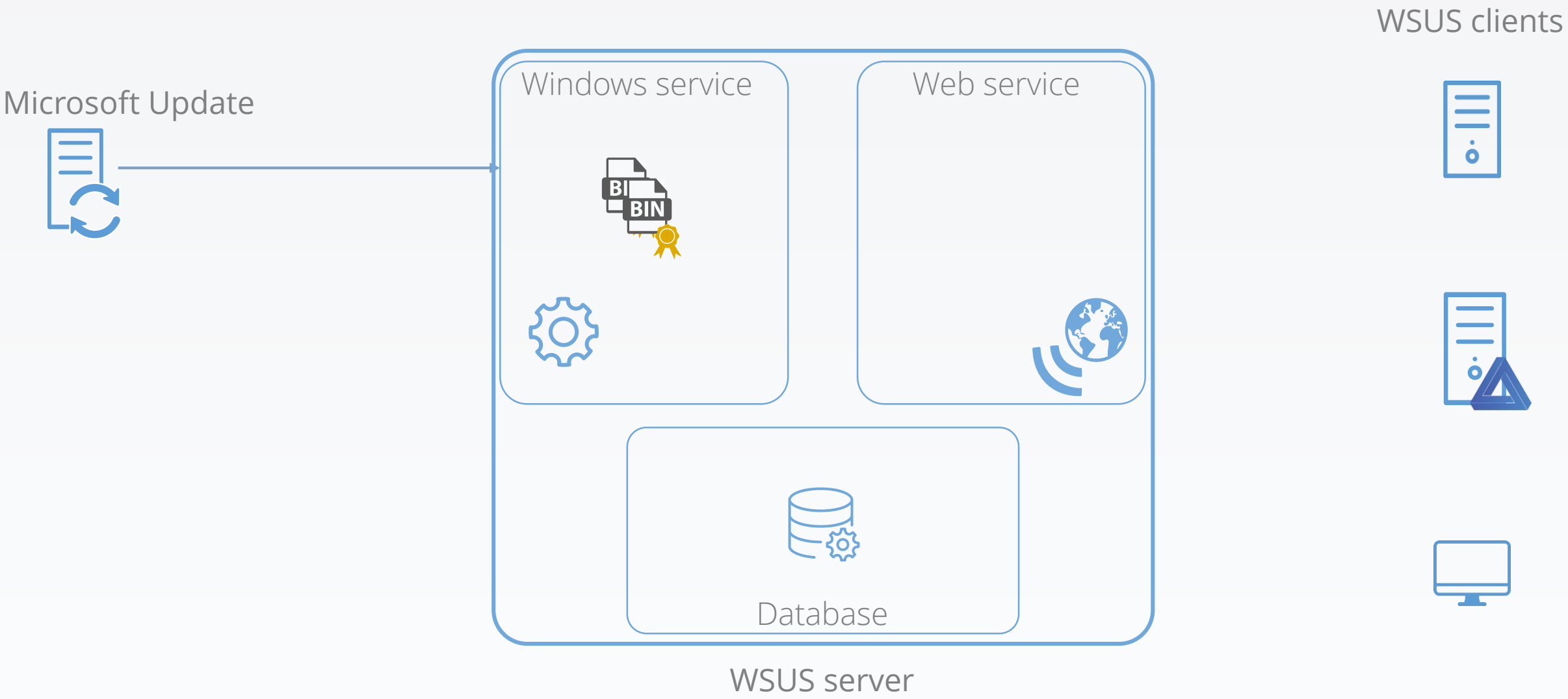
Updates journey within a WSUS server

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



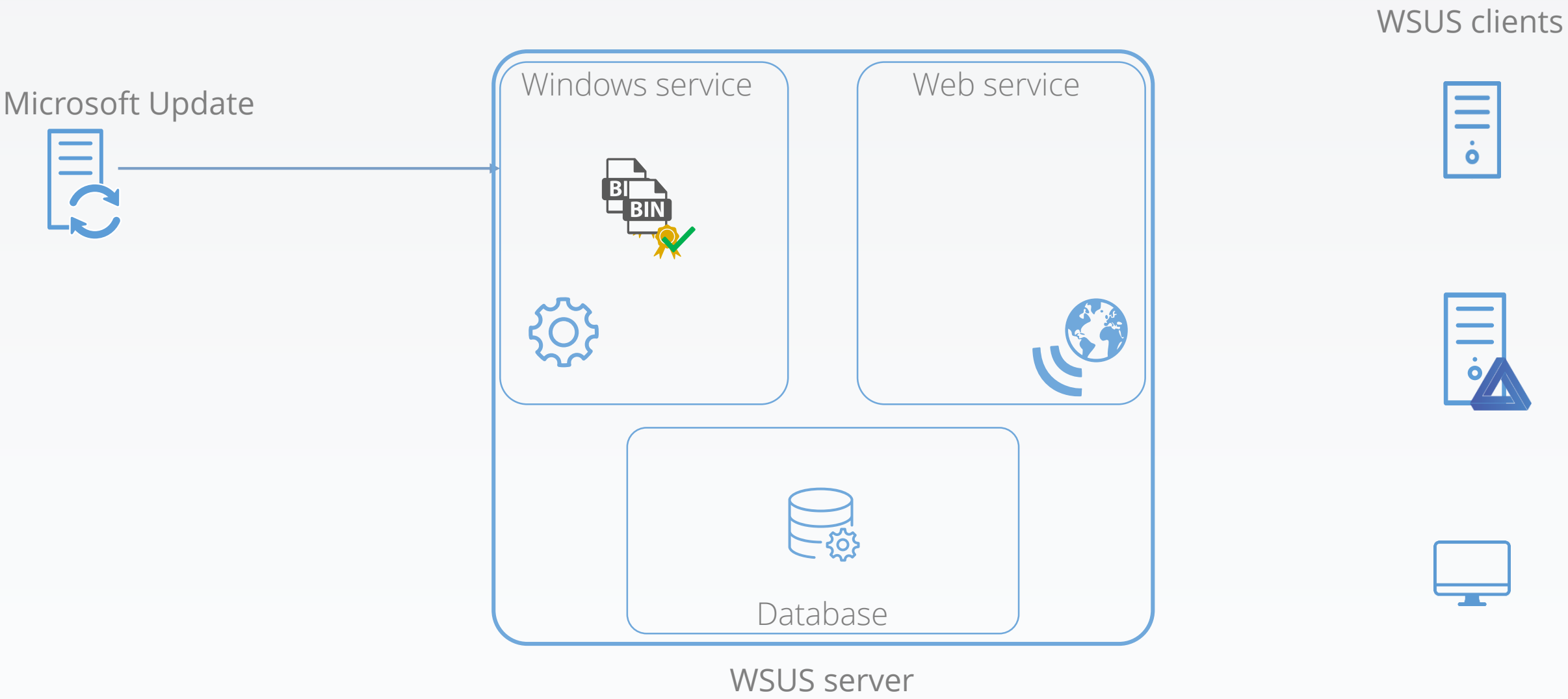
Updates journey within a WSUS server

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



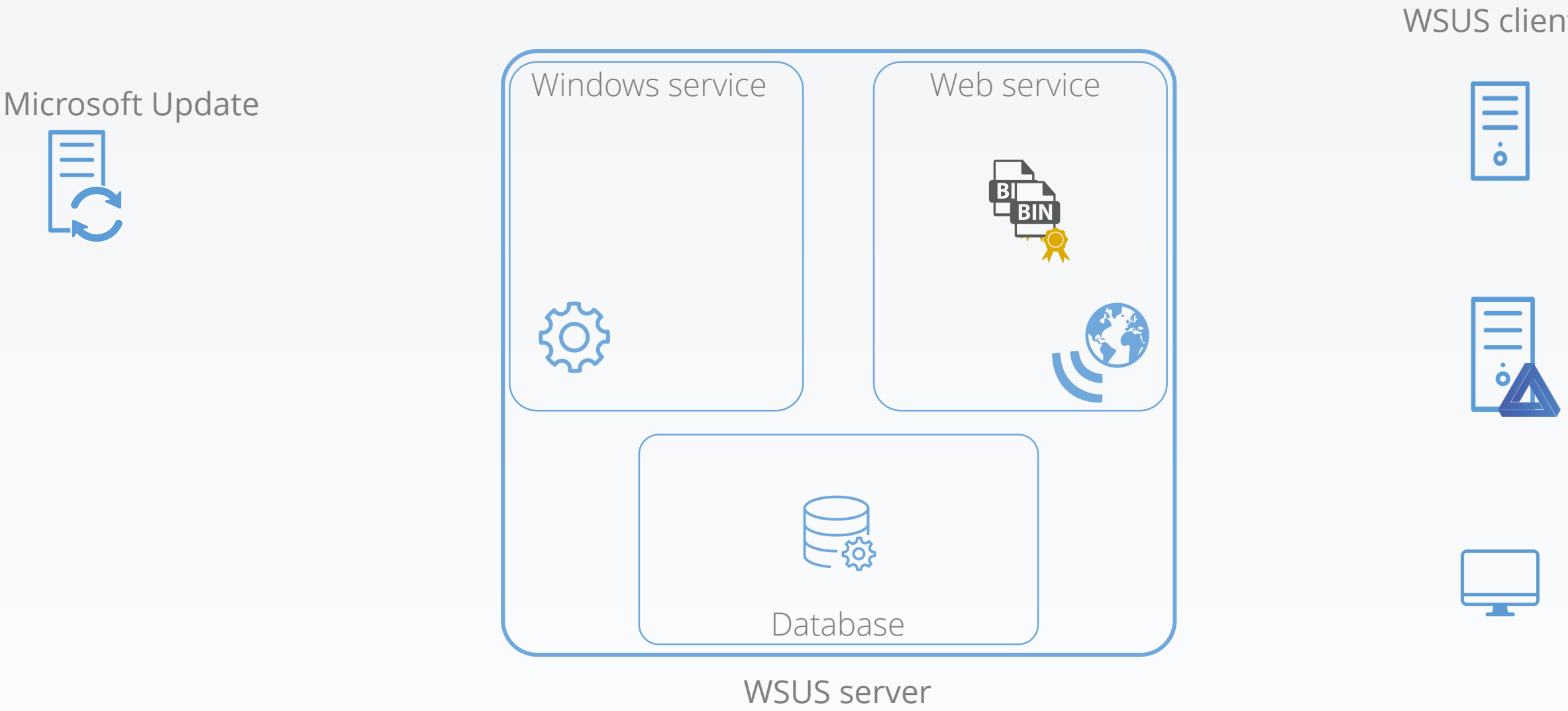
Updates journey within a WSUS server

6. Each binary signature is checked



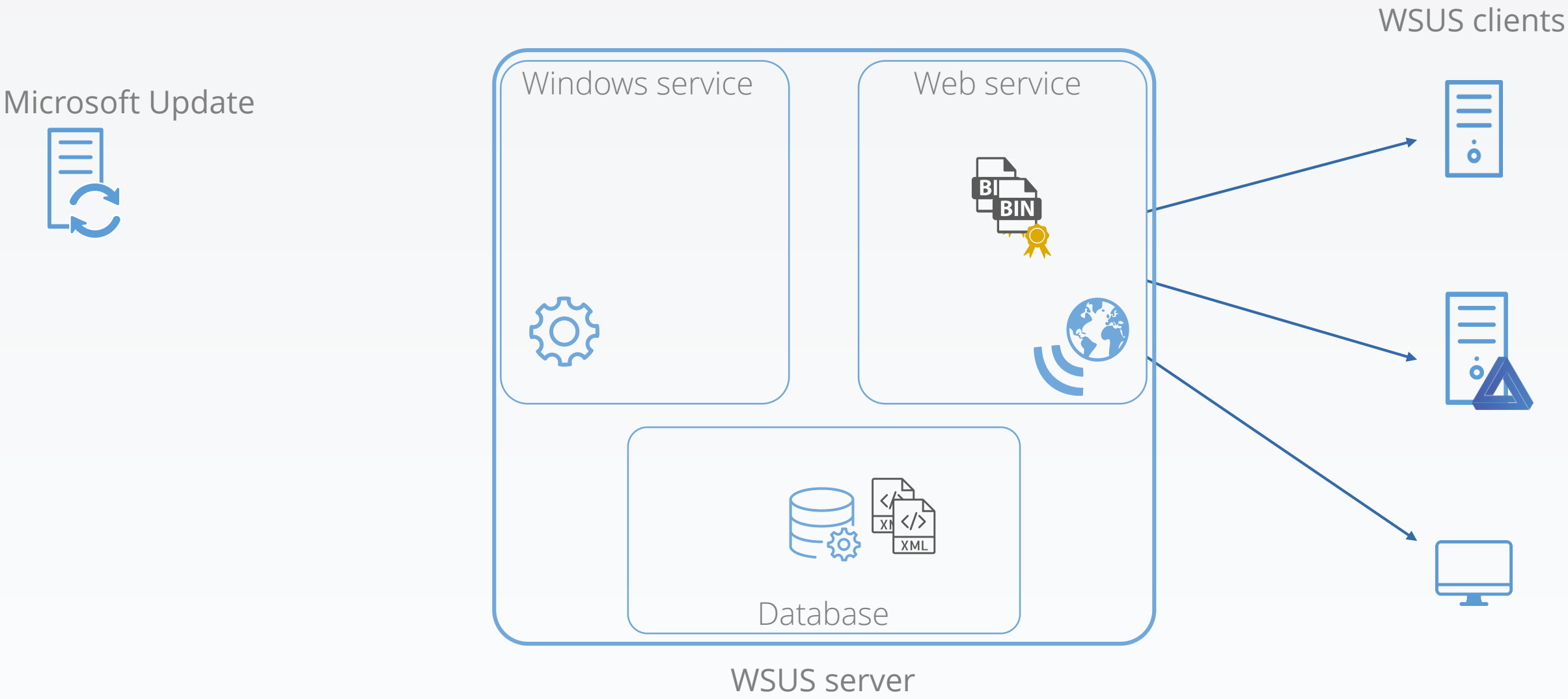
Updates journey within a WSUS server

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



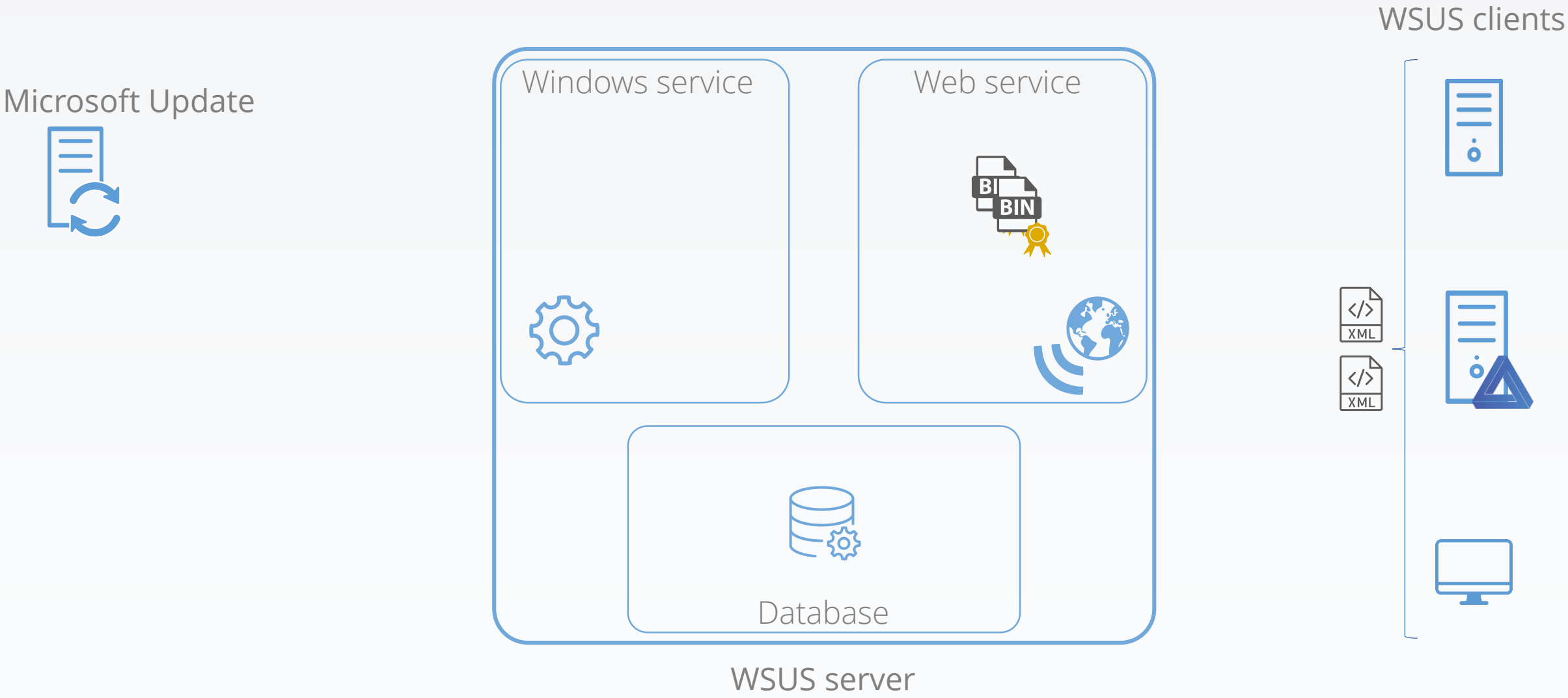
Updates journey within a WSUS server

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



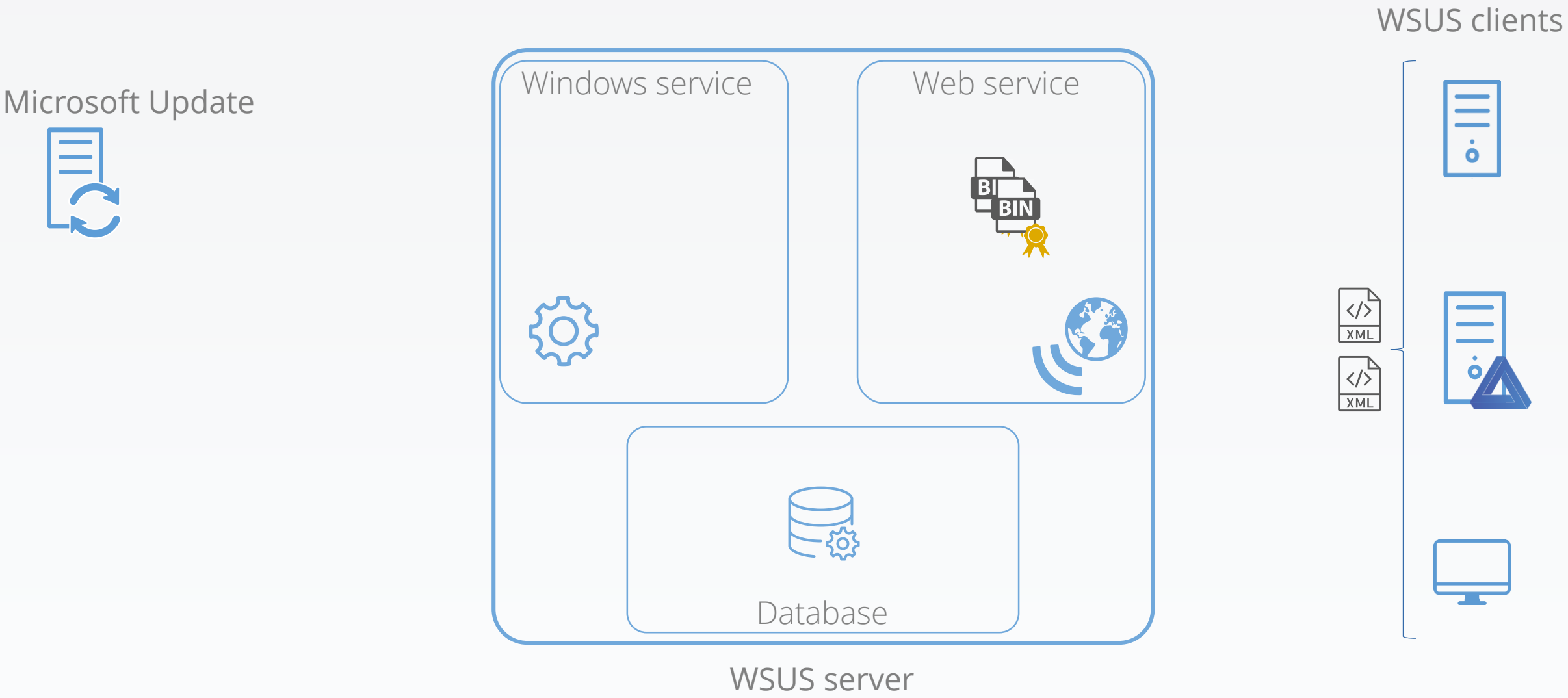
Updates journey within a WSUS server

9. Web service transmits the metadata to the WSUS clients



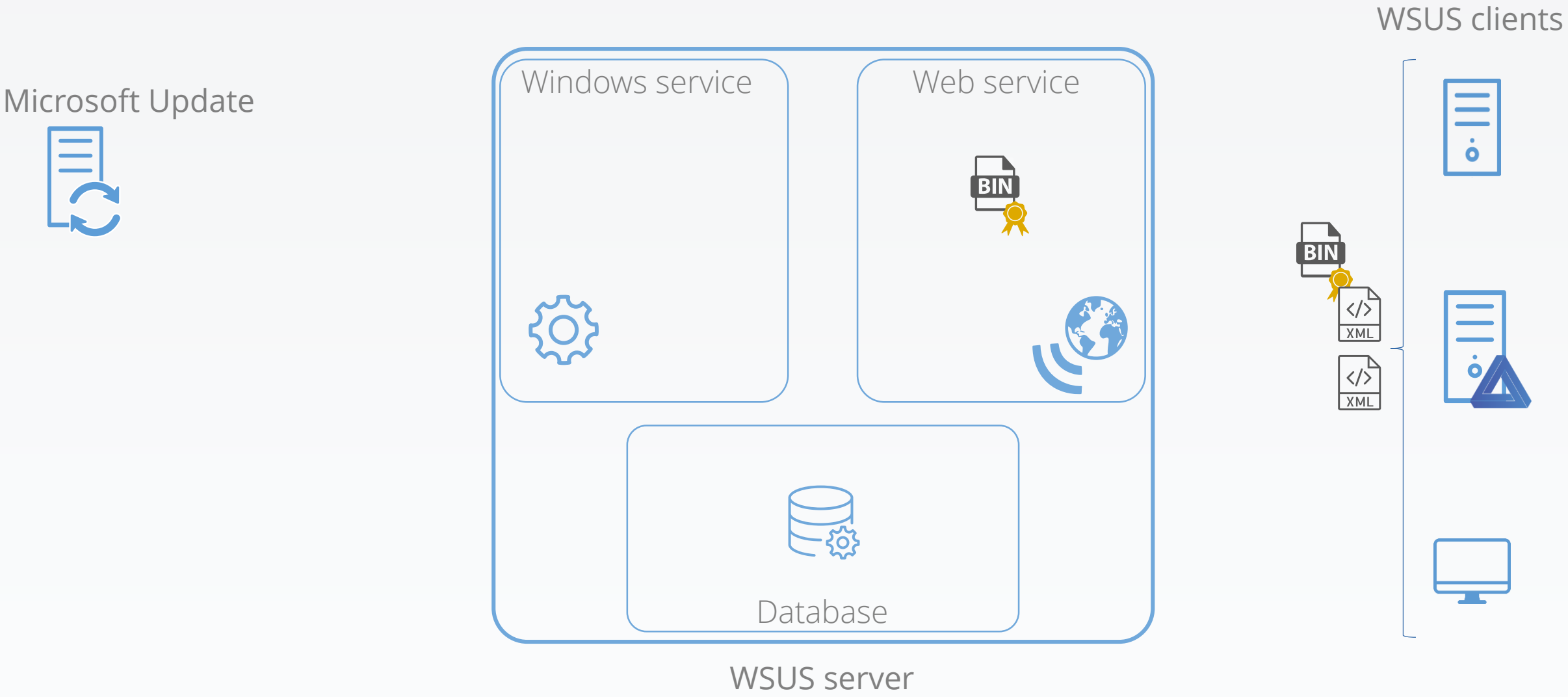
Updates journey within a WSUS server

10. Each client evaluates if the updates is installable



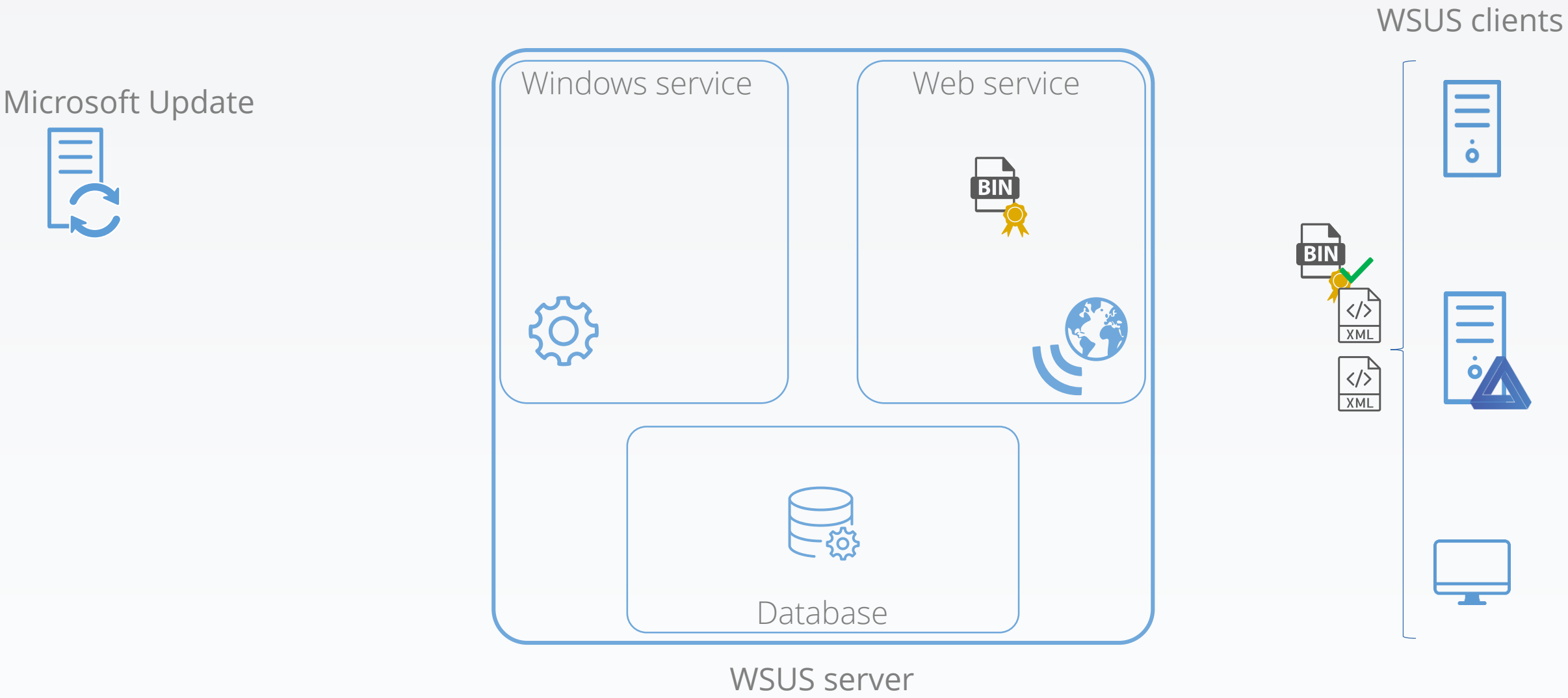
Updates journey within a WSUS server

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



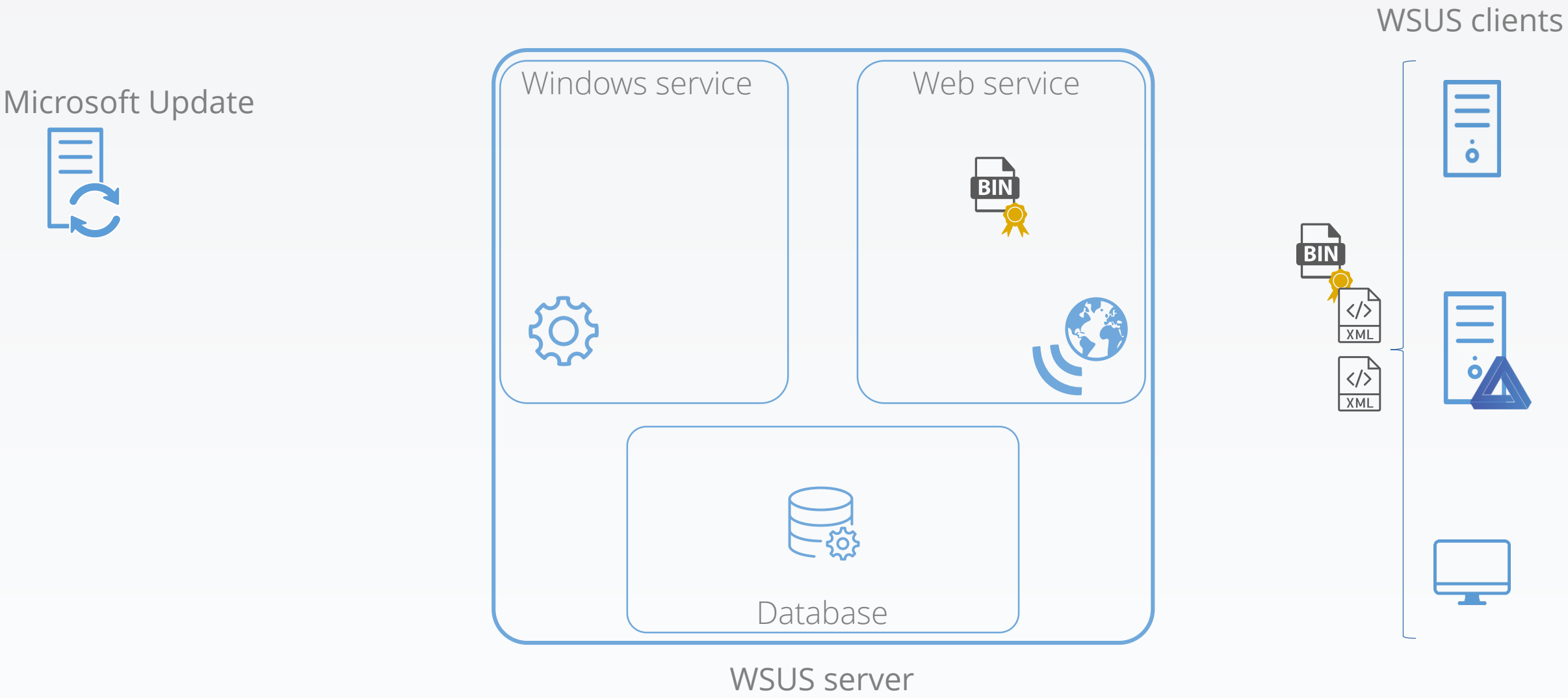
Updates journey within a WSUS server

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



How to connect to the database

HKLM\Software\Microsoft\Update Services\Server\Setup

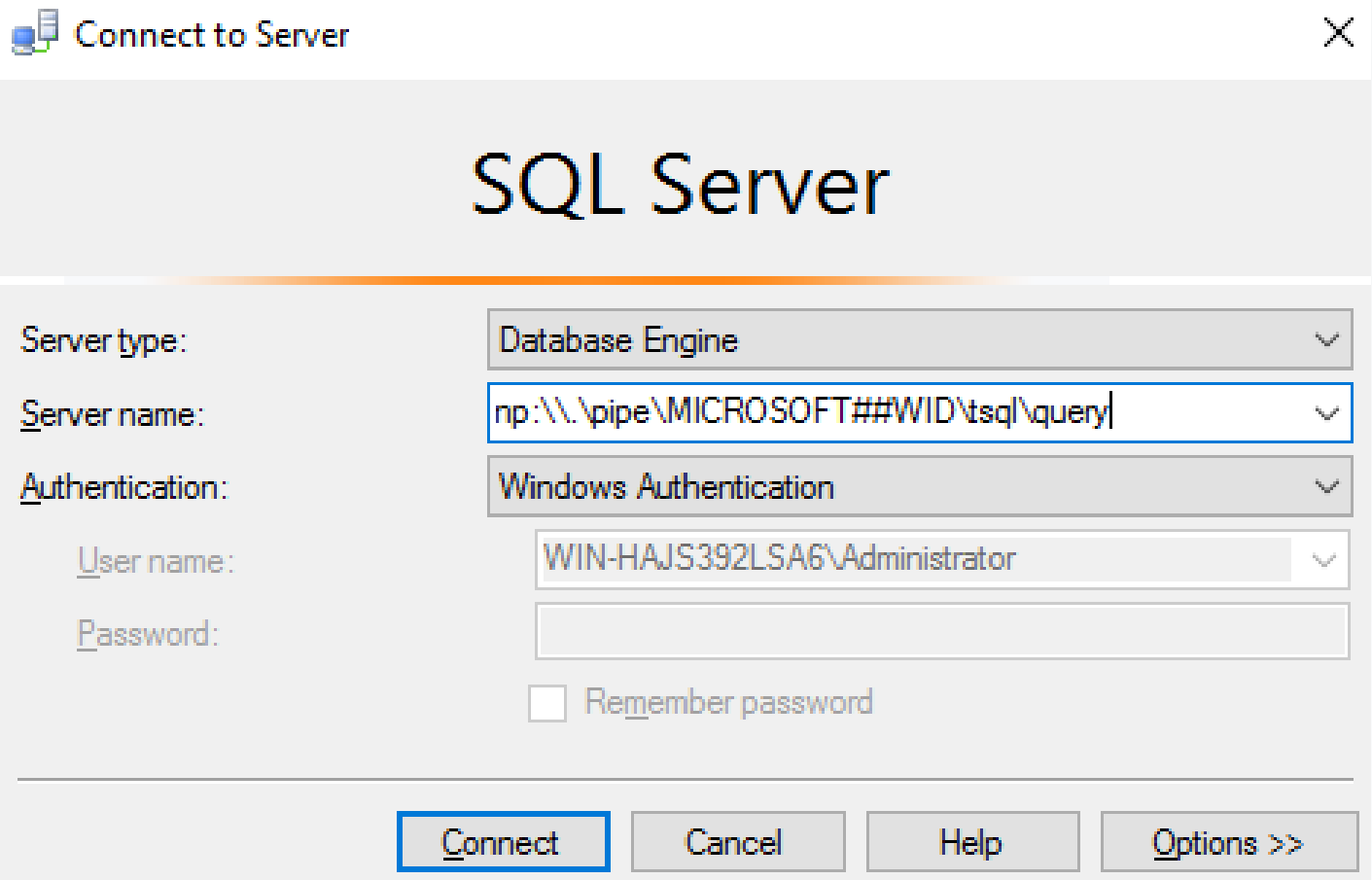
PortNumber	REG_DWORD	0x00002152 (8530)
ServicePackLevel	REG_DWORD	0x00000000 (0)
SqlAuthenticationMode	REG_SZ	WindowsAuthentication
SqlDatabaseName	REG_SZ	SUSDB
SqlEncryptedPassword	REG_SZ	
SqlServerName	REG_EXPAND_SZ	MICROSOFT##WID
SqlUserName	REG_SZ	
TargetDir	REG_EXPAND_SZ	%ProgramFiles%\Update Services\
UsingSSL	REG_DWORD	0x00000000 (0)
Version	REG_DWORD	0x00000005 (5)
VersionString	REG_SZ	10.0.14393.0
WsusAdministratorsSid	REG_SZ	S-1-5-21-3553850934-3542133063-197517862-1000
WsusReportersSid	REG_SZ	S-1-5-21-3553850934-3542133063-197517862-1001

Initial configuration

How to connect to the database

HKLM\Software\Microsoft\Update Services\Server\Setup

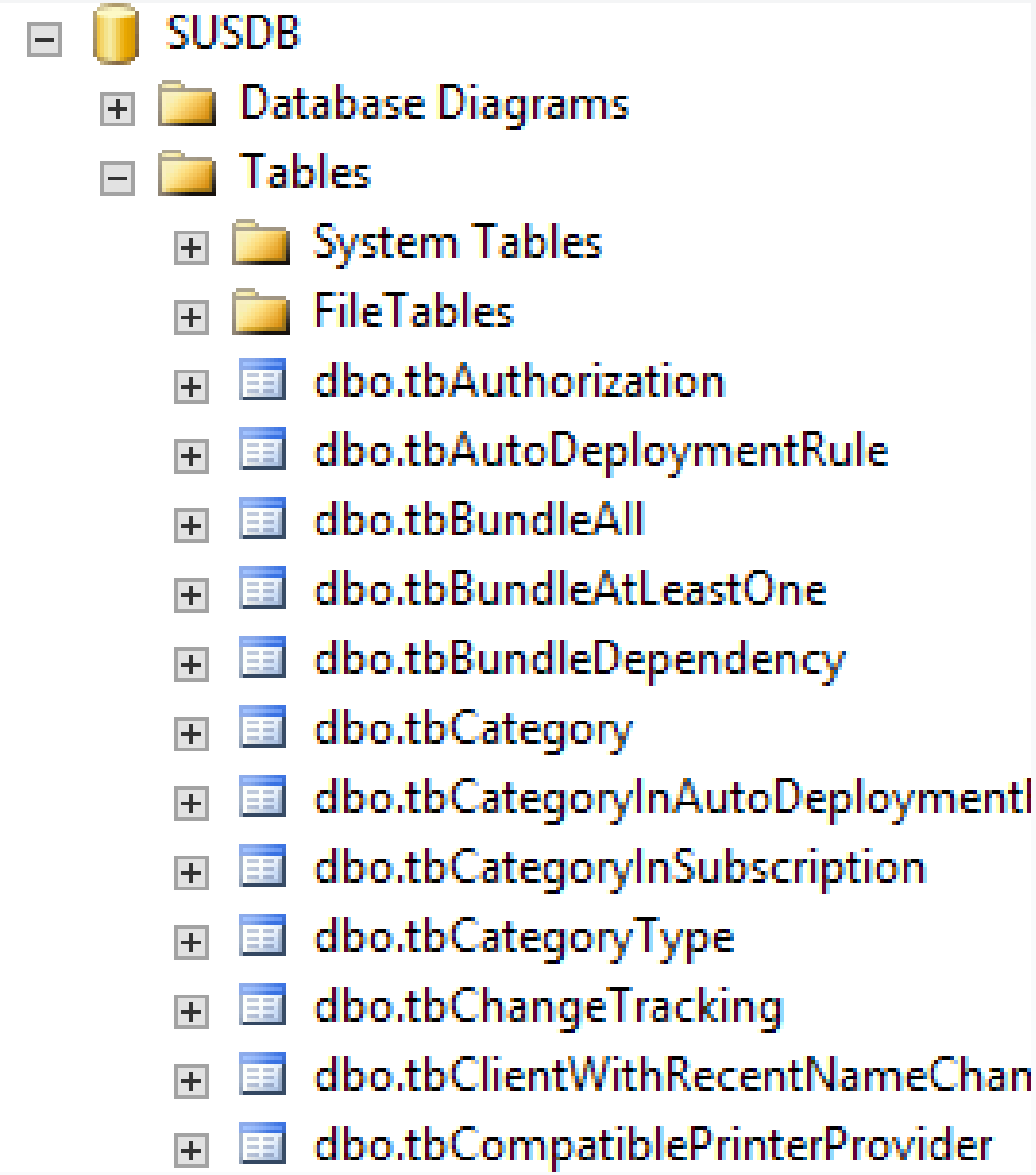
SqlServerName = "MICROSOFT##WID" →



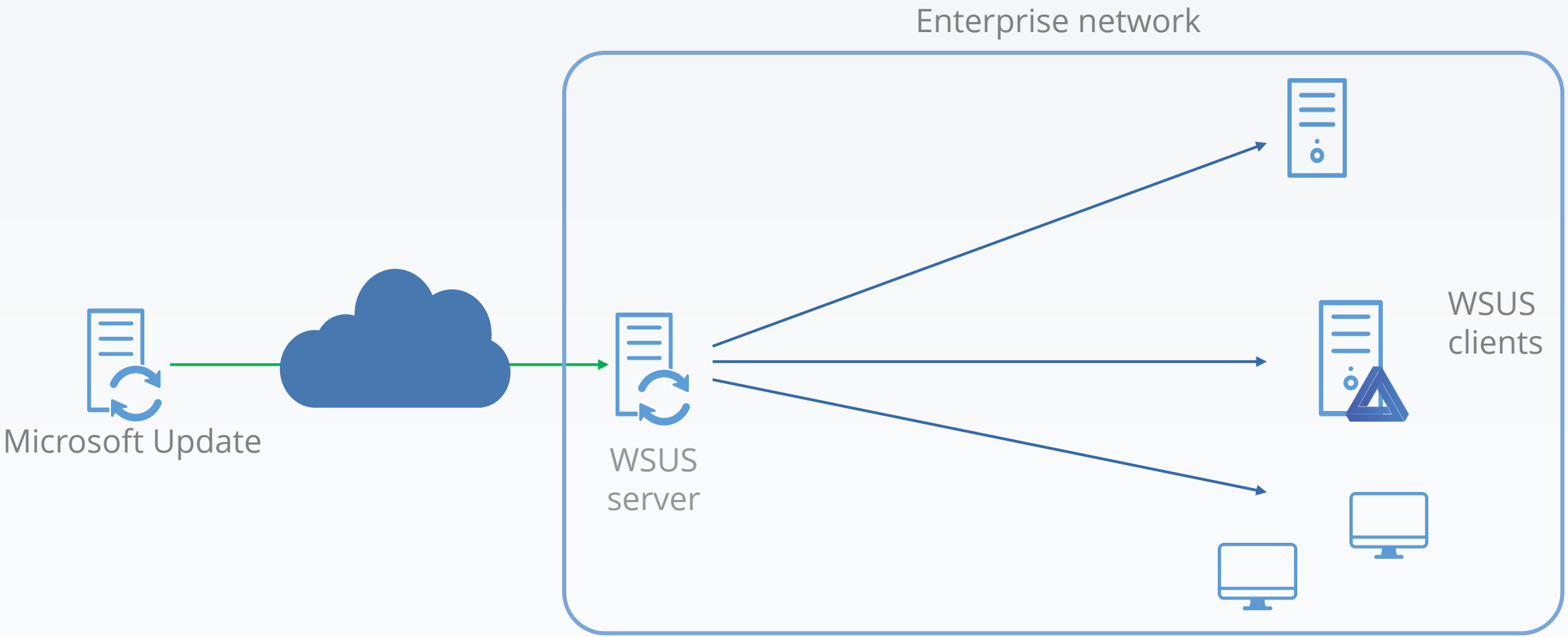
What's in the database?

Everything:
- Full WSUS configuration
- Updates metadata
- Approvement states
- …

Some stats:
- 31 views
- 35 triggers
- 52 functions
- 108 tables
- 380 stored procedures

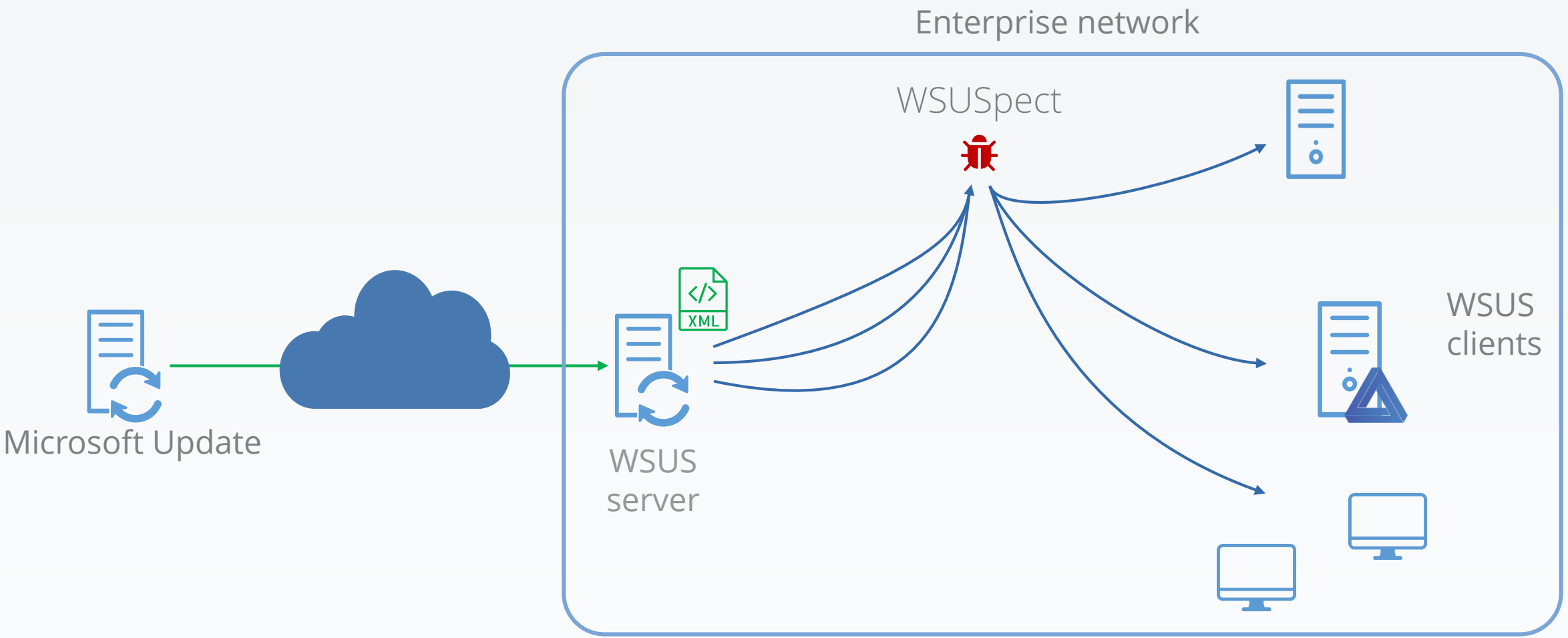


WSUS attacks: Black Hat USA 2015, WSUSpect



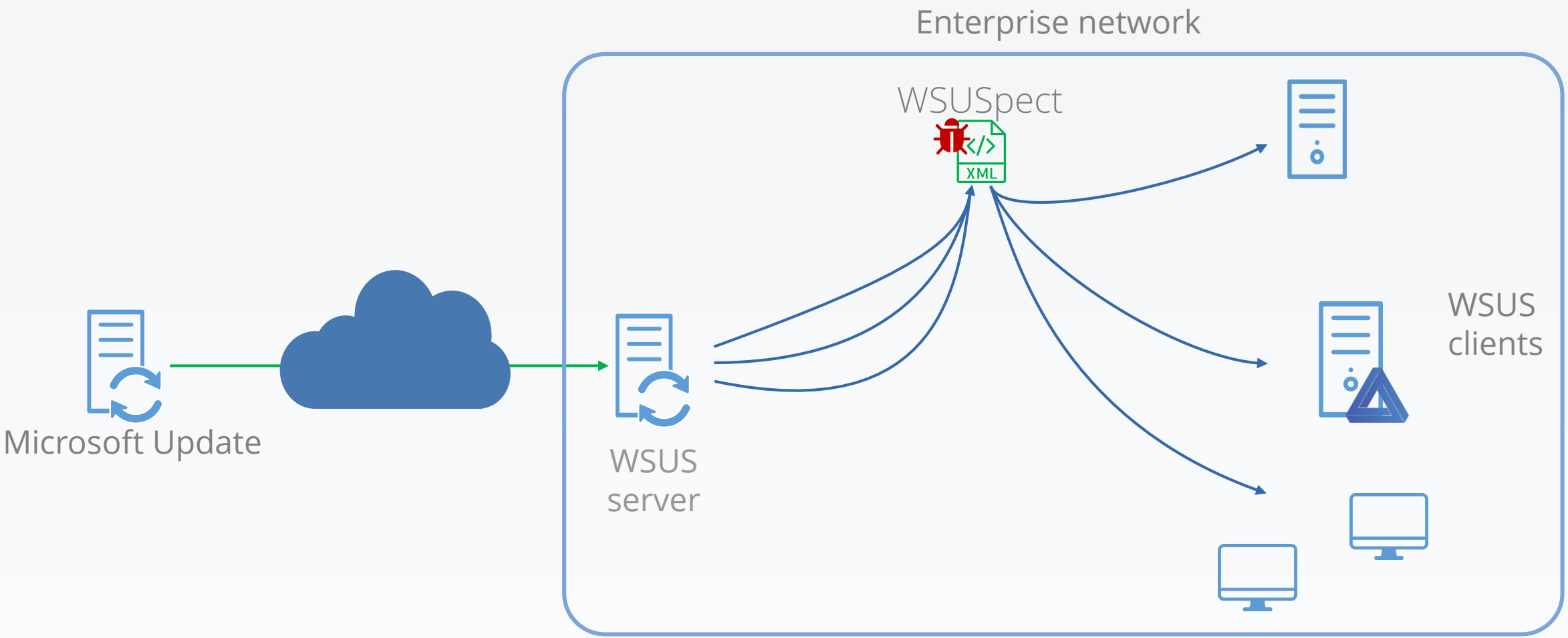
State-of-the-art

1. Get a mitm position

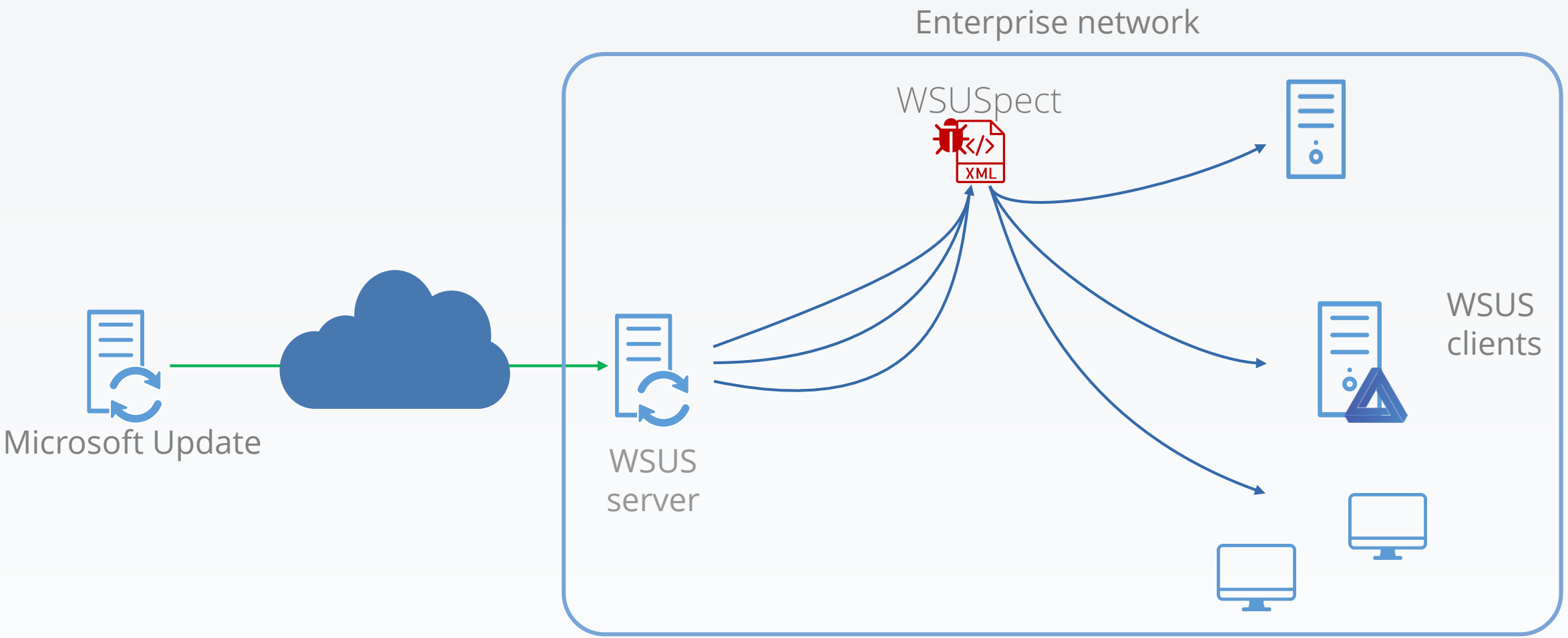


State-of-the-art

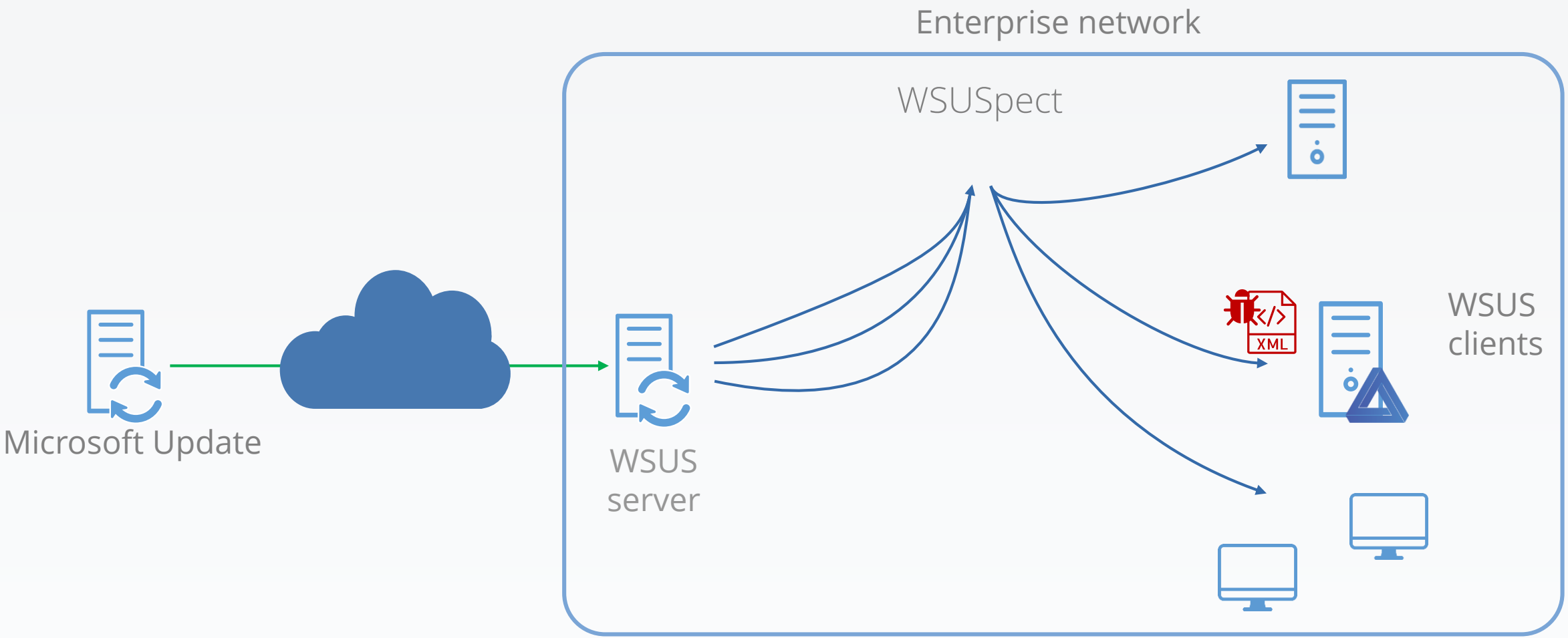
2. Intercepts new update queries



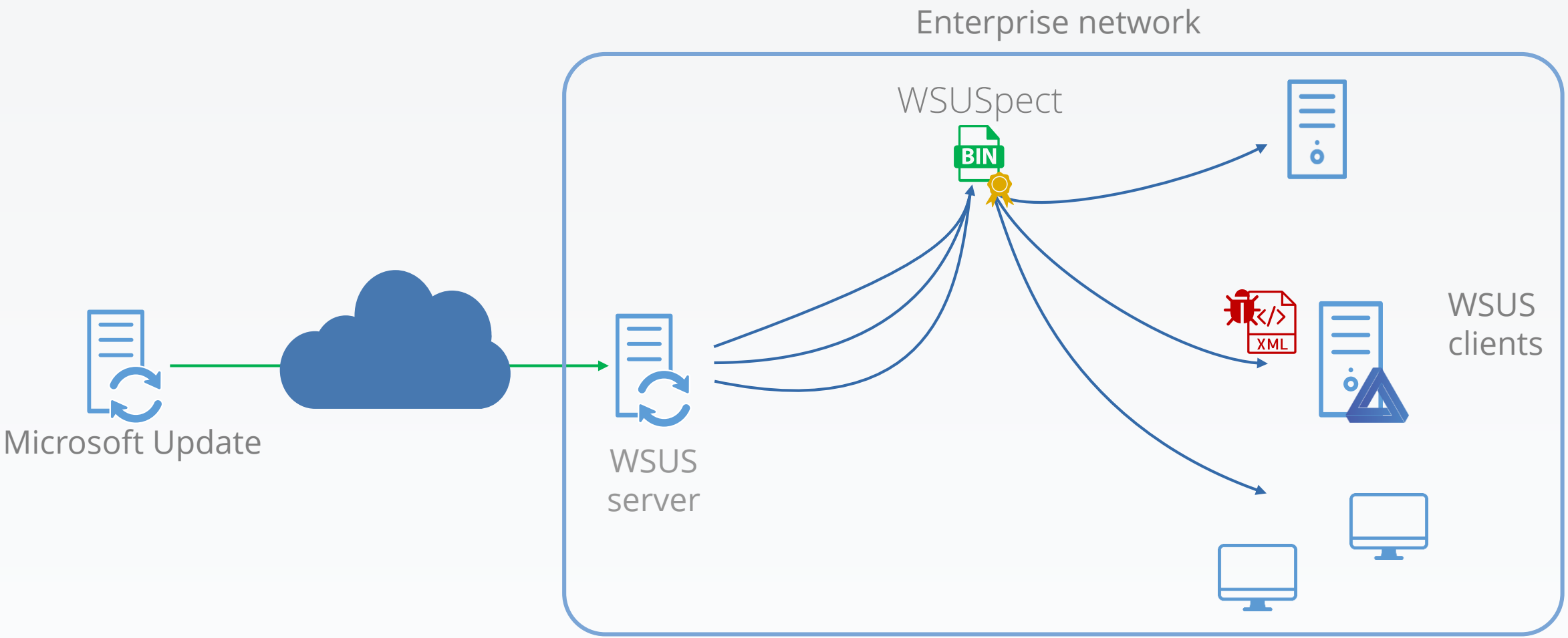
3. Infects the on-network metadata with a new, malicious update



4. The client sees a new available and installable update

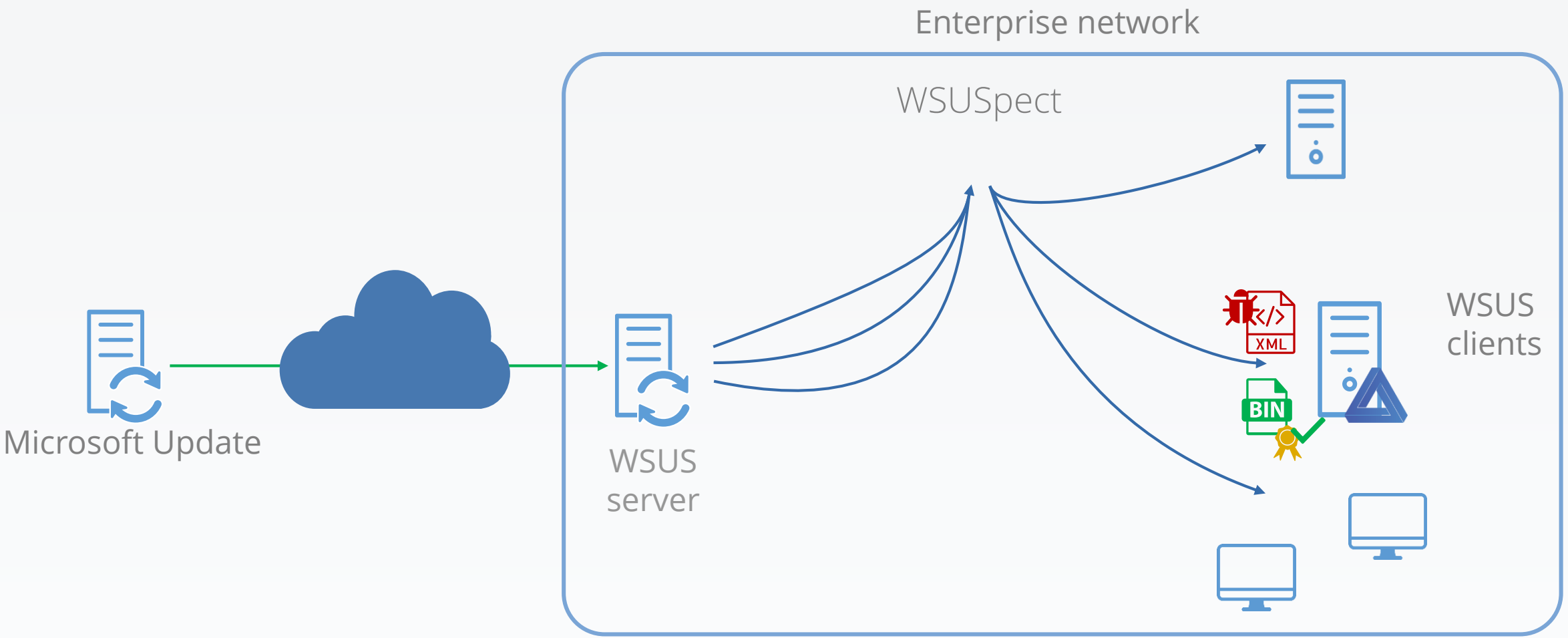


5. Fetches the related binary

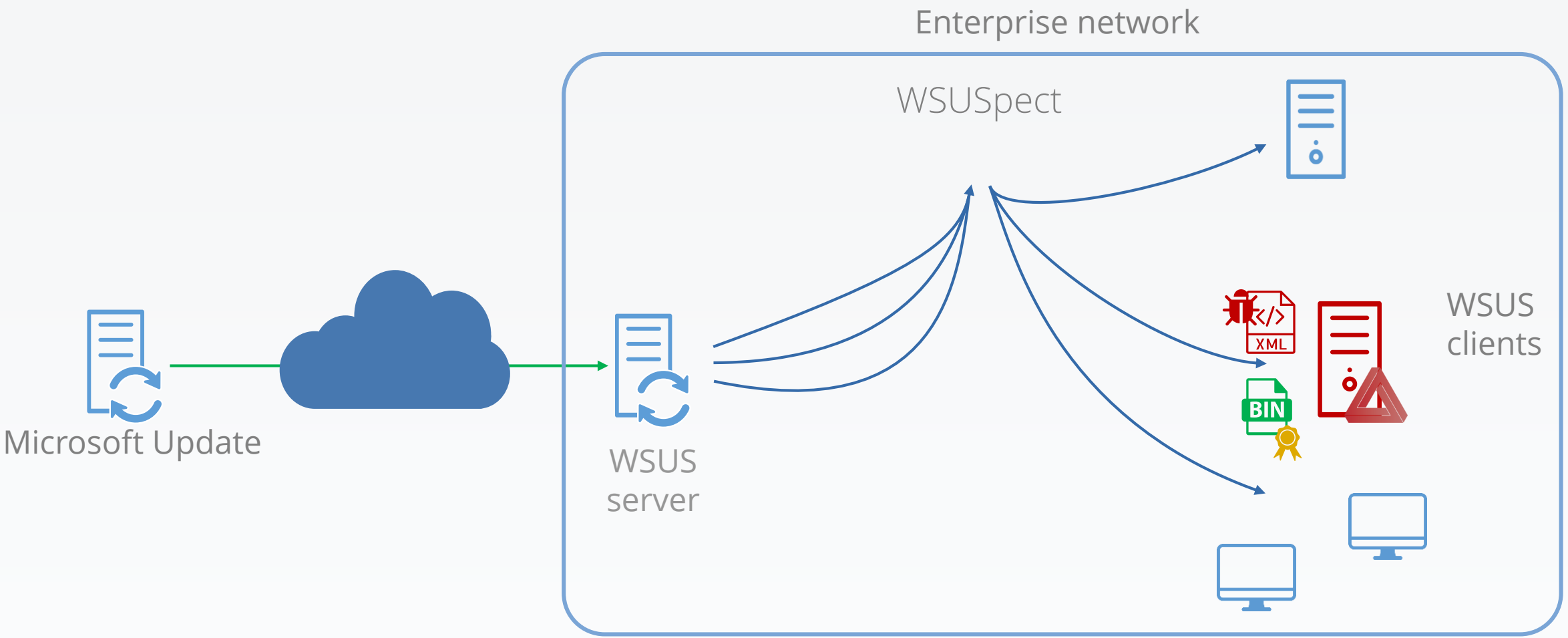


State-of-the-art

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 ESAE-managed domain controllers ☹

So, where are we?

We know:

- That injecting into the metadata between WSUS server/client is possible
- Where metadata are stored: in the database
- How to connect to this database

We want:

- To inject a metadata to compromise a client, without a network attack

So, where are we?

We know:

- That injecting into the metadata between WSUS server/client is possible
- Where metadata are stored: in the database
- How to connect to this database

We want:

- To inject a metadata to compromise a client, without a network attack

So, let's try to inject a new update into the database!

So, where are we?

We know:
- That injecting into the metadata between WSUS server/client is possible
- Where metadata are stored: in the database
- How to connect to this database

We want:
- To inject a metadata to compromise a client, without a network attack

So, let's try to inject a new update into the database!

...let's start by studying how updates are inserted...

How to check for inserted rows on SQLServer?

First try:

- Look for update information in tables

How to check for inserted rows on SQLServer?

First try:

- Look for update information in tables
- Find update information in some tables

How to check for inserted rows on SQLServer?

First try:

- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables

How to check for inserted rows on SQLServer?

First try:

- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger…

How to check for inserted rows on SQLServer?

First try:

- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger…
- Read and understand the trigger

How to check for inserted rows on SQLServer?

First try:

- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger…
- Read and understand the trigger
- Try to respect this trigger by inserting into another table

How to check for inserted rows on SQLServer?

First try:

- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger…
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
- Second slap, this time by a foreign key…

How to check for inserted rows on SQLServer?

First try:

- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger…
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
- Second slap, this time by a foreign key…
- Study the relation between tables

How to check for inserted rows on SQLServer?

First try:

- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger…
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
- Second slap, this time by a foreign key…
- Study the relation between tables
- Take an aspirin

How to check for inserted rows on SQLServer?

First try:

- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger…
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
- Second slap, this time by a foreign key…
- Study the relation between tables
- Take an aspirin
- Try to insert data into a table to respect the trigger and the foreign keys constraints

How to check for inserted rows on SQLServer?

First try:

- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger…
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
- Second slap, this time by a foreign key…
- Study the relation between tables
- Take an aspirin
- Try to insert data into a table to respect the trigger and the foreign keys constraints
- Get kicked by another trigger

How to check for inserted rows on SQLServer?

First try:

- Look for update information in tables
- Find update information in some tables
- Try to insert data in one of the identified tables
- Get slapped by a trigger…
- Read and understand the trigger
- Try to respect this trigger by inserting into another table
- Second slap, this time by a foreign key…
- Study the relation between tables
- Take an aspirin
- Try to insert data into a table to respect the trigger and the foreign keys constraints
- Get kicked by another trigger…
- Throw laptop across the room

How to check for inserted rows on SQLServer?

Second try:

- Define triggers on tables (remember: 108 tables) to trace inserts
- Get SQLServer to activate audit logs

Way too complicated...

SQL profiler to the rescue

- Monitors SQL queries as done on the database
- Use it while WSUS is synchronizing with Microsoft Update

Import update sample:

RPC:Completed	declare @p3 int set @p3=1 declare...	WSUS:WsusService:1800	NETWORK...	NT AUT...	0	829	6	15
RPC:Completed	exec sp_executesql N' exec spSaveXm...	WSUS:WsusService:1800	NETWORK...	NT AUT...	0	48	0	0
Audit Logout		WSUS:WsusService:1800	NETWORK...	NT AUT...	0	42064	415	23
RPC:Completed	exec sp_reset_connection	WSUS:WsusService:1800	NETWORK...	NT AUT...	0	0	0	0

```
declare @p3 int
set @p3=1
declare @p4 int
set @p4=57799
exec spImportUpdate @UpdateXml=N'<upd:Update xmlns:pub="http://schemas.microsoft.com/msus/2002/12/Publishing" xmlns:bar="http://schemas.microsoft.com/msus/2002/12/B
xmlns:upd="http://schemas.microsoft.com/msus/2002/12/Update"><upd:UpdateIdentity UpdateID="be616889-5b81-4bb3-b7c3-d687ffdb358b" RevisionNumber="203" /><upd:Propert
DefaultPropertiesLanguage="en" IsPublic="false" UpdateType="Detectoid" DetectoidType="SKU or Feature" PublicationState="Published" CreationDate="2017-04-25T22:17:03
PublisherID="fa34d14e-27d3-42c2-bc5f-070f466300d1"></upd:Properties><upd:LocalizedPropertiesCollection><upd:LocalizedProperties><upd:Language>en</upd:Language><upd:
in Release Preview ring</upd:Title><upd:Description>Evaluates to true if the RegKey value for RingId is
8</upd:Description></upd:LocalizedProperties></upd:LocalizedPropertiesCollection><upd:Relationships><upd:Prerequisites><upd:AtLeastOne><upd:UpdateIdentity
UpdateID="05EEBF61-148B-43CF-80DA-1C99AB0B8699" /><upd:UpdateIdentity UpdateID="C1006636-EAB4-4B0B-B1B0-D50282C0377E"
/></upd:AtLeastOne></upd:Prerequisites></upd:Relationships><upd:ApplicabilityRules><upd:IsInstalled><bar:RegDword Key="HKEY_LOCAL_MACHINE"
Subkey="Software\Microsoft\WindowsSelfHost\Applicability" Value="RingId" Comparison="EqualTo" Data="8" xmlns:bar="http://schemas.microsoft.com/msus/2002/12/BaseAppl
/></upd:IsInstalled></upd:ApplicabilityRules></upd:Update>',@UpstreamServerLocalID=1,@Imported=@p3 output,@localRevisionID=@p4 output
select @p3, @p4
```

Notice the horizontal slider? It's a **very** large XML

Isolate the right calls

- WSUS service is only using stored procedure calls

- Calls five stored procedures to insert one update:
  - spImportUpdate
  - spSaveXmlFragment (actually called a bunch of times)
  - spSetBatchURL
  - spDeploymentAutomation
  - spProcessPrerequisitesForRevision

Isolate the right calls

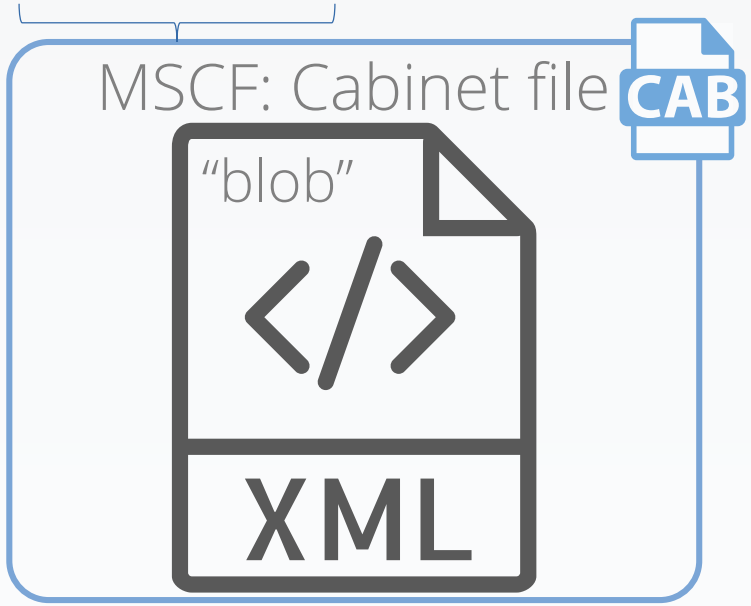
- WSUS service is only using stored procedure calls

- Calls five stored procedures to insert one update:
  - spImportUpdate
  - spSaveXmlFragment (actually called a bunch of times)
  - spSetBatchURL
  - spDeploymentAutomation
  - spProcessPrerequisitesForRevision

Copy/Paste a valid update

- Lessons learned:
  - Image-typed columns can store cab files
    - Which can store a file named “blob”
      - Which can store an even bigger XML
      - Ones bigger than SQLServer’s NVARCHAR max size (8K)

spSaveXmlFragment NULL,4D53434600000000FB07...



Copy/Paste a valid update

- Lessons learned:
  - Minimalization cannot be pushed too far
    - Works on Windows 7 and Windows 10:1607

1607

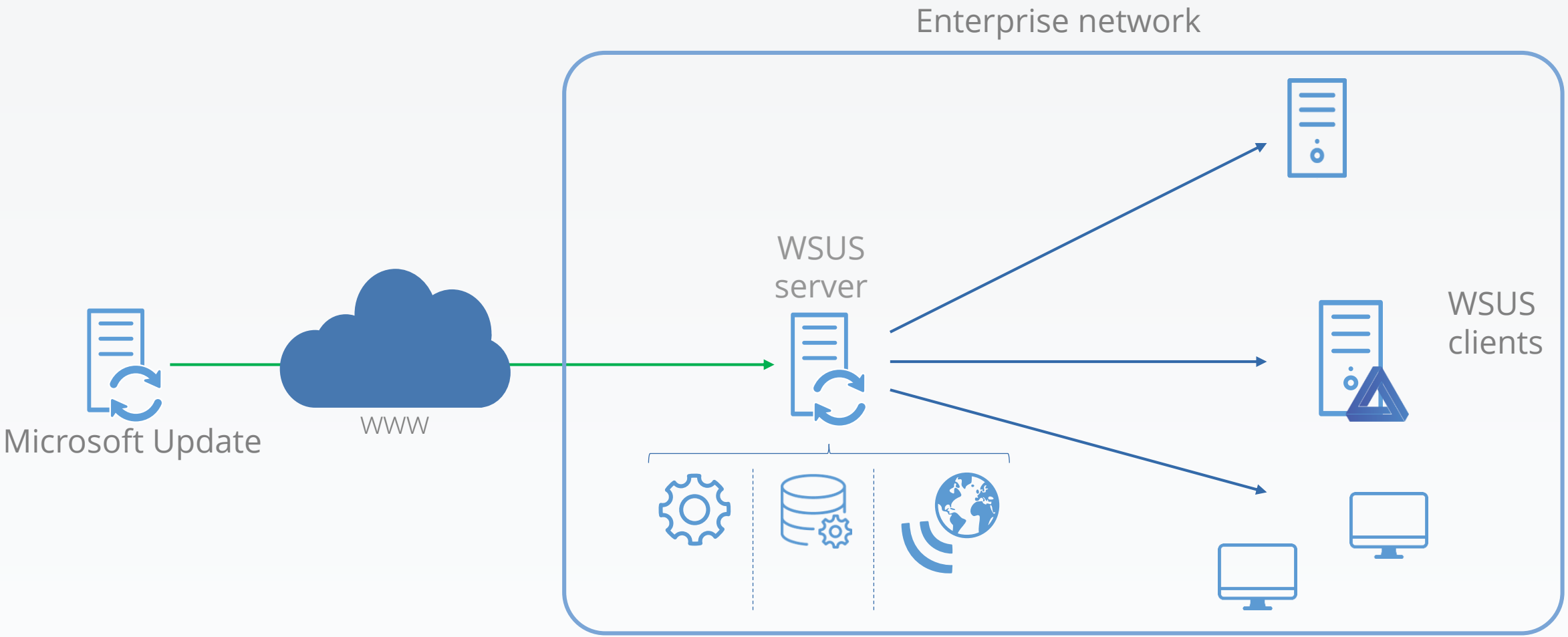
Copy/Paste a valid update

- Lessons learned:
  - Minimalization cannot be pushed too far
    - Works on Windows 7 and Windows 10:1607
      - Doesn't work on versions in-between
      - Doesn't work on server versions

✗ 2008(R2) ✗ 2012(R2) ✗ 2016

Introducing WSUSpendu[@]

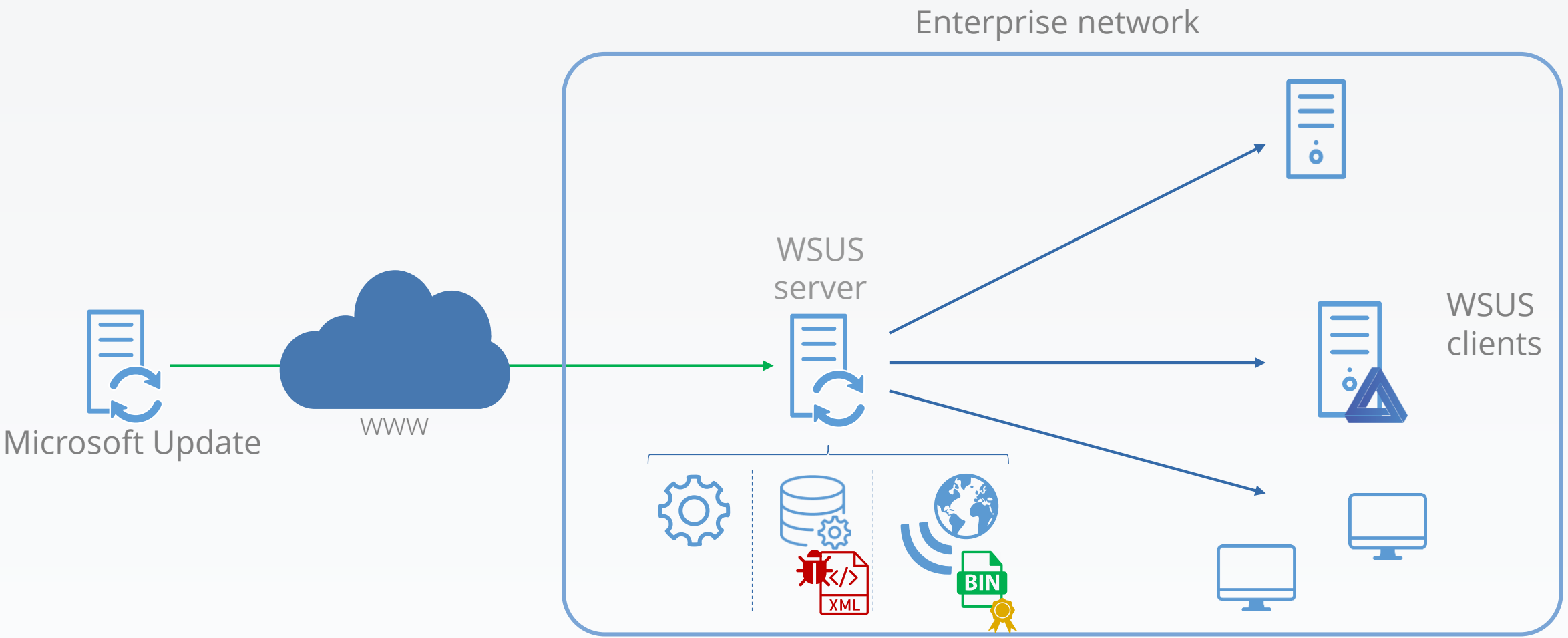
Open-source: https://github.com/AlsidOfficial/WSUSpendu



[@] Thx Maman

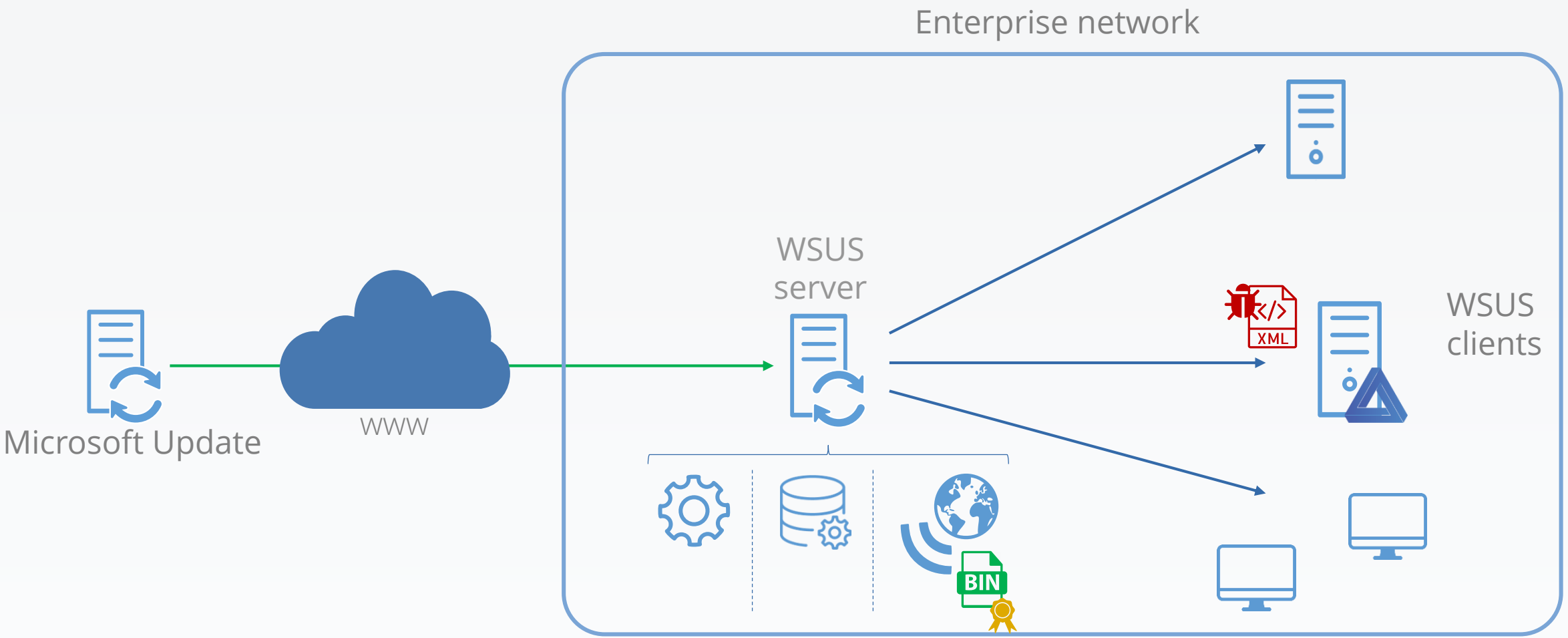
Introducing WSUSpendu

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



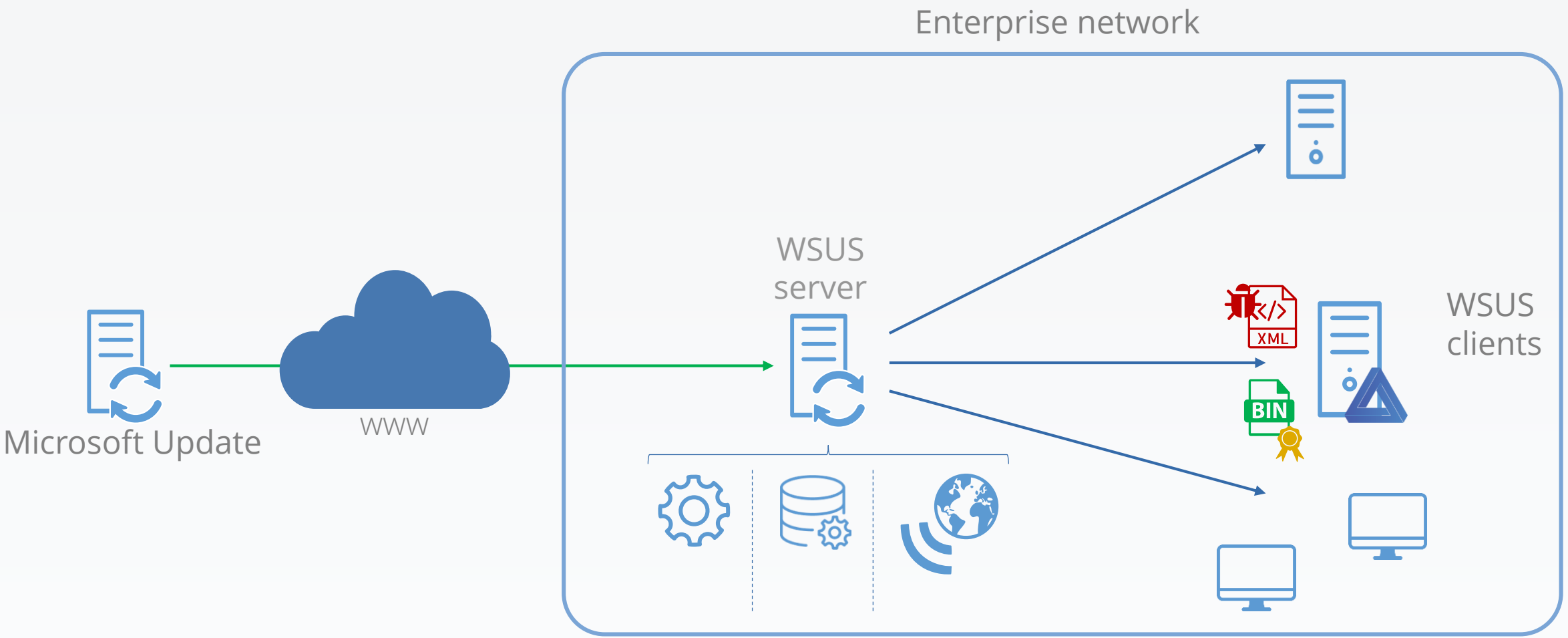
Introducing WSUSpendu

2. The client sees a new available and installable update



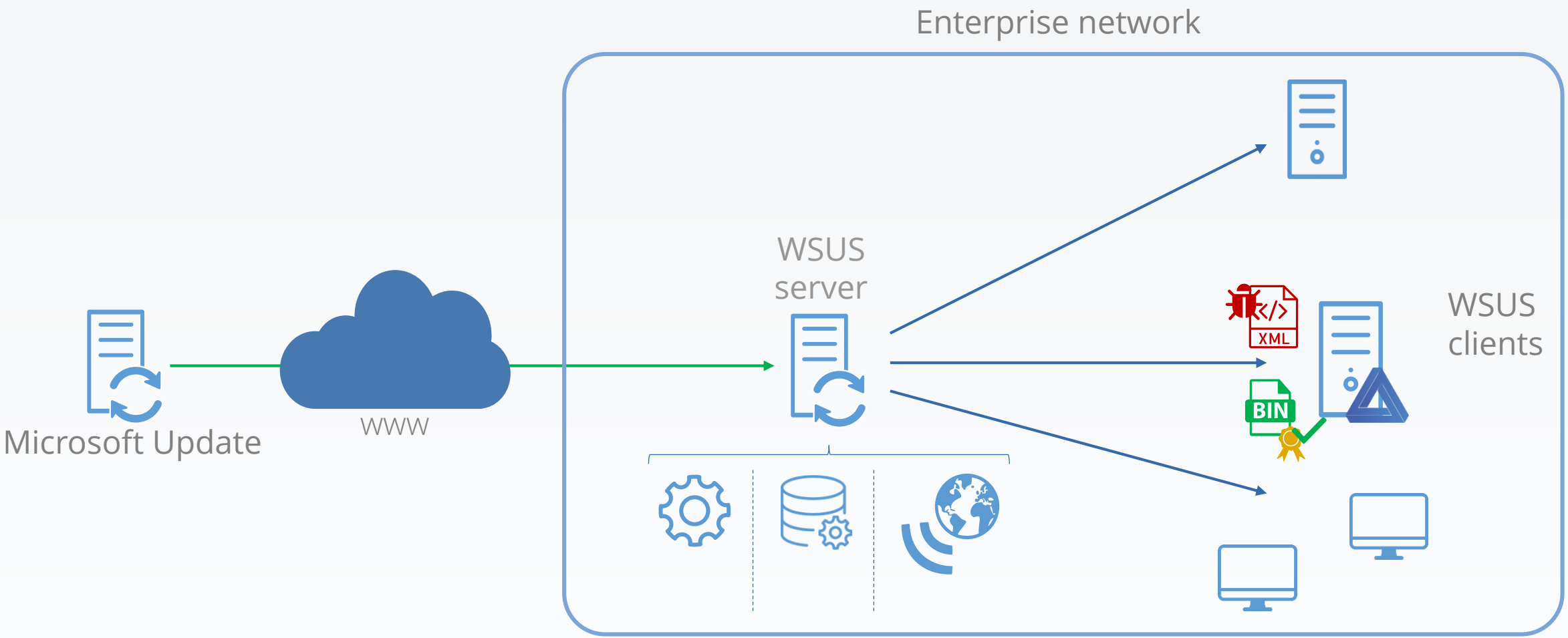
Introducing WSUSpendu

3. Fetches the related binary



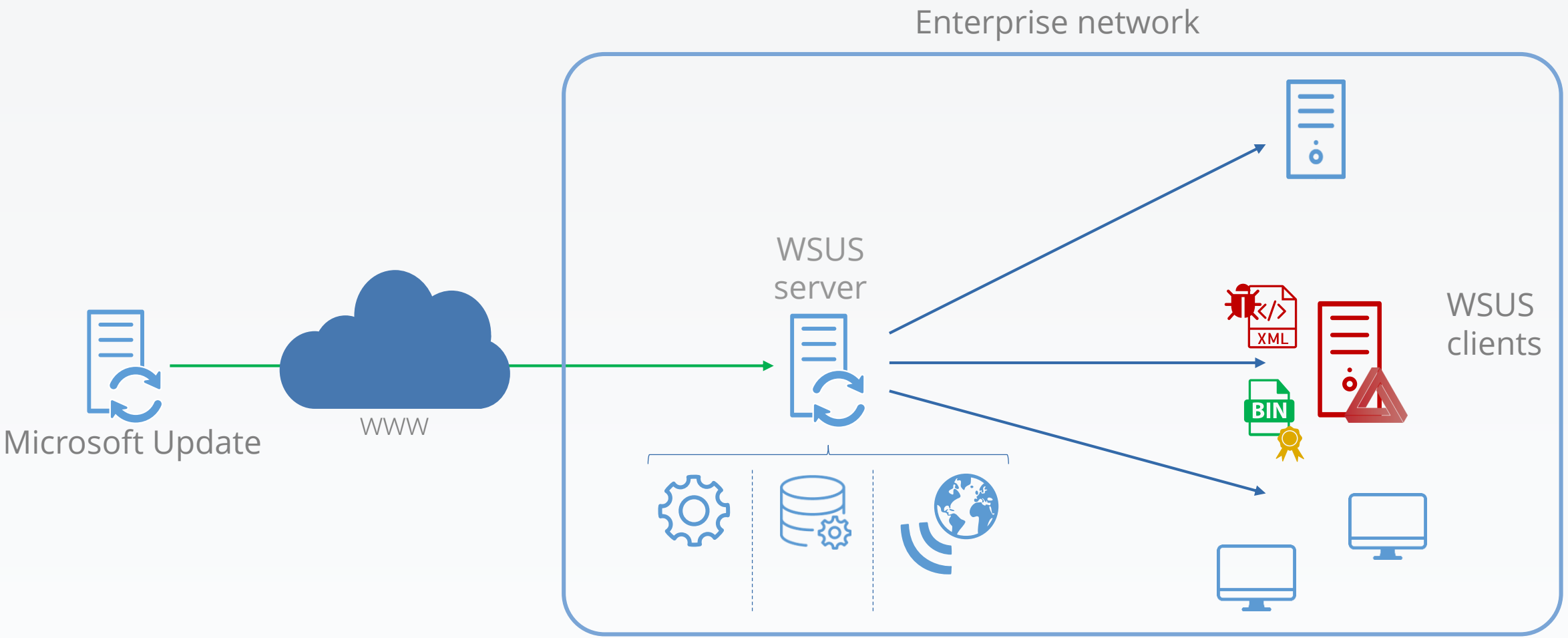
Introducing WSUSpendu

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



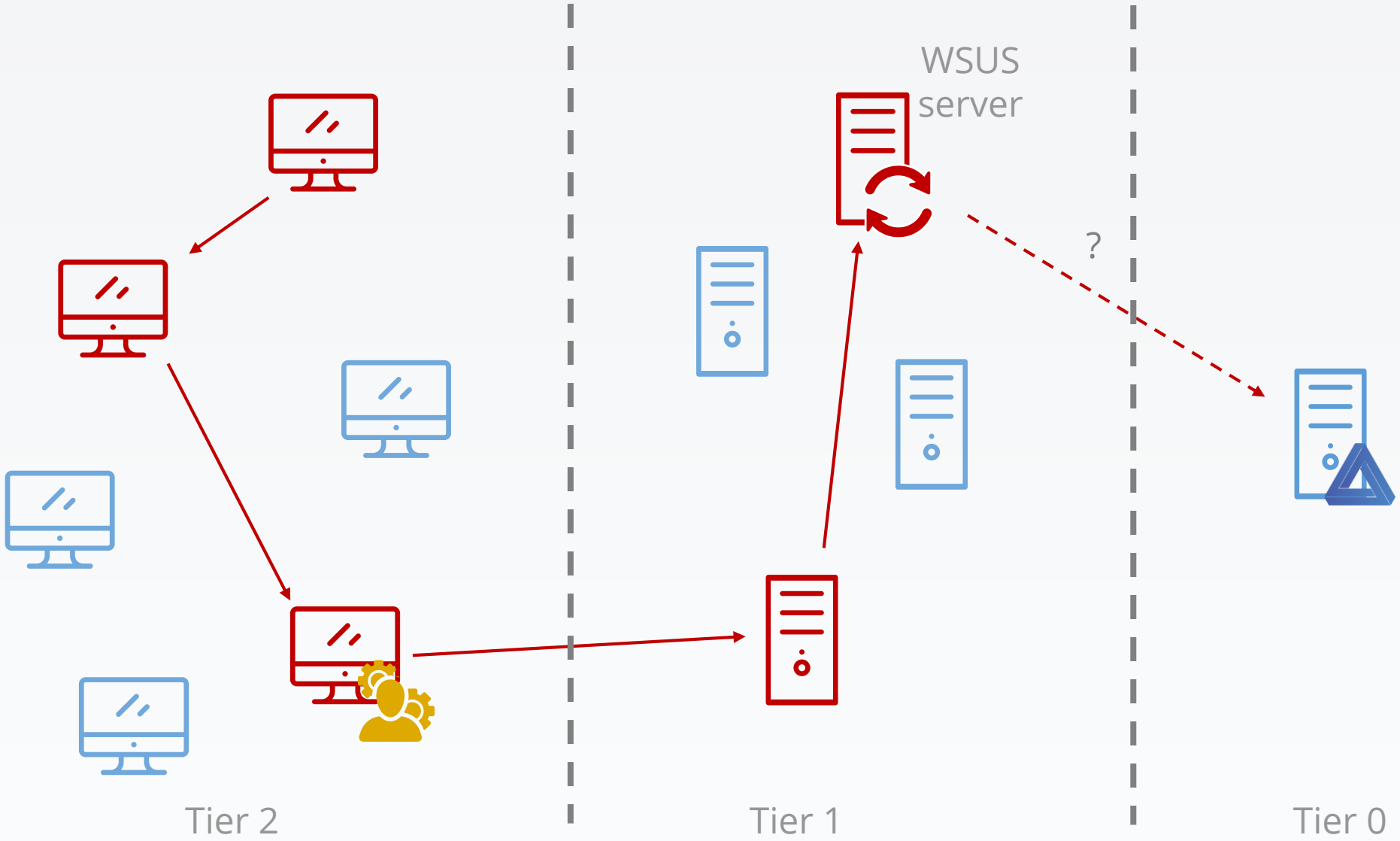
Introducing WSUSpendu

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

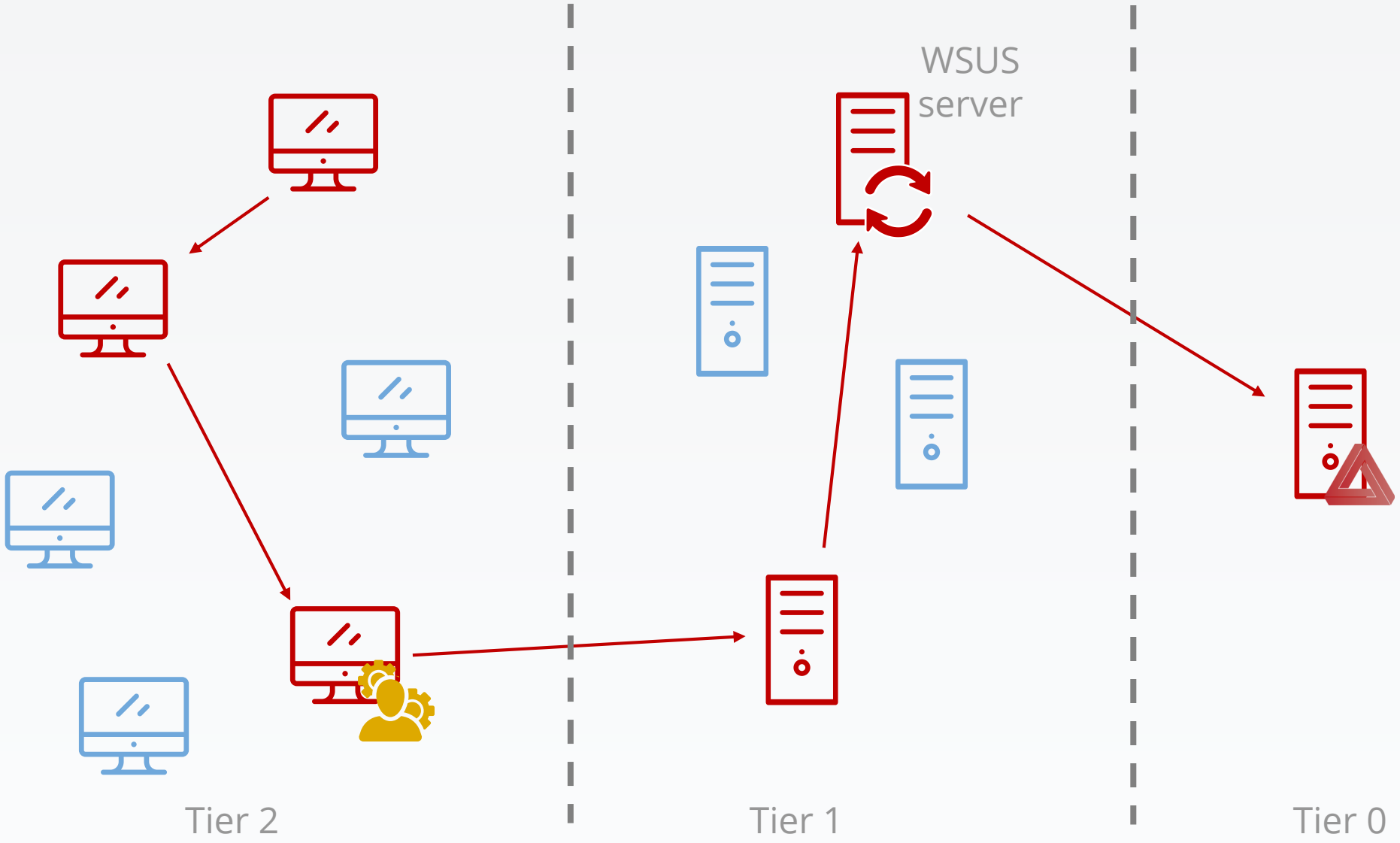


Demonstration...

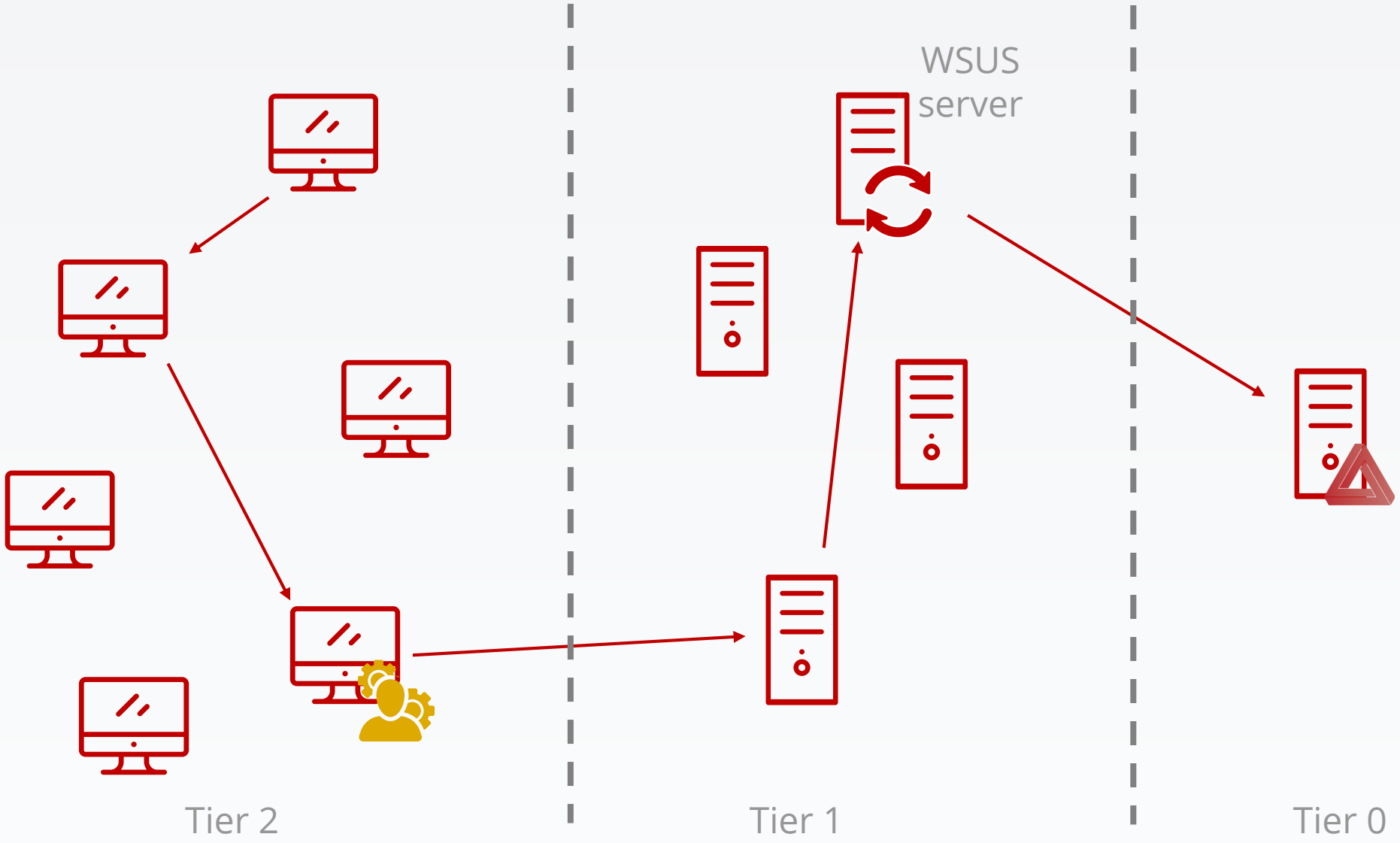
What if a WSUS server serves updates to the DCs?



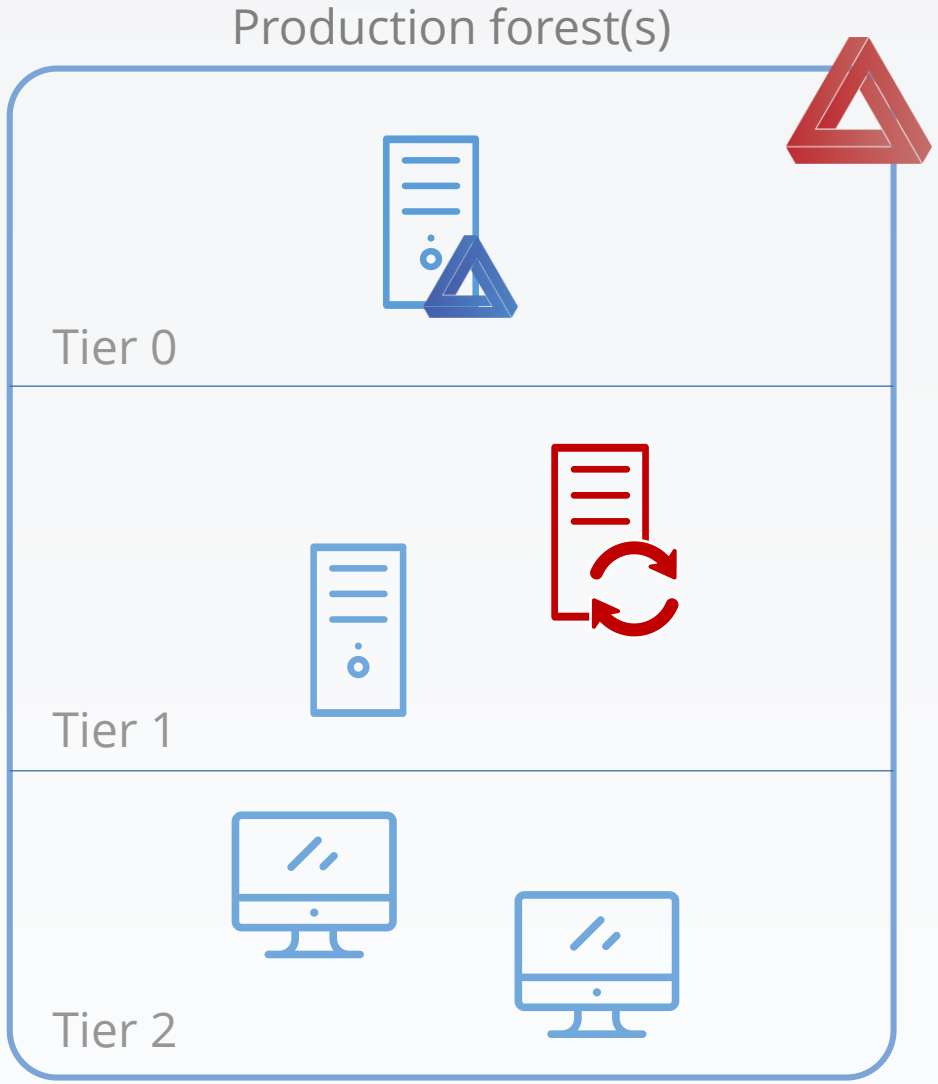
Compromise an ESAE-managed forest



Compromise an ESAE-managed forest

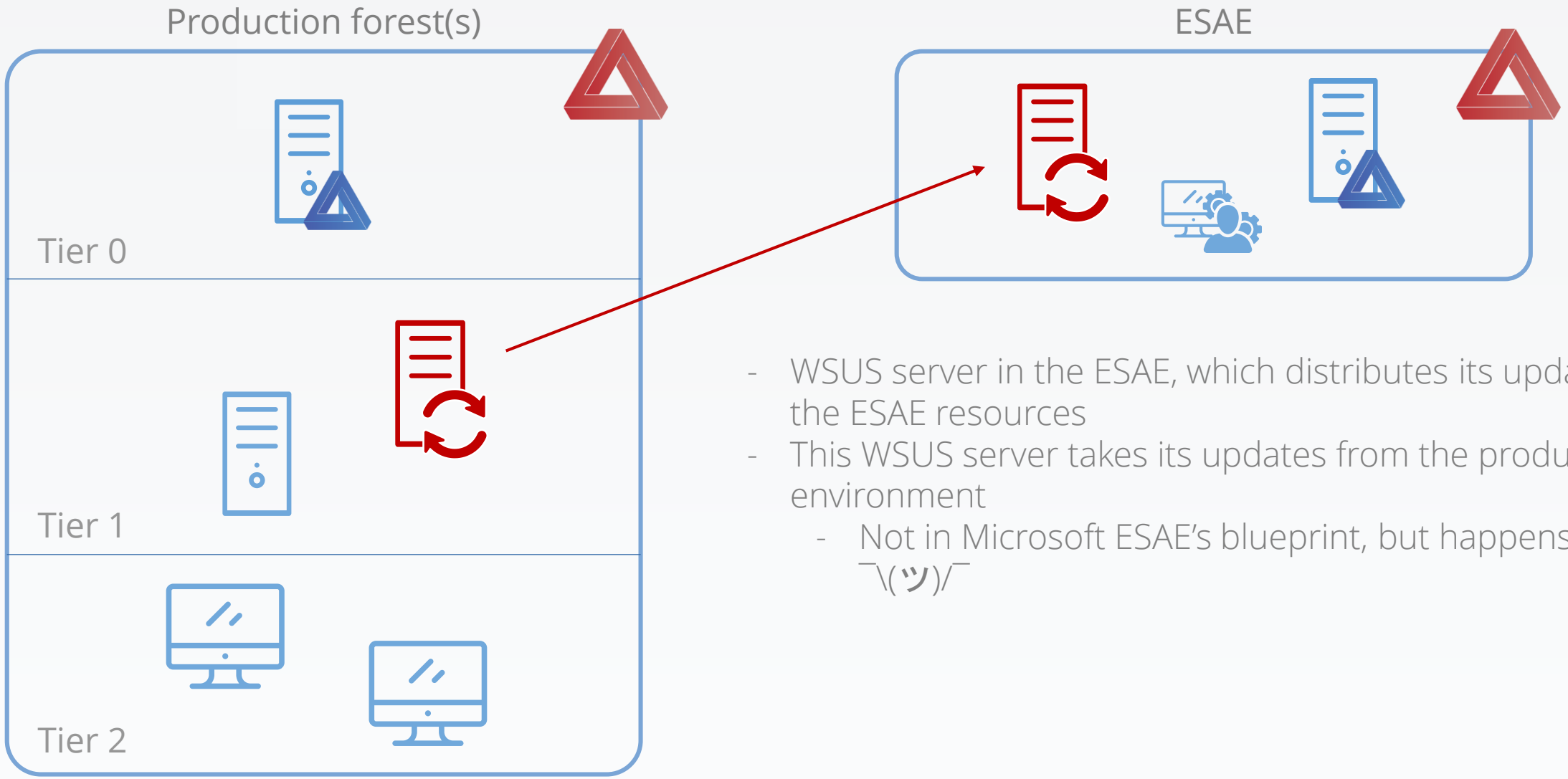


Sometimes, even compromise the ESAE forest itself



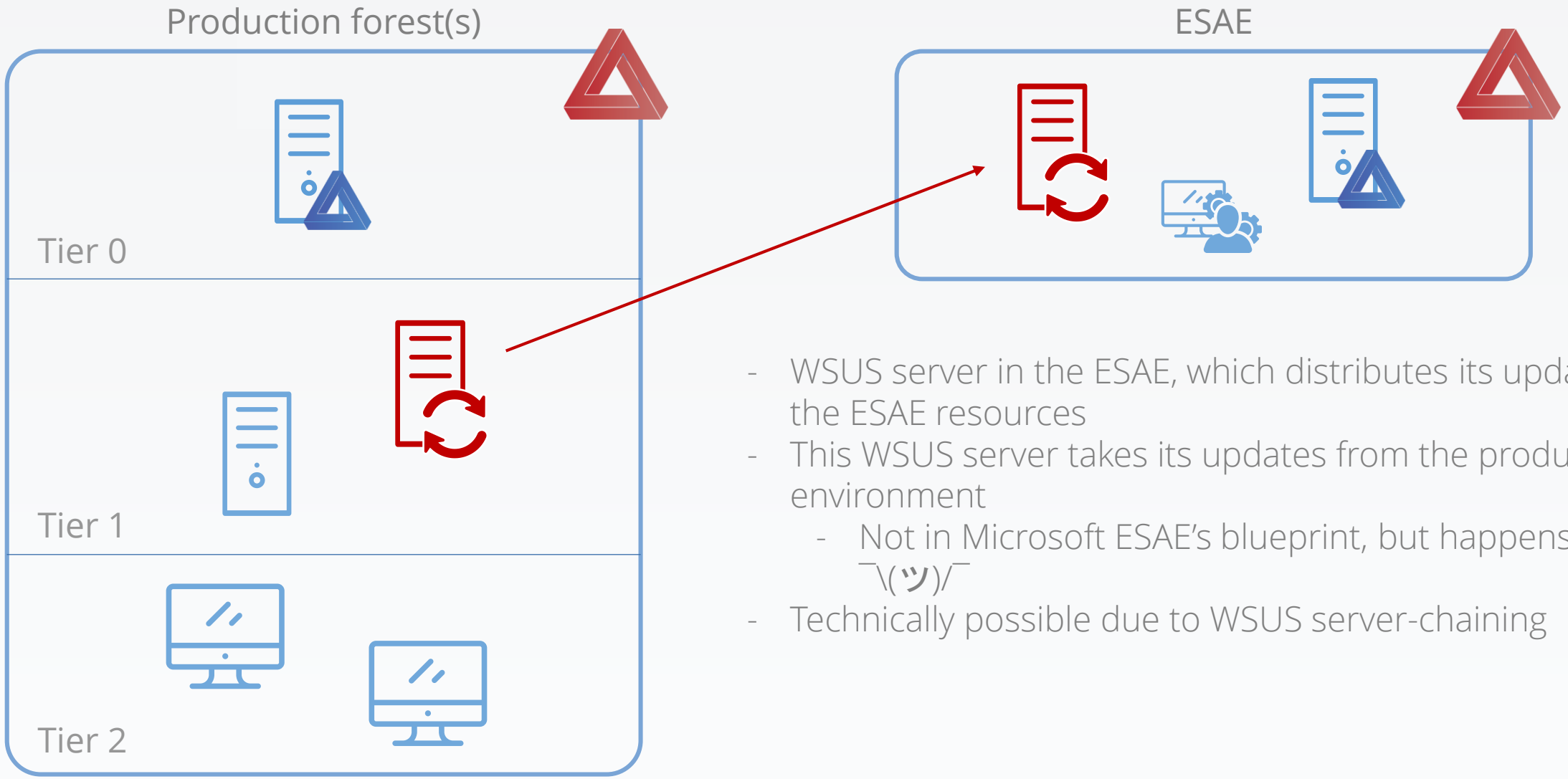
- WSUS server in the ESAE, which distributes its updates to the ESAE resources

Sometimes, even compromise the ESAE forest itself



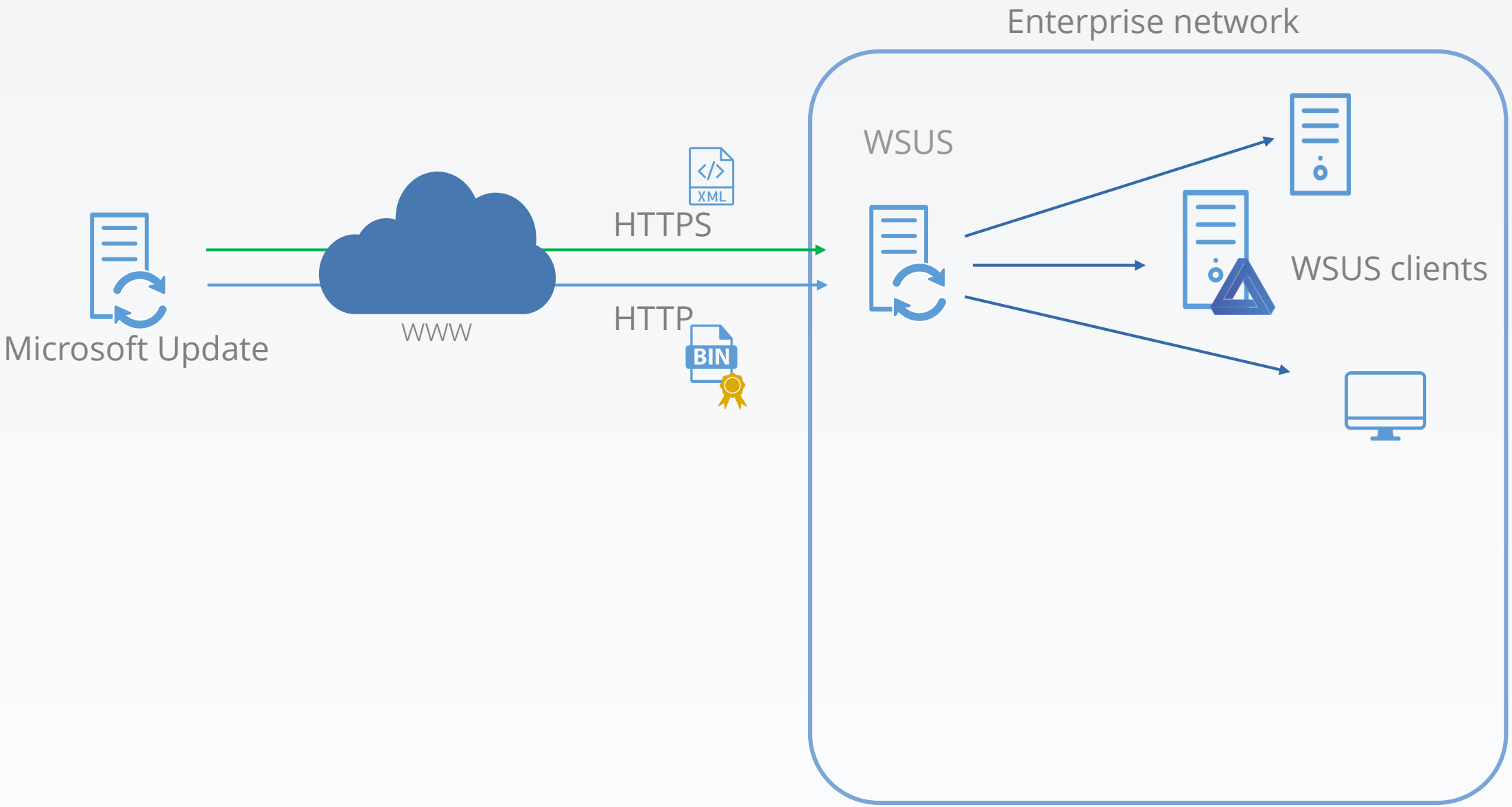
- WSUS server in the ESAE, which distributes its updates to the ESAE resources
- This WSUS server takes its updates from the production environment
  - Not in Microsoft ESAE's blueprint, but happens ¯\(ツ)/¯

Sometimes, even compromise the ESAE forest itself

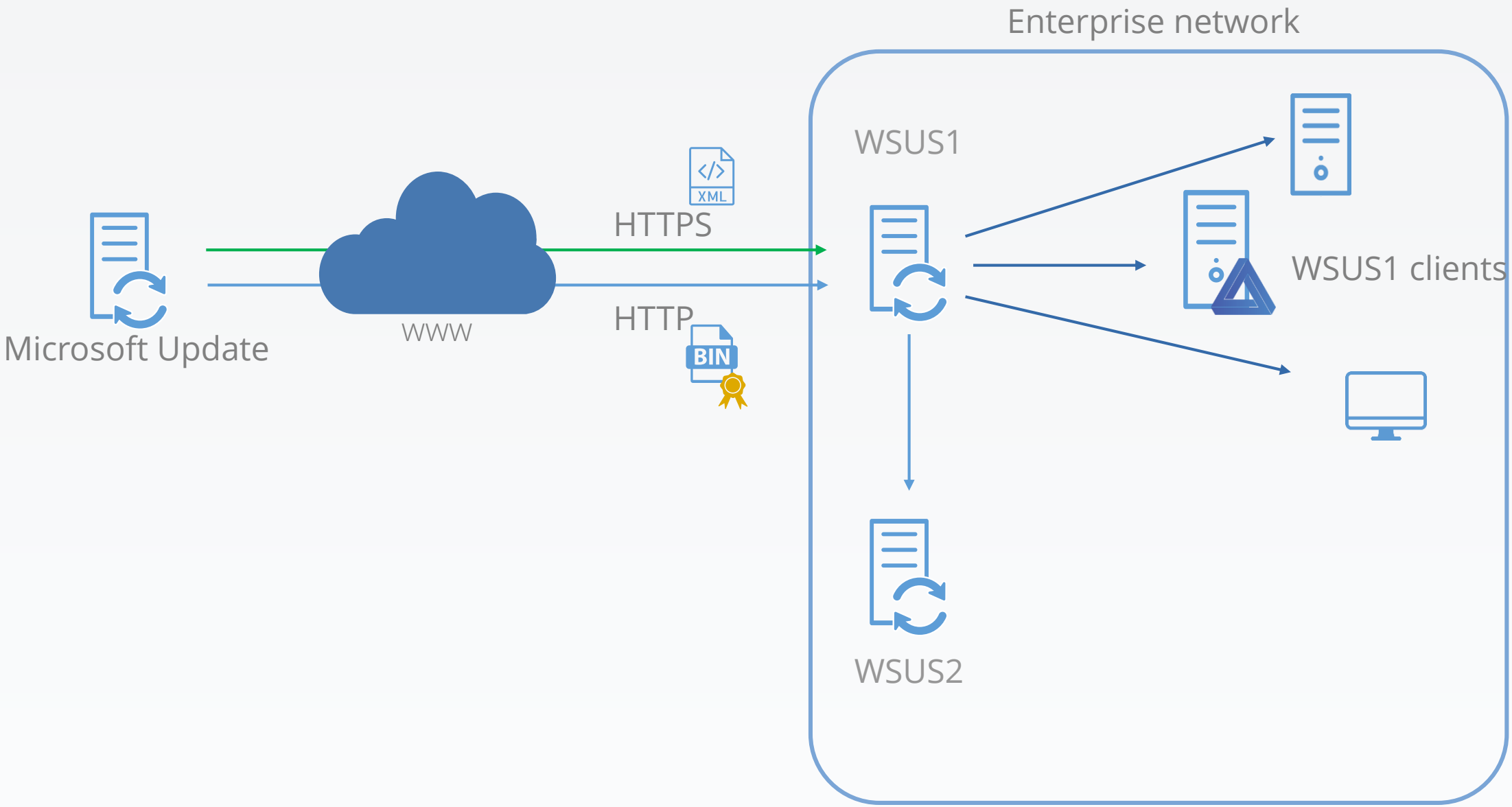


- WSUS server in the ESAE, which distributes its updates to the ESAE resources
- This WSUS server takes its updates from the production environment
  - Not in Microsoft ESAE's blueprint, but happens ¯\(ツ)/¯
- Technically possible due to WSUS server-chaining

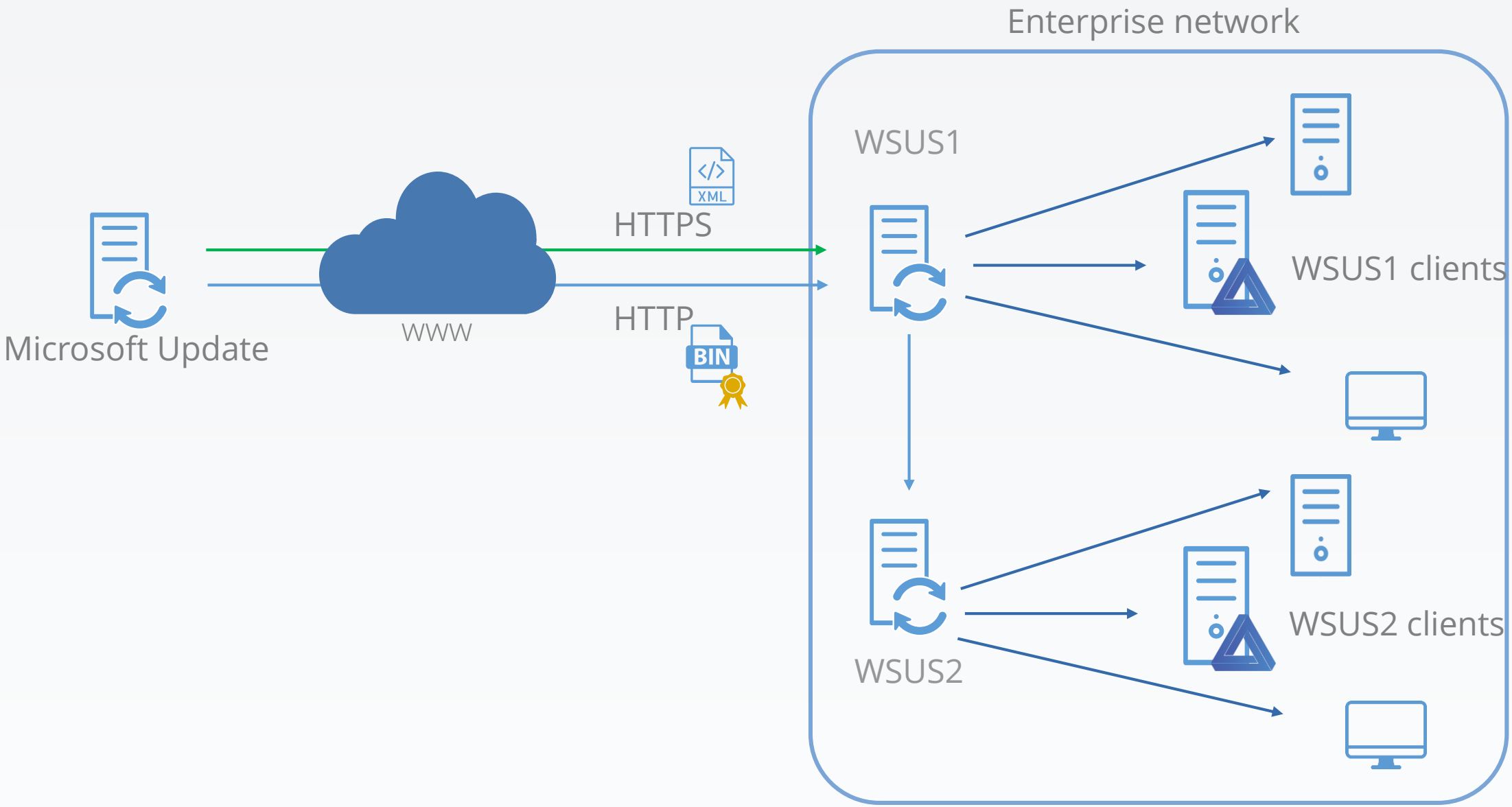
Upstream/Downstream update servers notion



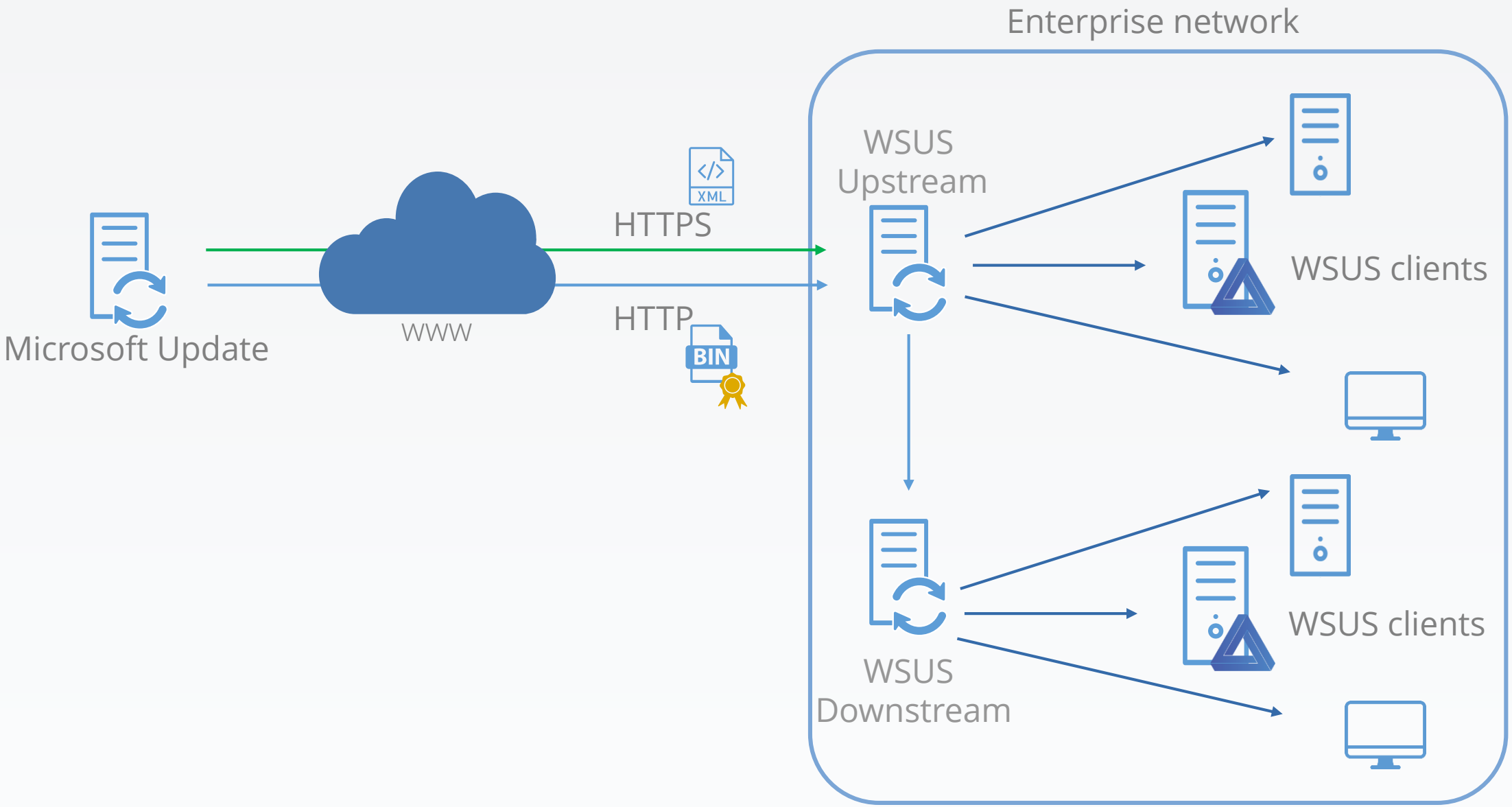
Upstream/Downstream update servers notion



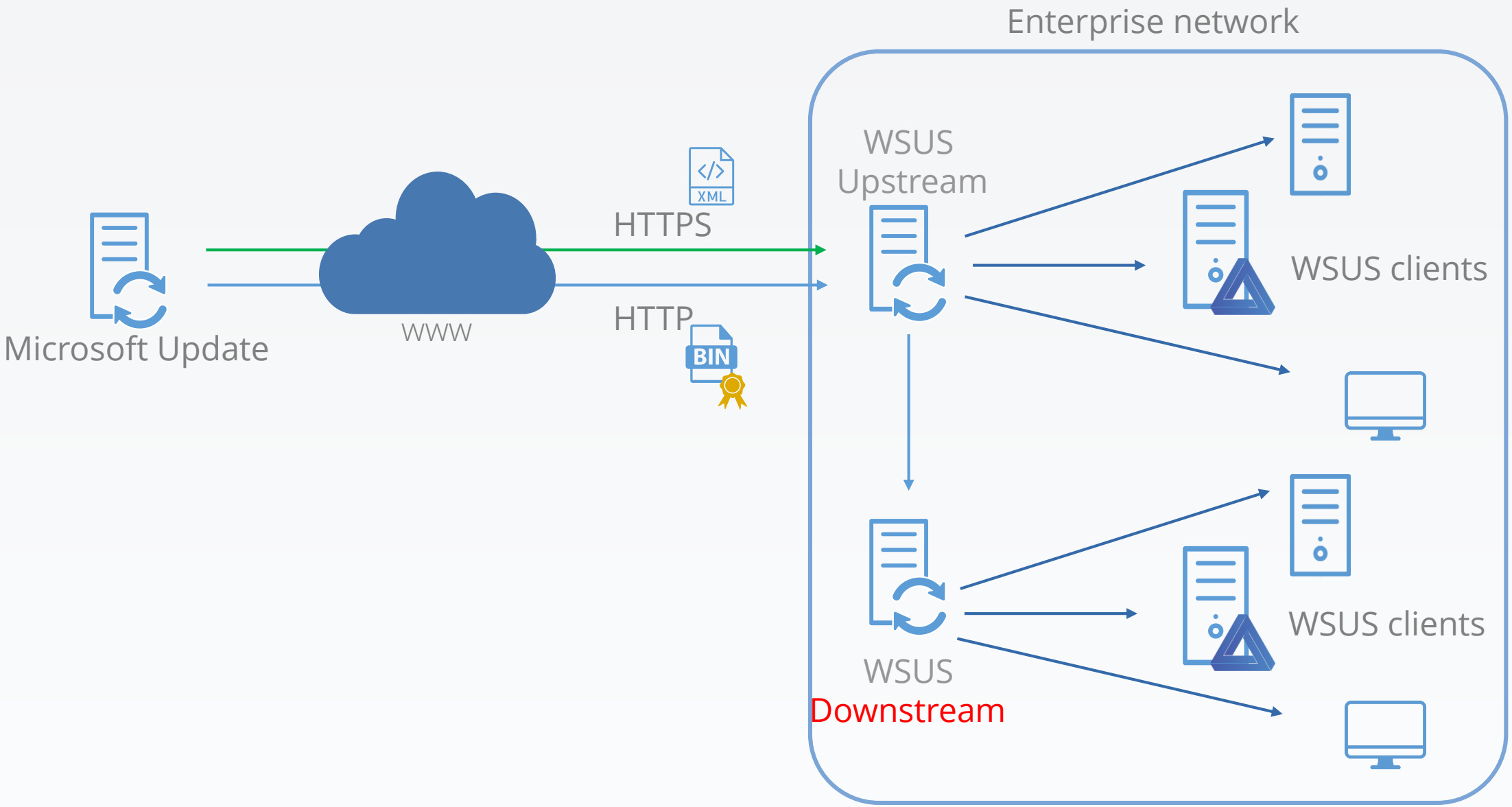
Upstream/Downstream update servers notion



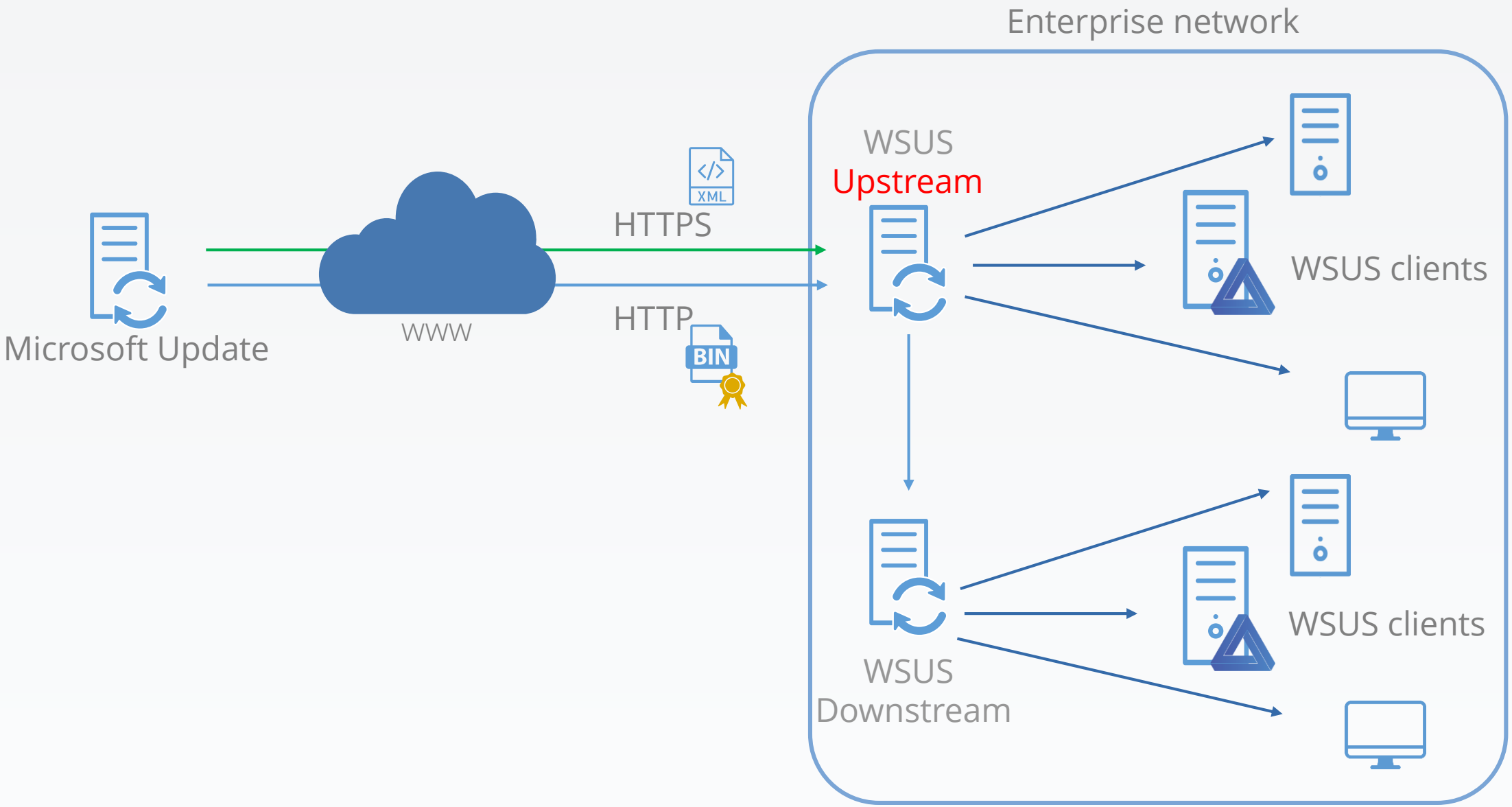
Upstream/Downstream update servers notion



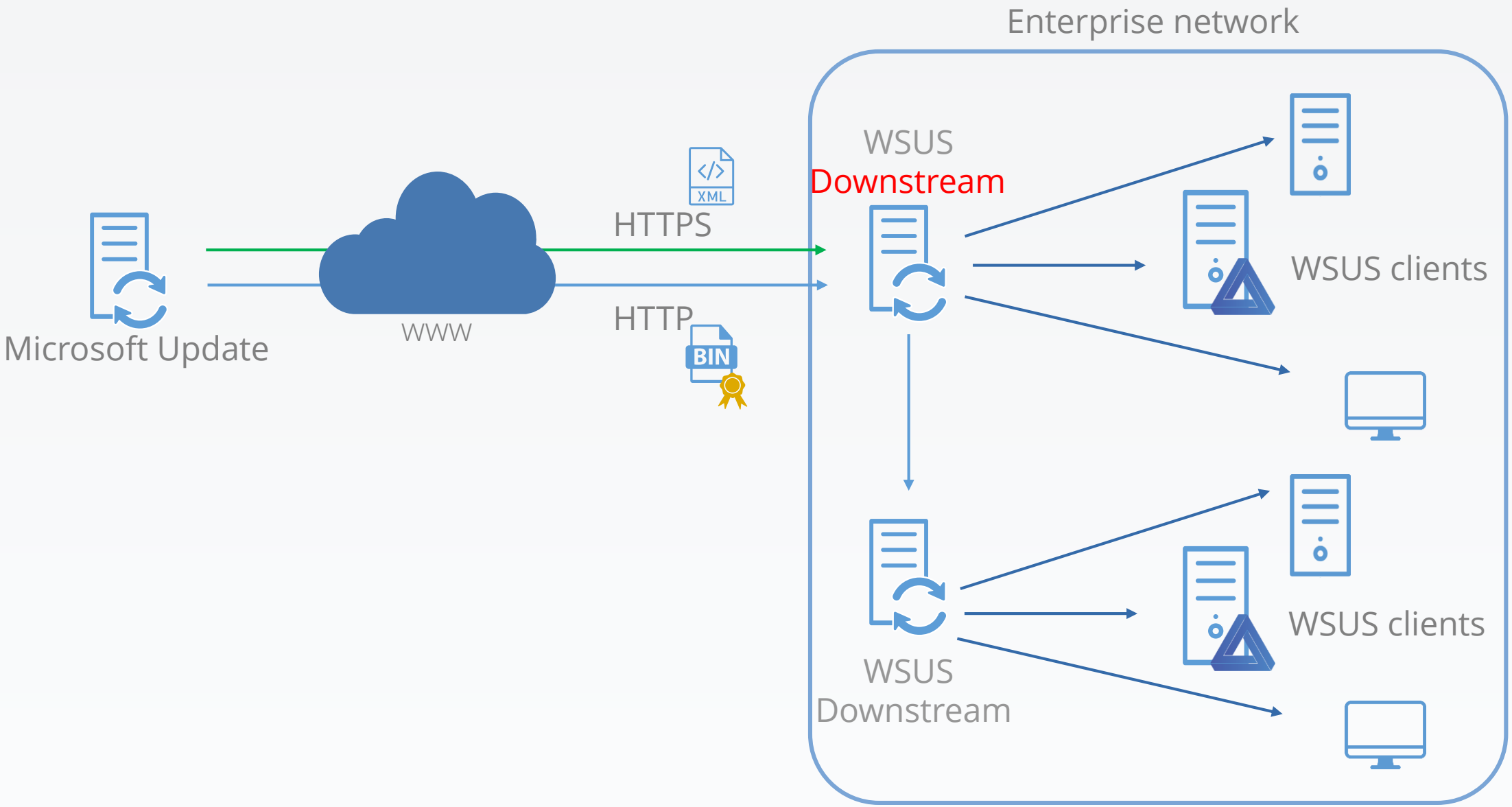
Upstream/Downstream update servers notion



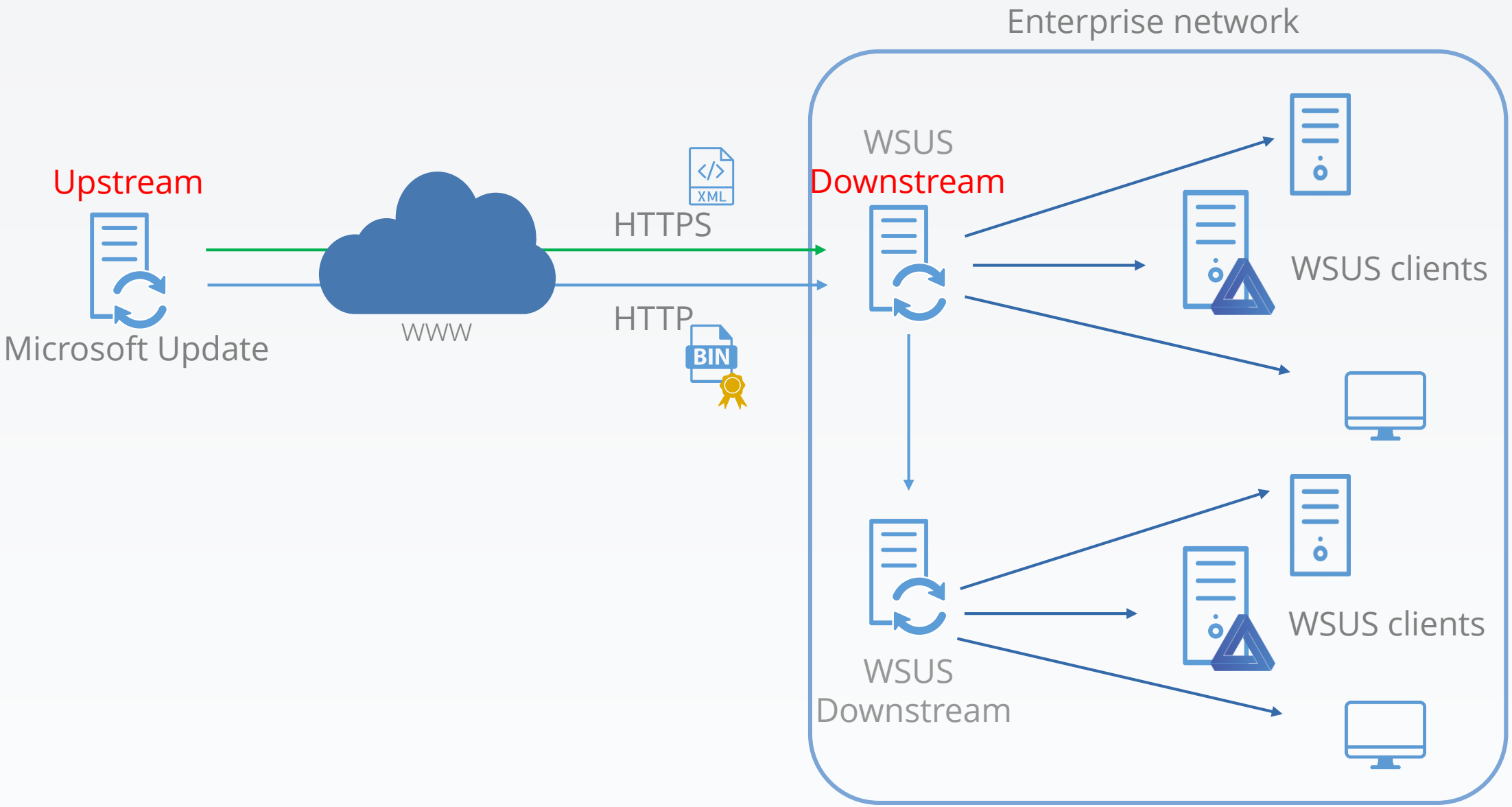
Upstream/Downstream update servers notion



Upstream/Downstream update servers notion



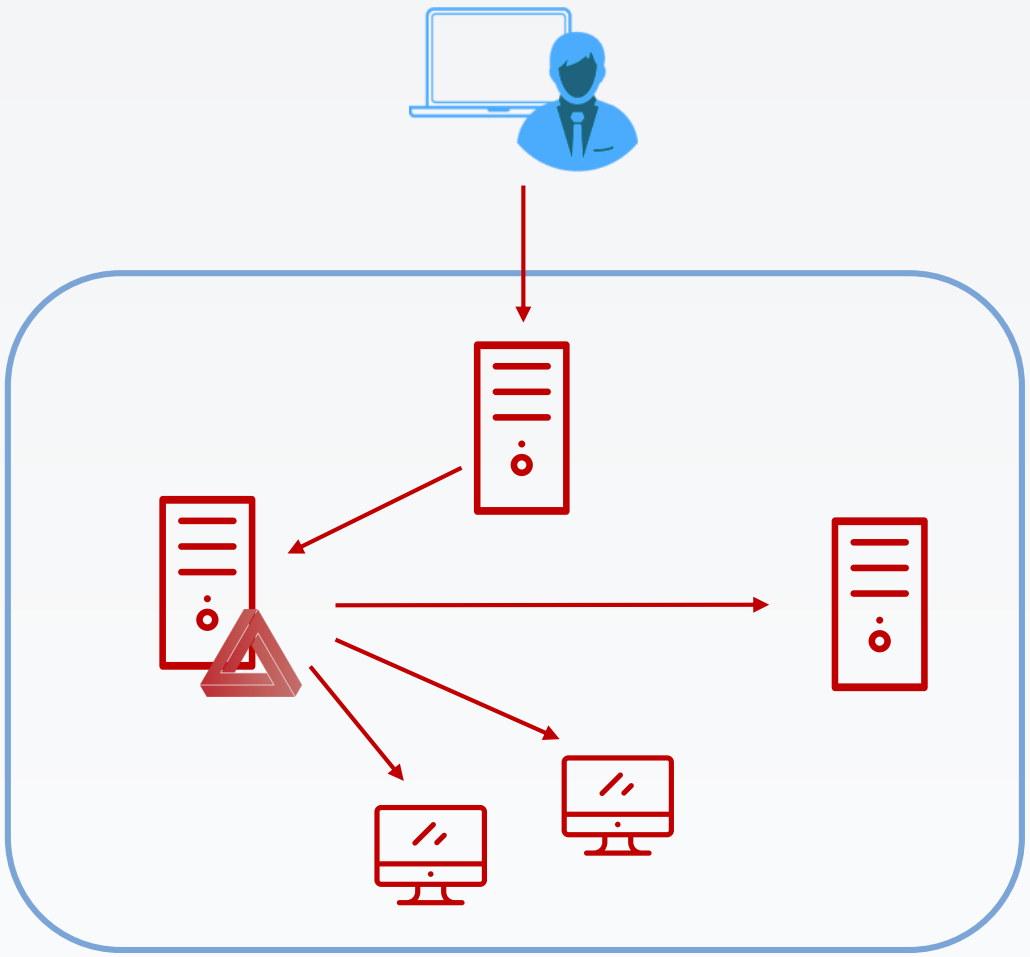
Upstream/Downstream update servers notion



Compromising Microsoft’s most secure environment was almost too easy.

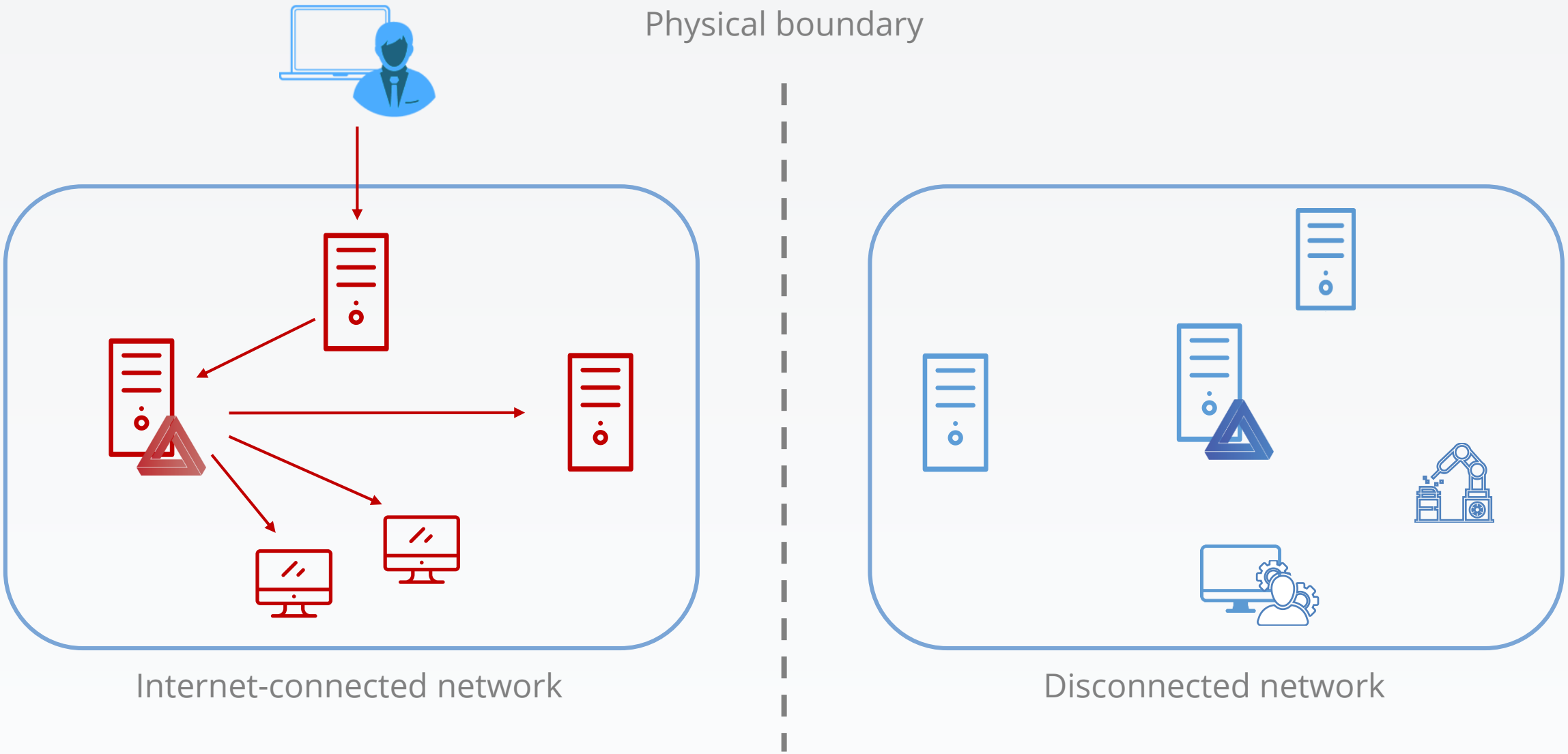
We need to go deeper…

Disconnected network case



Internet-connected network

Disconnected network case



Using disconnected network

Why?

- Protect sensitive data, classified information
- Protect industrial networks
- Just don’t want to be connected to the Internet…

Using disconnected network

Why?
- Protect sensitive data, classified information
- Protect industrial networks
- Just don’t want to be connected to the Internet…

For which security improvement?
- Isolation as protection
- "No reach, no issue"

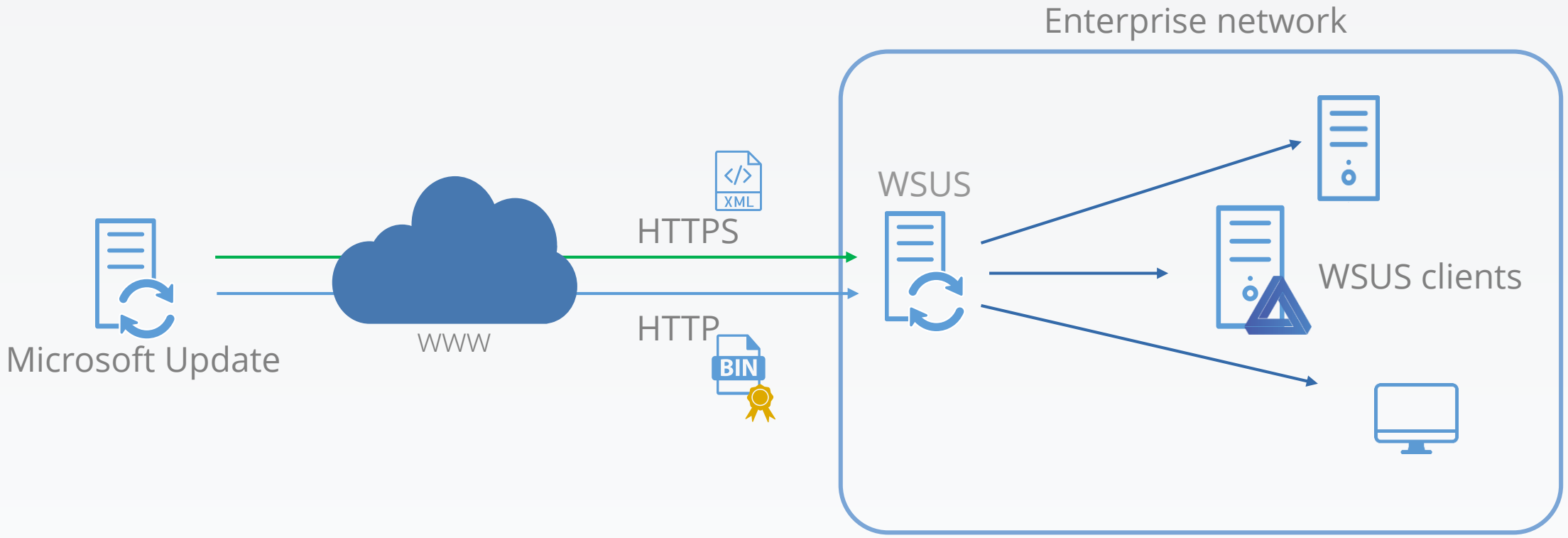
Using disconnected network

Why?
- Protect sensitive data, classified information
- Protect industrial networks
- Just don’t want to be connected to the Internet…

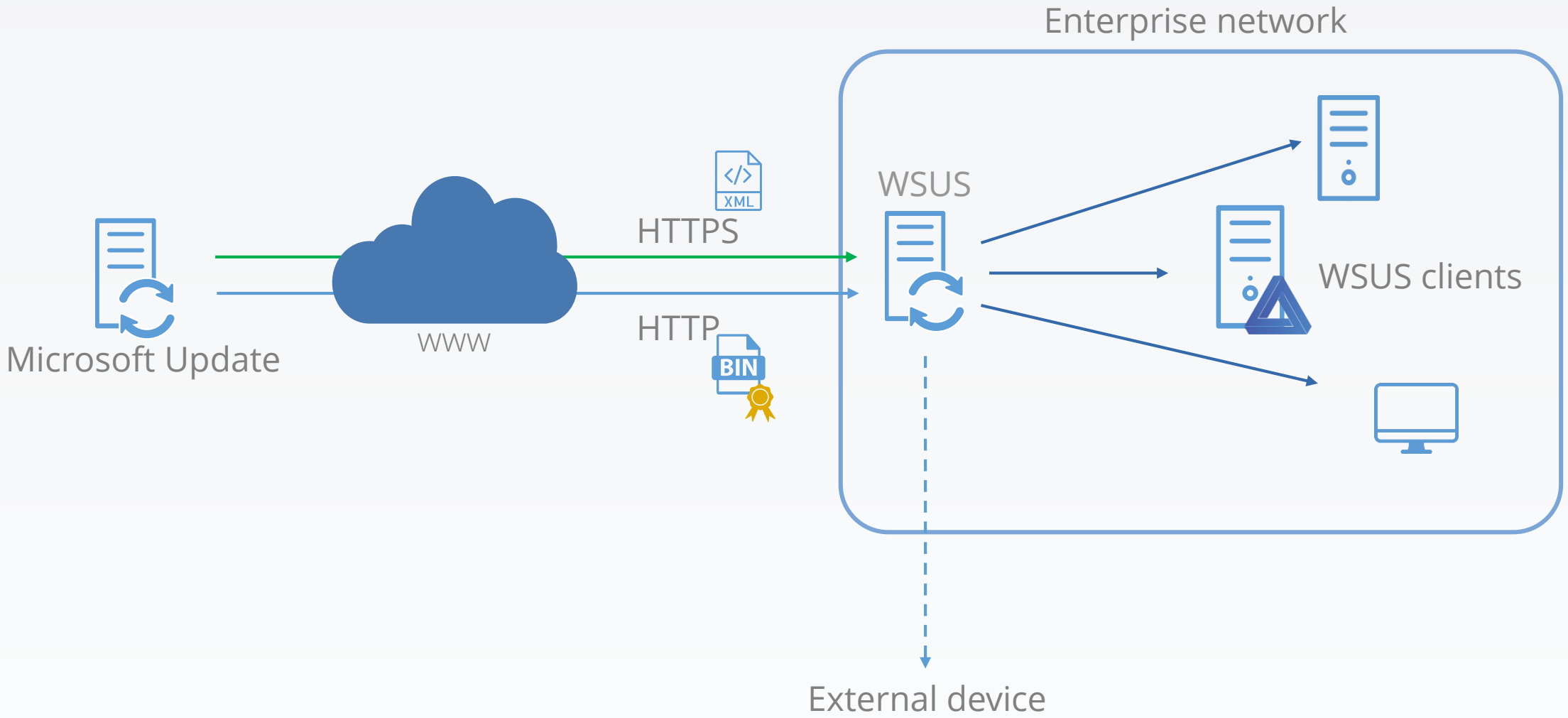
For which security improvement?
- Isolation as protection
- "No reach, no issue"

Is it sufficient? … Due to sensitivity, you have to:
- continue securing your network/servers/apps/…
- thus, stay up-to-date

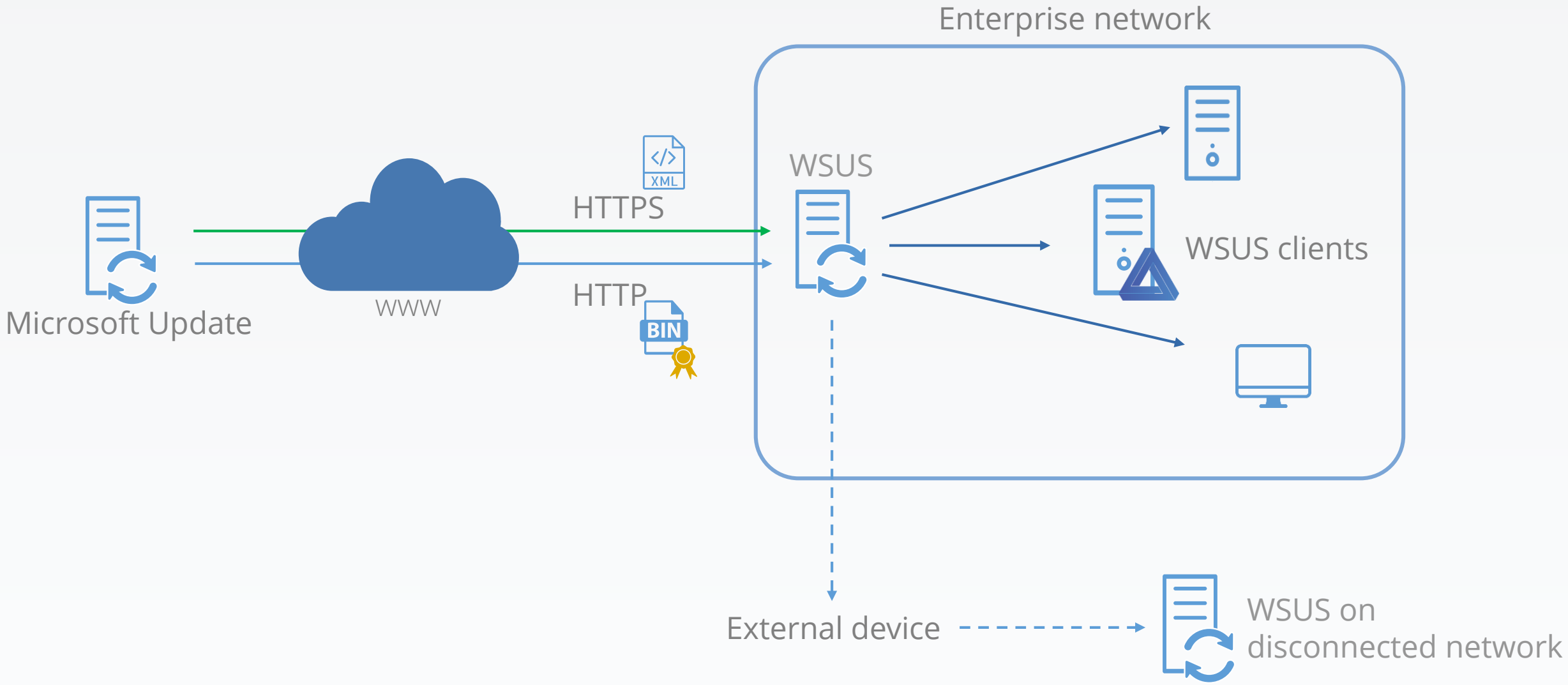
Updates for disconnected network



Updates for disconnected network



Updates for disconnected network



Get updates to the disconnected network

Microsoft solution:

- wsusutil, export / import tool for metadata
- Binaries need to be transfered manually

Note
It can take three to four hours for the WSUS database to validate newly imported content.

Get updates to the disconnected network

Microsoft solution:

- wsusutil, export / import tool for metadata
- Binaries need to be transfered manually

Note
It can take three to four hours for the WSUS database to validate newly imported content.

Mostly-used solution:

- WSUS on a Virtual Machine
- Clone the VM
- Transfer the clone onto the disconnected network

WSUSpendu & disconnected network

Once metadata are imported, still needs approbation

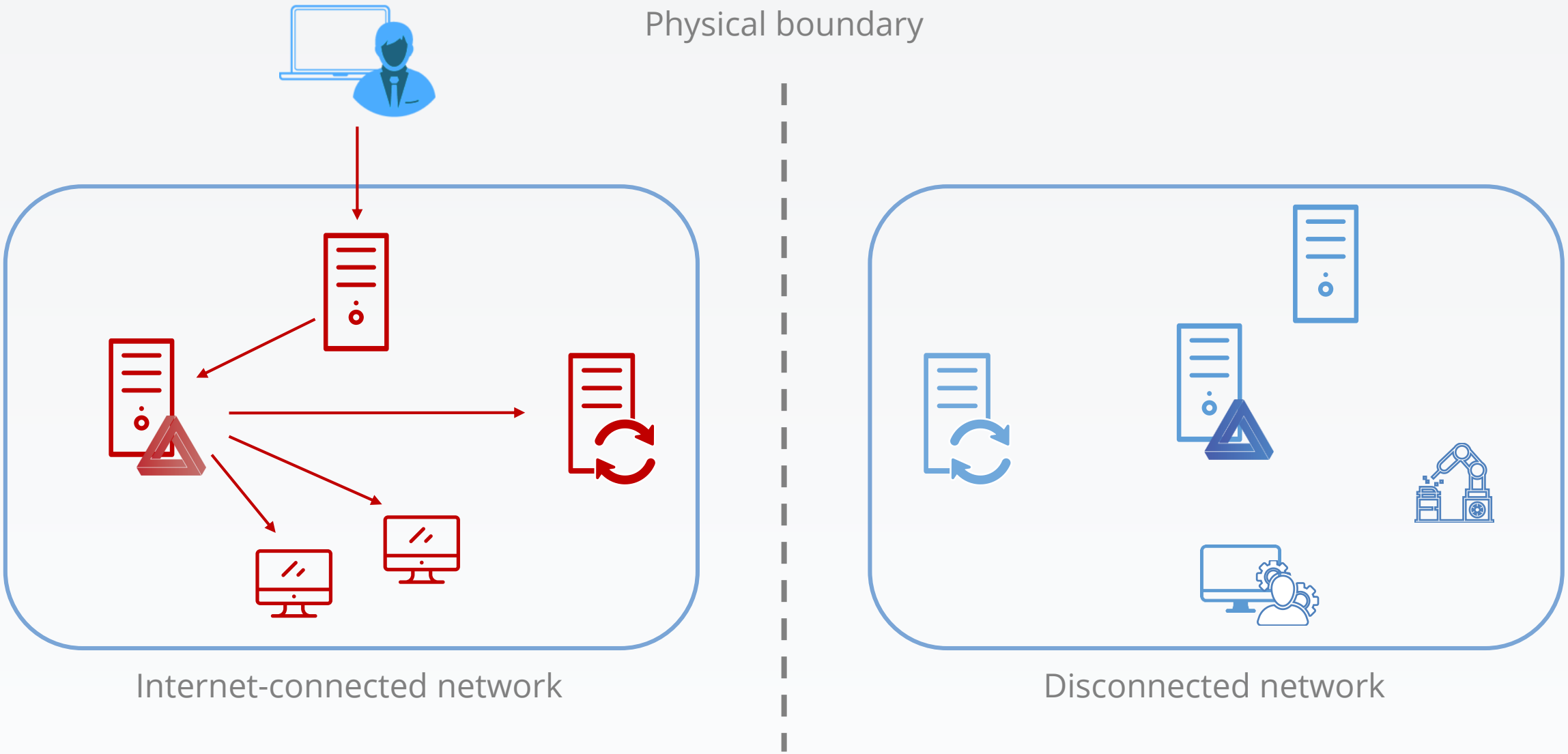
- Approbation through auto-approval rules
- Social Engineering

Airgap-attack ready

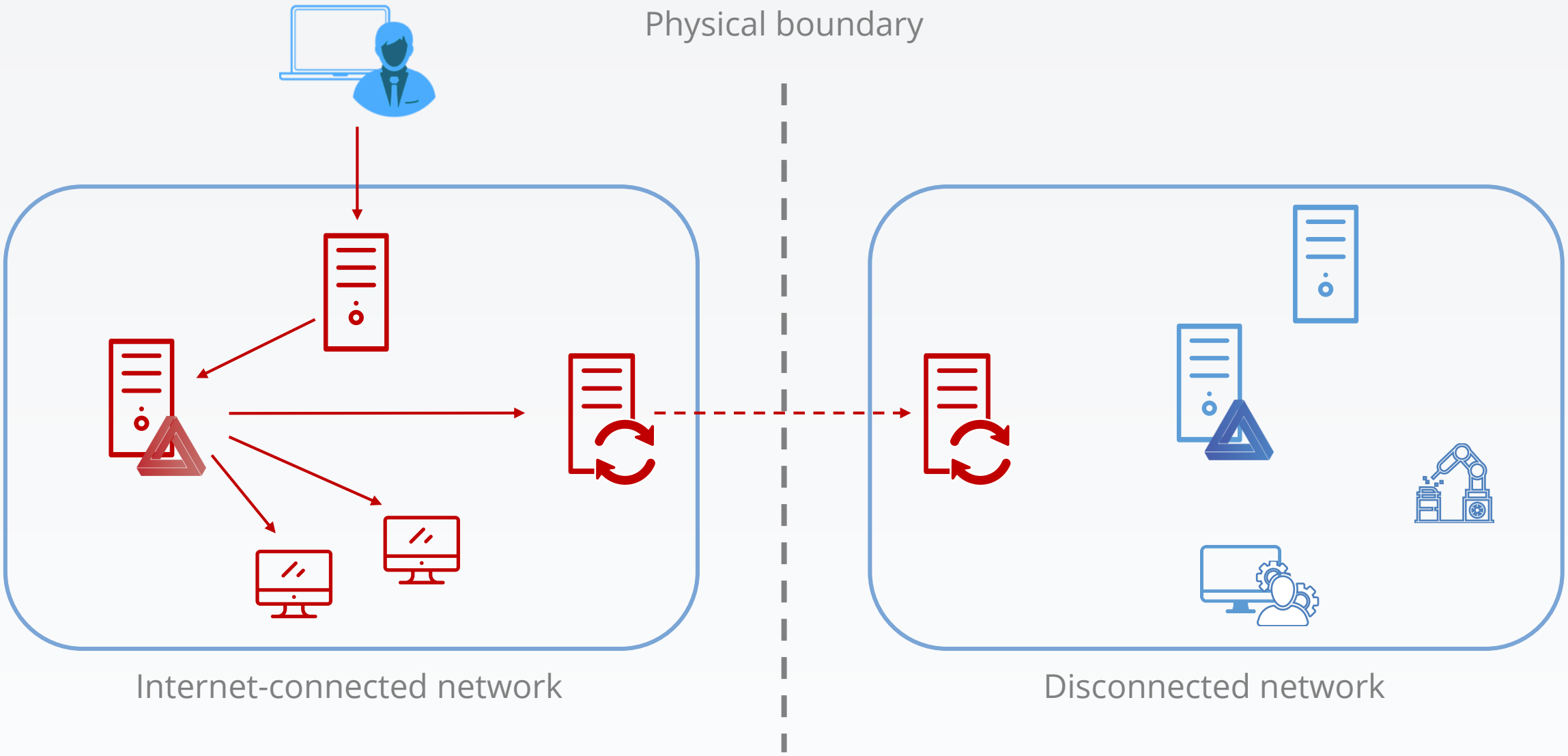
- Inject malicious update in database
- Disconnected database is syncronised with connected database
- Update is approved and deployed
- Payload is executed on designated target…

Demonstration...

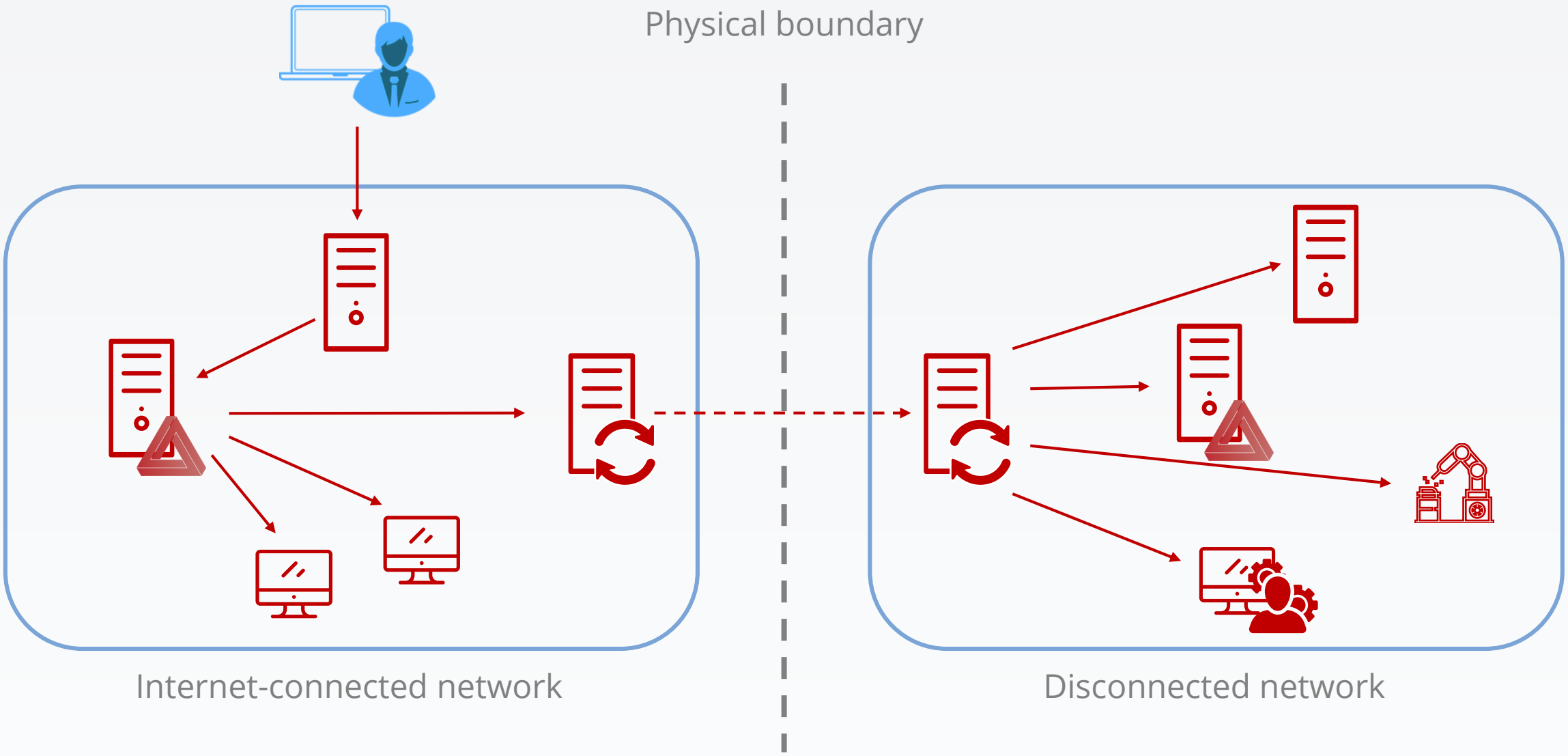
Compromise a disconnected network



Compromise a disconnected network

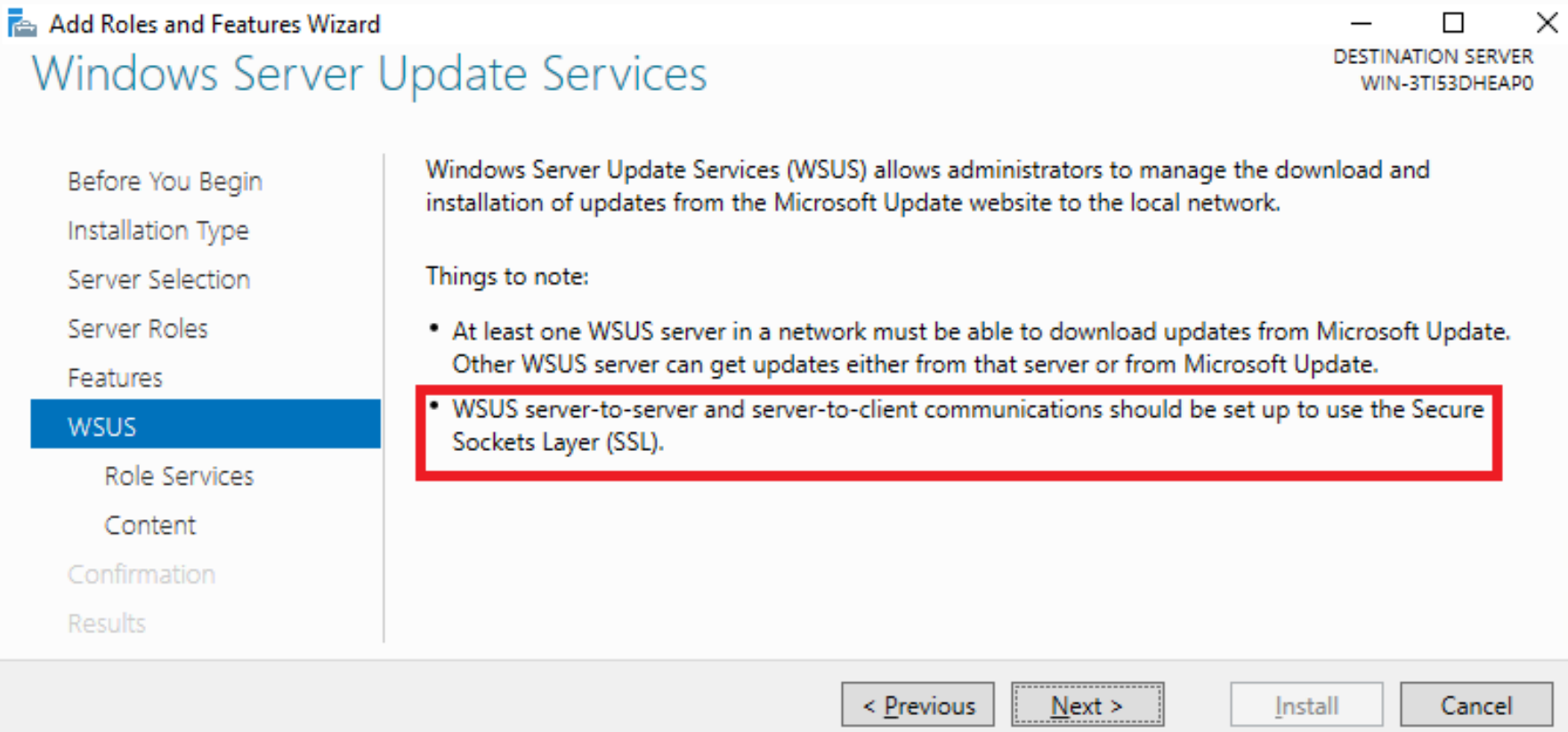


Compromise a disconnected network



That’s scary and all good, but how do I protect myself?

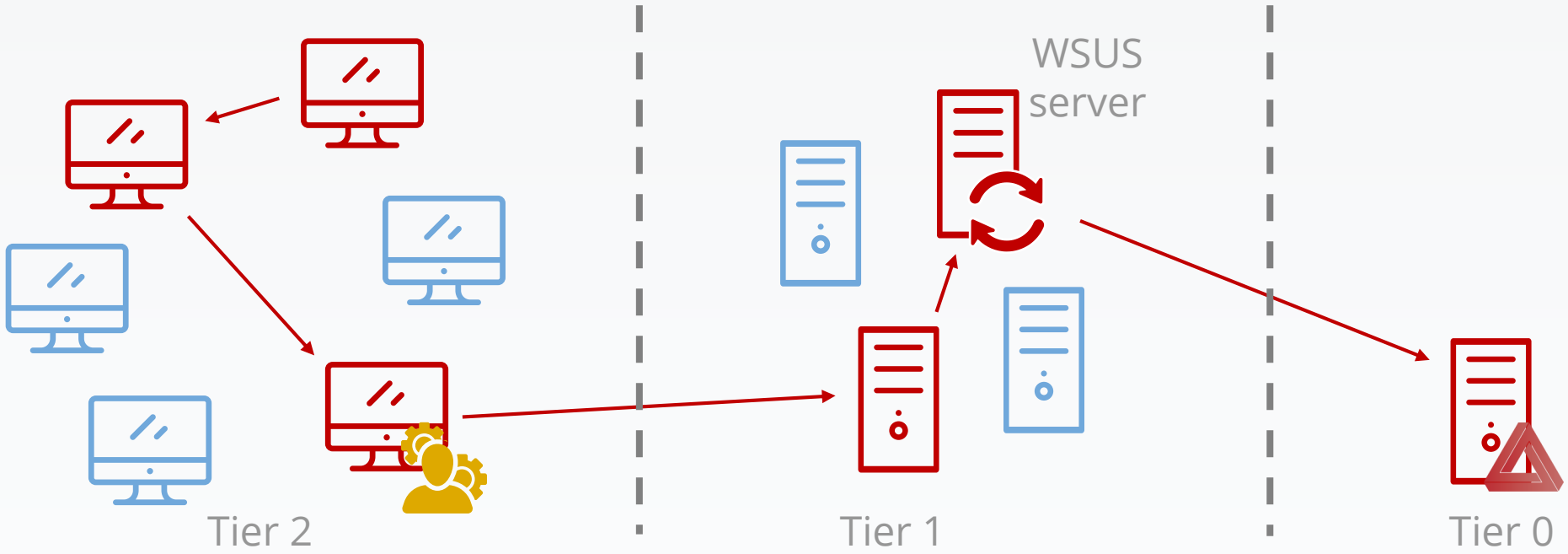
WSUS recommendations
- Activate TLS



How to protect your architecture

WSUS recommendations

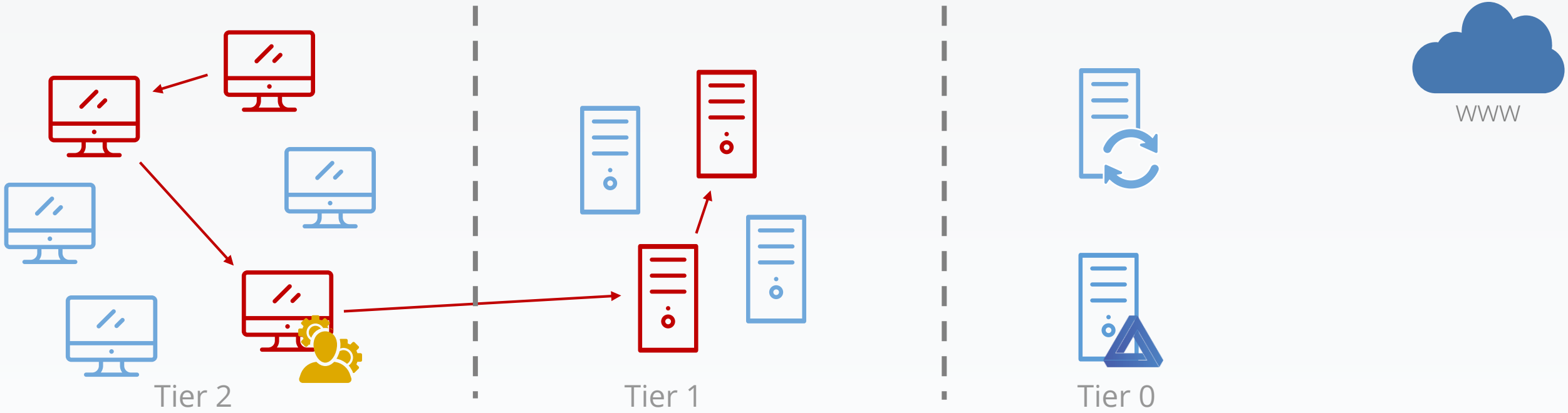
- Activate TLS
- Include WSUS server in tier-0



How to protect your architecture

WSUS recommendations

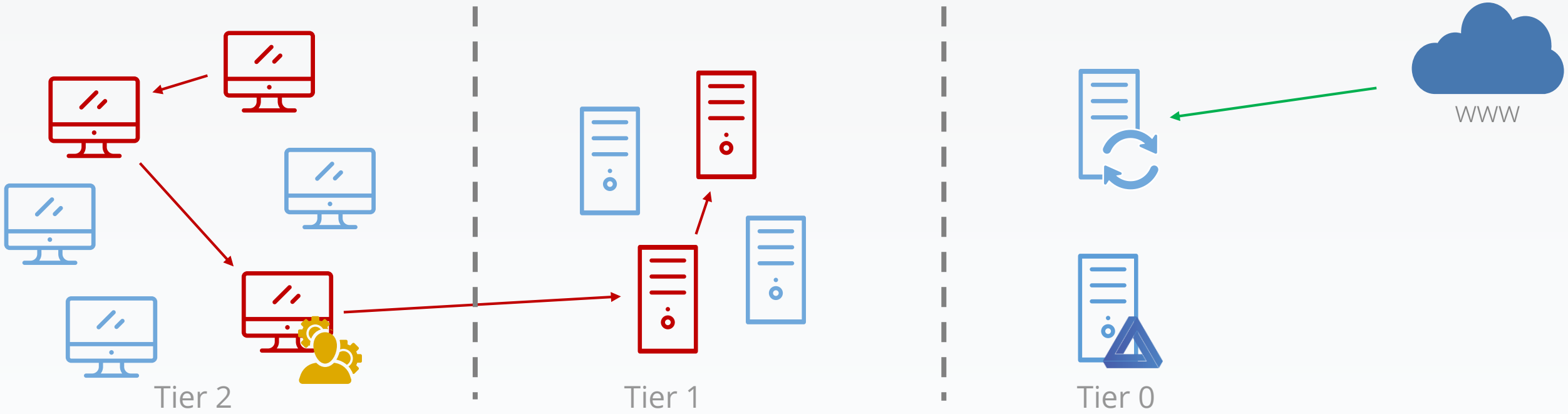
- Activate TLS
- Include WSUS server in tier-0



How to protect your architecture

WSUS recommendations

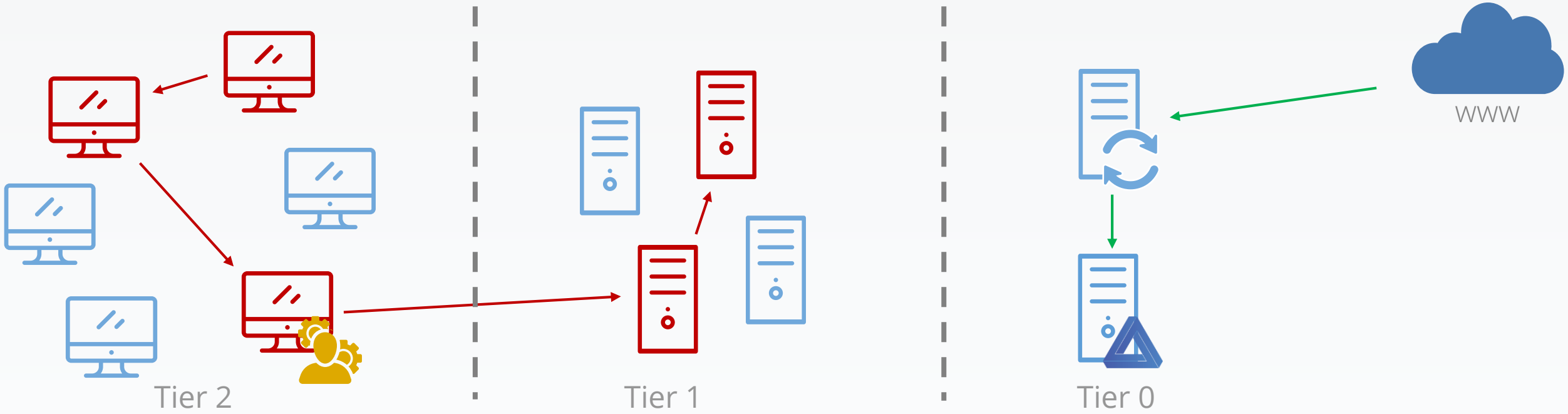
- Activate TLS
- Include WSUS server in tier-0



How to protect your architecture

WSUS recommendations

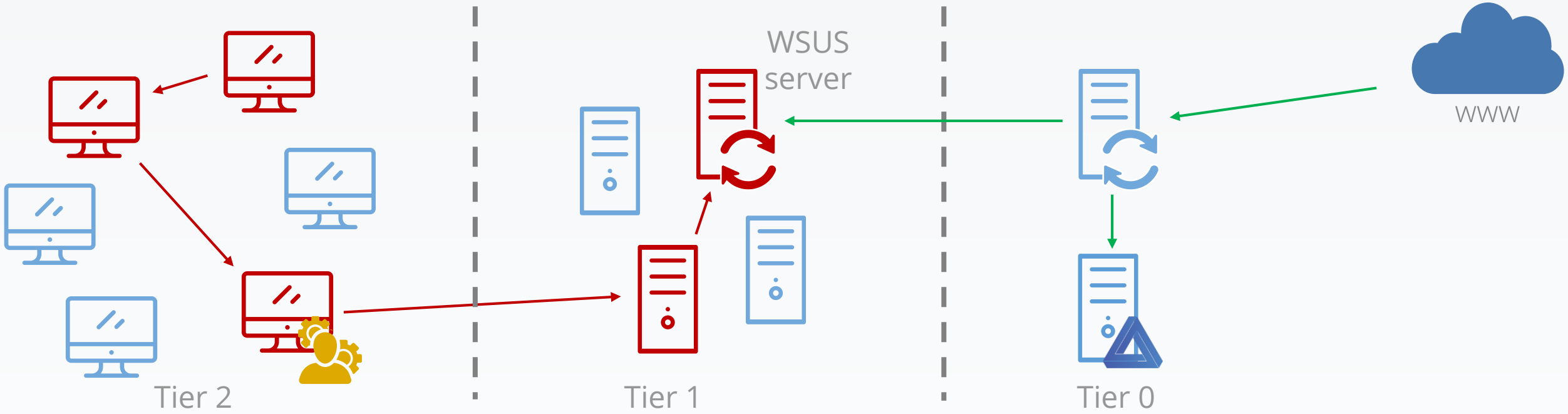
- Activate TLS
- Include WSUS server in tier-0



How to protect your architecture

WSUS recommendations

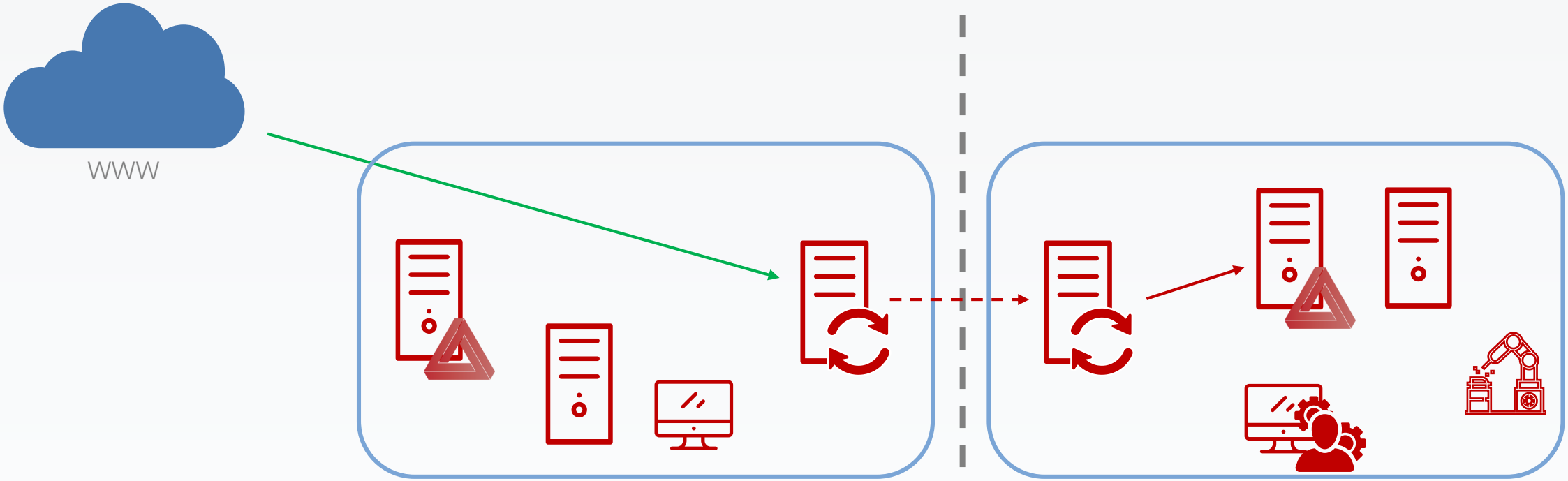
- Activate TLS
- Include WSUS server in tier-0



How to protect your architecture

WSUS recommendations

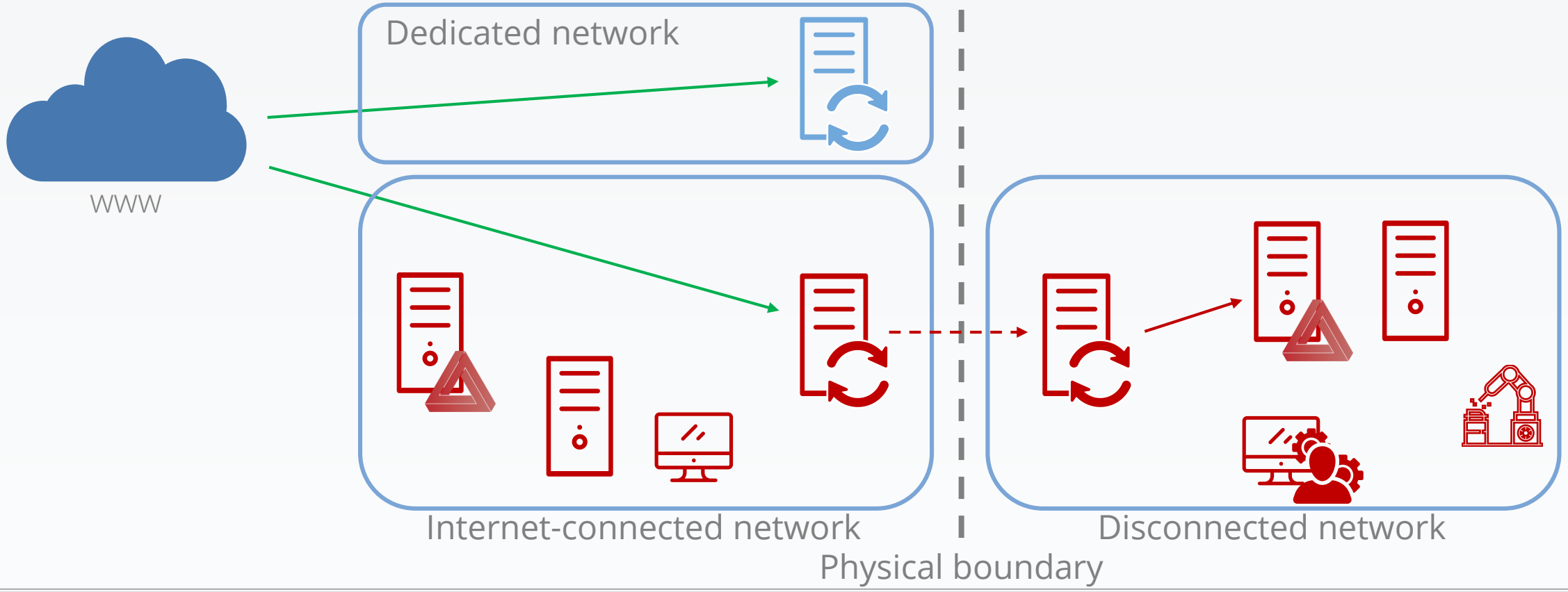
- Activate TLS
- Include WSUS server in tier-0
- Independant network → Independant WSUS server



How to protect your architecture

WSUS recommendations

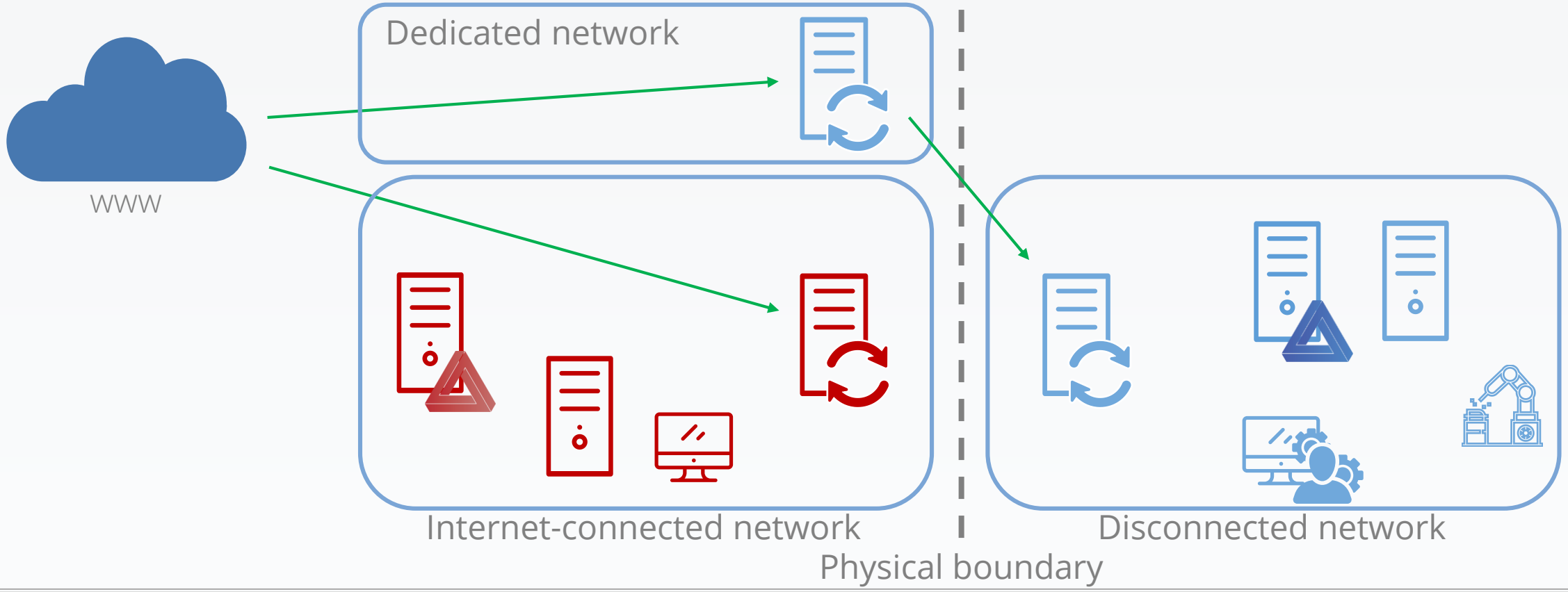
- Activate TLS
- Include WSUS server in tier-0
- Independant network ➡ Independant WSUS server



How to protect your architecture

WSUS recommendations

- Activate TLS
- Include WSUS server in tier-0
- Independant network ➡ Independant WSUS server



How to protect your architecture

Seen on a Windows 10 1703 (Creators update):

"[metadataintegrity]GetFragmentSigningConfig failed with 0x8024402C.
Using default enforcement mode: Audit."

Conclusion

Stop updating

Conclusion

~~Stop updating~~ ☺

Control relationship WSUS server → clients

ALSID
Romain Coltel

ANSSI
Yves Le Provost

Thank you all.