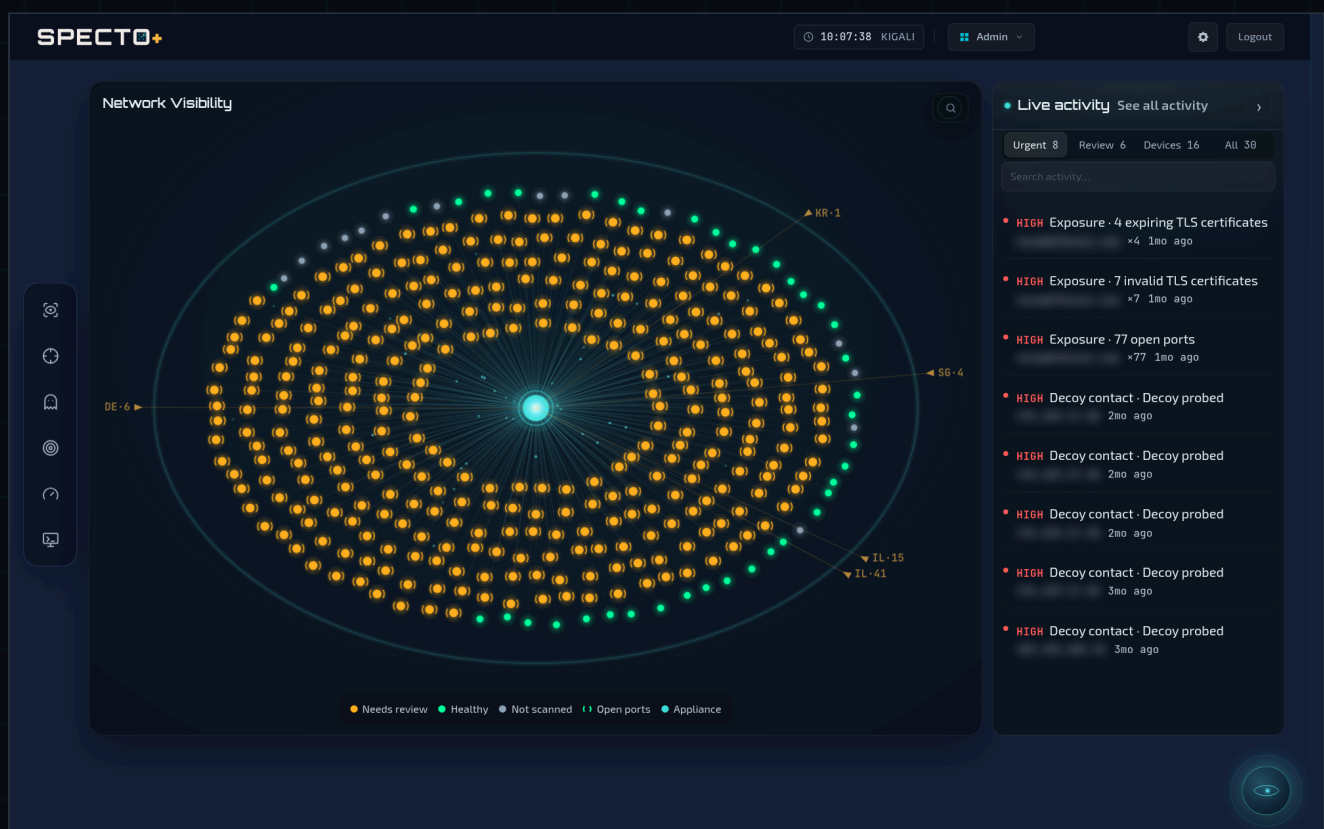


SPECTO+

See what is on your network,
what a stranger can reach, and
what was actually checked.

Specto+ is a self-hosted network defense appliance. It inventories every device it can reach, matches what each one runs against published vulnerabilities, places decoys that nobody has a reason to touch, and tells the person accountable for the network where the picture is complete and where it is not.



Specto+ 1.7.6, Network Visibility. Every device the appliance has found, by state: needs review, healthy, not scanned, open ports.

PRODUCT OVERVIEW

Network visibility that states what it knows, and what it does not

Most organizations are accountable for a network they cannot fully see. Devices arrive without a ticket, services stay open after a project ends, and a scanner report that says “no findings” is read as “secure” even when the scanner never reached half of the machines.

Specto+ is built around a single rule: **a result is only reported as proven when it is proven**. The appliance records, for every device, whether it was reached, whether it was scanned in full, and what that scan returned. A machine that answered with nothing listening is reported as a result. A machine that could not be reached is reported as unreached, and is never presented as clean. A vulnerability is marked *Confirmed* only when the exact version a service announces falls inside the published affected range; anything less certain is marked *Needs review* and goes to a person.

The product runs as one virtual machine on hardware the customer owns, attached by a bridged adapter to the network it watches. Nothing is installed on the devices it assesses. Findings, device records and captured traffic are stored on the appliance. Every external connection is started by the appliance and is listed in Section 11 of this document. ThinkCyber cannot reach the appliance unless the customer’s administrator turns on support access, for a time limit the administrator chooses, and can end at any time.

Six capabilities on one appliance

Capability	What it answers	Edition
Internal Visibility	What is on the network, what each device runs, which known vulnerabilities apply, and which devices were actually checked.	Free
Attack Surface	What a stranger on the internet can find out about the organization’s domains and public addresses.	Professional
Phantom Bait	Whether anything inside the network is touching machines that no legitimate user has a reason to touch.	Professional
SOC Drills	Whether the security team can work a real captured intrusion, role by role, under time pressure.	Professional
Executive Readiness	Whether the management team can make decisions in a crisis built from this network’s own findings.	Professional
Endpoint Control	How to act on a Windows or Linux machine from the same screen: read what is really there, then stop, remove or isolate, with a person approving every change.	Professional

Table 1. Specto+ capabilities. Cy, the AI advisor, works across all six in every edition (Section 7).

AT A GLANCE

This document

Describes Specto+ release 1.7.6.

Form factor

Virtual appliance (OVA) on customer-owned hardware. Not SaaS.

Agents

None. Nothing is installed on assessed devices.

Network attachment

One bridged adapter.

Device limit

None, in any edition.

Vulnerability sources

NIST National Vulnerability Database; CISA Known Exploited Vulnerabilities catalog.

Intrusion engine

Built in, on traffic that reaches the appliance.

AI advisor

Customer’s own cloud key, or a model the customer runs. No AI key ships in the product.

Industrial networks

Passive zones and per-device OT marking; never actively scanned.

Licensing

Free edition without time limit.
Professional: yearly licence per appliance, never per device.

CONTENTS

1 The evidence model	3
2 Architecture and deployment	4
3 Internal Visibility	6
4 Attack Surface	8
5 Phantom Bait	10
6 SOC Drills and Executive Readiness	11
7 Cy, the AI advisor	12
8 Endpoint Control	12
9 Sites, industrial networks, operations	14
10 Security of the appliance	15
11 Data handling	16
12 Standards alignment	17
13 Design boundaries	17
14 Editions, ordering, specifications	18

1 The evidence model

Every device and every finding in Specto+ ends in exactly one of a small, fixed set of states. The states are part of the product, not a reporting option: they appear on the device record, in the vulnerability views, in PDF and CSV exports, and in the answers Cy gives.

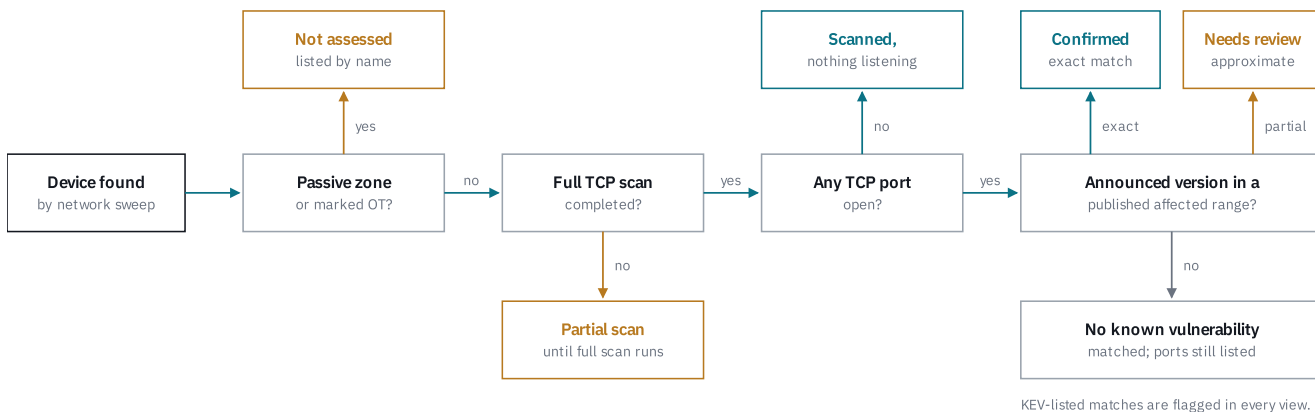


Figure 1. How a device reaches its state. Devices the customer has excluded, and devices not yet fully scanned, are named as such; they are never counted as clean.

The distinction matters most where it is least visible. A report that lists ten findings and says nothing about the forty machines it saw but could not scan invites the reader to assume those forty are fine. Specto+ lists them, by name, as not assessed or partially scanned.

An empty open-ports list can mean two opposite things: the device was scanned and is quiet, or the scan never completed. Specto+ records which is true and prints it on the device record, so an empty section is never left for the reader to interpret.

A version match is evidence that a known weakness is present. It is not proof that the machine can be exploited: a vendor may have back-ported a fix without changing the version string, or a configuration may close the path. *Confirmed* findings are therefore presented as the place to start, and a person decides before action is taken.

Vulnerabilities on the CISA Known Exploited Vulnerabilities catalog are flagged wherever they appear, so that weaknesses attackers already use are reviewed first.

State	Meaning	How Specto+ presents it
Confirmed	The exact version a service announced falls inside the affected range of a published vulnerability.	Listed under <i>Fix first</i> ; known-exploited entries flagged.
Needs review	A match that depends on an approximate or partial version.	Shown separately; never counted as Confirmed.
Scanned, nothing listening	The last full scan reached the device and found no open TCP port.	Reported as a result, not as a gap.
Partial scan	The quick scan is complete; the full port scan has not yet run.	Marked partial until the full scan completes.
Not assessed	The device is in a passive zone or is marked OT.	Listed by name; never shown as clean or safe.

Table 2. Finding states. “No findings” is never presented as “secure”.

2 Architecture and deployment

One virtual machine per network, on hardware the customer owns. No agents, no cloud tenancy, and no port opened from the internet.

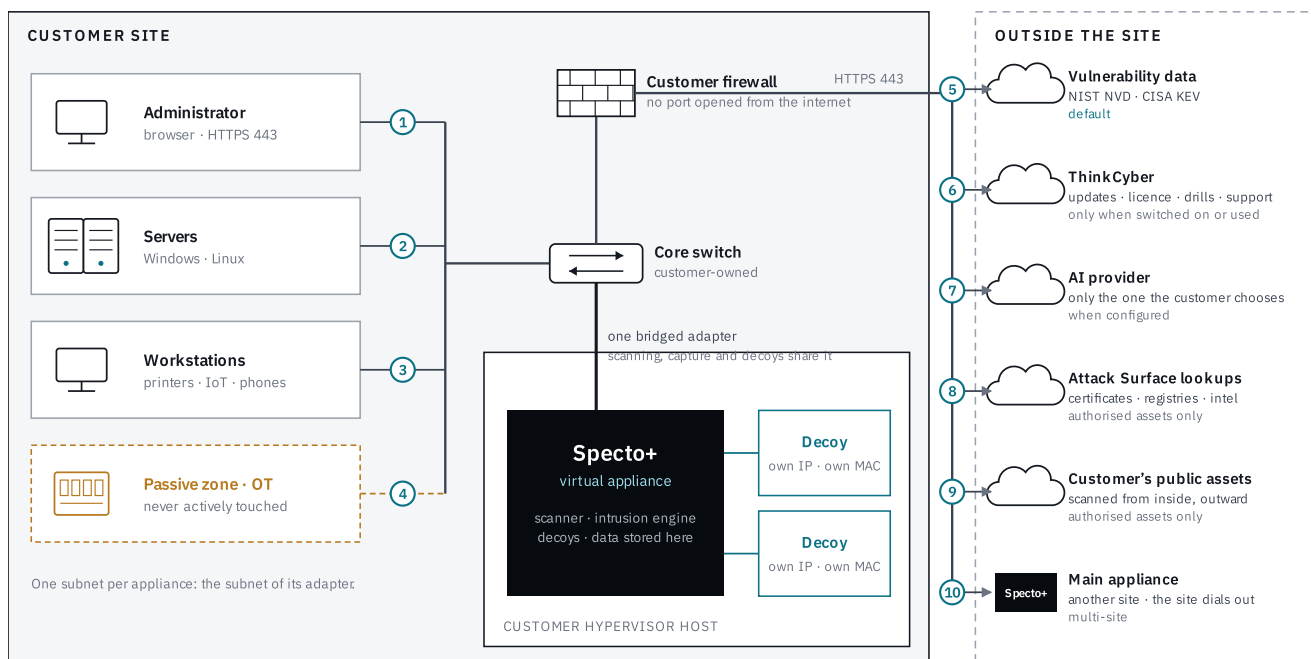


Figure 2. Reference deployment. One appliance per subnet, attached by a single bridged adapter that carries scanning, traffic capture and decoys. Every connection that leaves the site is started by the appliance. Numbers refer to Table 3.

#	From → to	Protocol · port	Purpose	When
1	Administrator → appliance	HTTPS 443 (TLS 1.2/1.3); port 80 redirects	Web interface; certificate generated by each appliance. No SSH or console login.	Inside the network
2	Appliance → servers	WinRM 5985 · SSH 22	Endpoint Control, with an account the customer provides.	When configured
3	Appliance → devices on its subnet	ARP · TCP, private addresses	Discovery, then port, service and operating-system scans.	Default
4	Passive zones and OT devices	None sent	Never actively touched; seen only in passing traffic.	As declared
5	Appliance → NIST · CISA	HTTPS 443	Vulnerability data from the NVD and the KEV catalog.	Default
6	Appliance → ThinkCyber	HTTPS 443	Update checks, licence activation, SOC Drill content, support tunnel.	Only when switched on or used
7	Appliance → AI provider	HTTPS 443	Cy and Executive Readiness, to the one provider the customer configures.	When configured
8	Appliance → lookup services	HTTPS 443	Attack Surface: certificates, registries, breach and reputation data.	Authorised assets only
9	Appliance → customer's public assets	TCP · HTTPS · DNS	Attack Surface scans, through the customer's own connection.	Authorised assets only
10	Site appliance → main appliance	HTTPS 443	Multi-site reporting. The site dials out; nothing connects into a site.	Multi-site

Table 3. Network flows in the reference deployment. Section 11 lists what each outbound connection sends.

2 ARCHITECTURE AND DEPLOYMENT, CONTINUED

Deployment

- 1 **Import the image.** A single OVA image, imported into the customer's hypervisor and bridged to the subnet it should watch.
- 2 **Run the first-run wizard.** Choose the edition and the network type (IT or OT), create the administrator account, and save the recovery key.
- 3 **Activate, if licensed.** The Free edition needs no code, sign-up or email. An evaluation or Professional code is activated with one online call; the appliance then verifies its signed licence locally.
- 4 **Discovery begins.** Devices appear at once; in-depth scanning completes over the following days.

Placement

The appliance has one network adapter. Discovery, scanning, the intrusion engine and the decoys all use it; there is no separate capture adapter.

Discovery covers the subnet of the adapter. Organizations with several networks place one appliance per network; additional appliances report to a main appliance (Section 9).

Before installation

Item	Requirement
Network adapter	One bridged adapter on the subnet to be watched.
Hypervisor settings	For decoys: allow MAC address changes, forged transmits and promiscuous mode on the appliance's adapter.
Addressing and DNS	DHCP, or a fixed address with its DNS servers. A fixed-address change rolls back after five minutes unless confirmed.
Time	The operating system's standard time synchronisation; not configured in the interface.
Proxy	Optional HTTP proxy with a bypass list, stored encrypted. Private address ranges never use it.
Firewall	Outbound HTTPS 443 to the destinations in Table 5 that the customer uses. No inbound rule from the internet.

Table 4. Prerequisites.

Destinations to allow

Use	Destination (HTTPS 443)	When
Vulnerability data	NIST and CISA	Default
Updates	ThinkCyber update service	Only when update checks are switched on; air-gapped sites update from a signed file
Licence, SOC Drills	ThinkCyber	On activation; when a drill is requested
Support access	ThinkCyber support relay	Only while support access is on
Cy, Executive Readiness	api.anthropic.com · generativelanguage.googleapis.com · api.openai.com	Only the provider configured, or none for a model on the customer's network
Attack Surface	crt.sh, rdap.org, Have I Been Pwned, DeHashed, Shodan, VirusTotal, AbuseIPDB, GitHub, public cloud storage	Only for declared, authorised assets
Alerts	The customer's own webhook address	Only if set
Location enrichment	ipinfo.io	Off unless an administrator turns it on

Table 5. Outbound destinations. ThinkCyber provides the exact host names on request. Blocking any of them stops only that function; with vulnerability data blocked, findings remain but the data ages.

3 Internal Visibility FREE EDITION

The inside of the network: every device the appliance can reach, what it runs, which published vulnerabilities apply to it, and whether it was checked in full.

ACTIVE ASSESSMENT



PASSIVE MONITORING



Figure 3. Internal Visibility. Active assessment runs continuously in six stages; passive monitoring inspects the traffic that reaches the appliance.

LEAVES THE APPLIANCE Nothing.

Discovery

The appliance sweeps the subnet it is attached to and records every device that answers. The headline count is the number of devices seen in the last 24 hours; devices that have gone quiet remain in the inventory and are found by search or by the “not seen recently” filter, so a machine that is only switched on at month-end is not lost.

Port scanning

Every device receives a frequent quick scan of commonly used ports and, in time, a full scan of every TCP port, one machine at a time to keep load on the network low; the full scan can be switched off. Until its full scan has run, a device is labelled *partial scan*. Devices marked OT, and subnets declared passive zones, are not actively scanned. UDP is not scanned.

Vulnerability matching

Operating systems and service versions are fingerprinted from what each device announces, then matched against the NIST National Vulnerability Database and the CISA Known Exploited Vulnerabilities catalog, both refreshed regularly. Two views organize the result: *Fix first*, which ranks Confirmed and known-exploited findings across the estate, and *By device*.

Network alerts

A built-in intrusion engine inspects the traffic that reaches the appliance. New-device alerts are grouped so that a first scan of a large network does not flood the alert list. The appliance can block an address on its own firewall by hand, or automatically for selected rules in prevention mode, which is off by default and never blocks private addresses. It does not push rules to network firewalls. Each outside address has a forensics view, with the related packet capture available for download.

Reporting and history

Every device record can be exported as PDF or CSV. Scan history shows what changed between scans: new services, closed ports, new findings, and devices that returned after an absence. Partial scans and devices not assessed are labelled as such, so the reader can see the coverage behind each number.

Network map

The Network Visibility view draws the devices the appliance has found, coloured by state: needs review, healthy, open ports, the appliance itself, and decoys. It is the starting point for an operator and the view most often shown to management.

3 INTERNAL VISIBILITY, CONTINUED

ON THE APPLIANCE

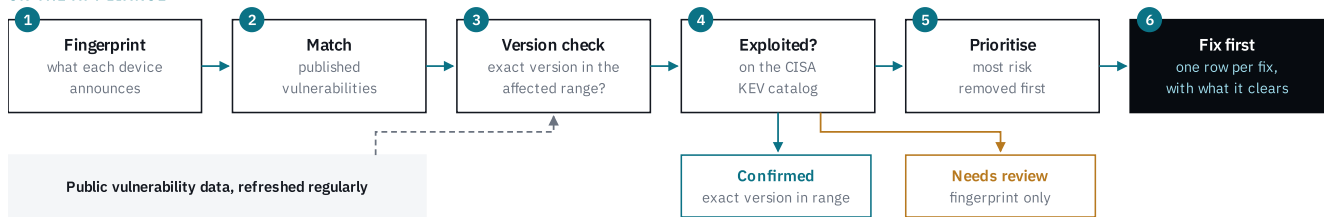


Figure 4. Vulnerability matching. A finding is Confirmed only when the exact announced version falls inside a published affected range; a match on a fingerprint alone stays Needs review.

LEAVES THE APPLIANCE Nothing about the devices. Vulnerability data is only downloaded.

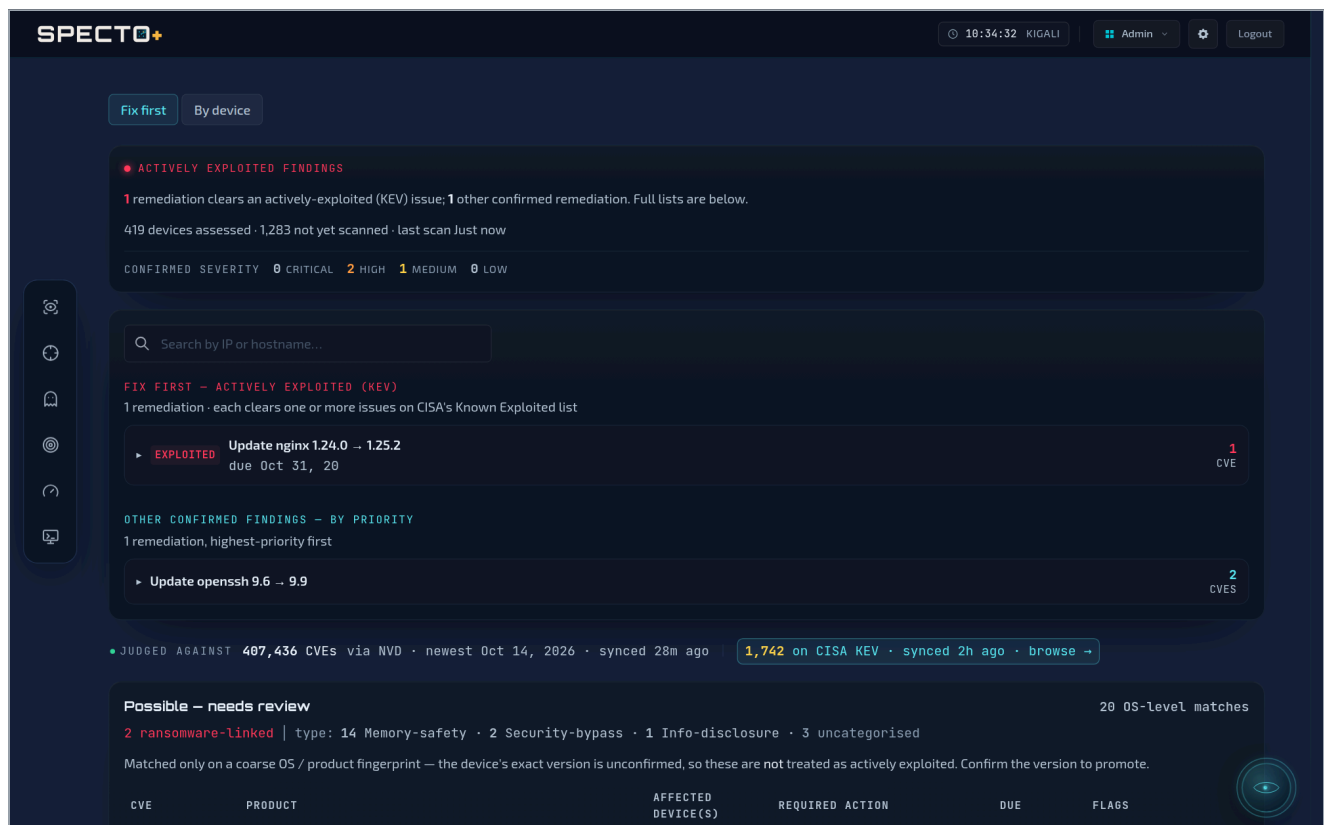


Figure 5. Specto+ 1.7.6, Fix first. Remediations are ranked so that the one clearing an actively exploited (KEV) issue comes first; matches made only from a coarse fingerprint are held apart as Possible, needs review.

Fix first

Fix first answers the question an operator has on a Monday morning: which single change removes the most risk. Findings are grouped by remediation rather than by vulnerability, so one upgrade that clears several issues appears once. Actively exploited issues from the CISA catalog lead the list, followed by other Confirmed findings by priority.

Matches that rest only on an operating-system or product fingerprint are listed separately as *needs review*, with the reason, and are never promoted to actively exploited until the exact version is confirmed. The page states how many devices were assessed and how many are not yet scanned, and when the vulnerability data was last synchronised.

The device record

Each device has one record that carries everything the appliance knows about it: addresses, identity, the operator's notes, open ports and services, matched vulnerabilities with their state, and the alerts that involve it. Actions sit on the record itself: inspect, run a full scan, use the device as the template for a decoy, add a note, or mark it as OT so that it is never actively probed again.

COVERAGE, NOT JUST FINDINGS

Every Specto+ report answers two questions: what was found, and how much of the network was actually examined to find it.

4 Attack Surface PROFESSIONAL

The outside of the organization, as a stranger sees it: assessed from the appliance through the customer's own internet connection, using only what the organization publishes or what its public services answer to anyone who asks.

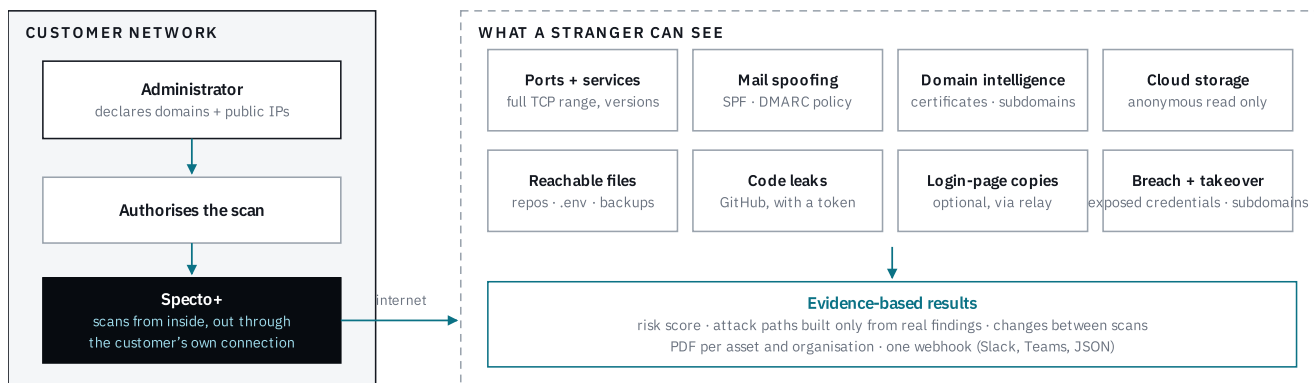


Figure 6. Attack Surface. The customer declares its assets and authorises the scan; every result is tied to evidence.

LEAVES THE APPLIANCE The declared domains and their hosts, to the lookup services and as scan targets.

The customer lists its domains and public addresses and confirms, in a logged declaration, that it owns them or is authorised to scan them; scanning checks for that declaration. Specto+ then examines each asset:

- **Ports and services** on each public address across the full TCP range, with versions matched to published vulnerabilities under the same evidence model as the inside of the network.
- **Email authentication.** SPF and DMARC records are read and evaluated: whether they stop others sending mail in the organization's name, and whether receiving servers are asked to reject such mail or only to report it.
- **Domain intelligence** from public certificate, subdomain and domain-ownership sources.
- **Public cloud storage** on Amazon, Google and Azure named after the organization, reported as exposed only when it answers an anonymous read.

- **Code repositories.** Public GitHub code is searched for leaked-secret candidates when the customer supplies a GitHub token.
- **Reachable files** such as exposed `.git` directories, `.env` files and backups. Evidence is the server's actual reply (status, type, size and a short excerpt with secrets masked); a bare "200 OK" never counts.
- **Breach and credential exposure** for the organization's domains, and **subdomain-takeover** checks.
- **Login-page copy detection** (optional) identifies copies of the organization's login page hosted elsewhere, an early sign of phishing preparation, through a relay run by ThinkCyber.
- **Threat intelligence** from Shodan, VirusTotal, AbuseIPDB and DeHashed, through ThinkCyber's service or with the customer's own keys.
- **Attack paths** are assembled only from findings that were actually made.

Specto+ does not run exploits. Its one active sign-in check sends a bounded set of requests using fictitious accounts at a reserved domain; checks with real credentials are off by default and need their own consent. The requests sent are recorded on the appliance.

4 ATTACK SURFACE, CONTINUED

Results and reporting

Each asset carries a risk score and a record of what changed between scans. Reports are produced per asset and for the whole organization as PDF, with an executive summary first and the technical detail behind it, so the same document serves a board and the team that fixes the findings.

Alerting

Attack Surface alerts can be sent to one webhook: Slack, Microsoft Teams, or any receiver that accepts JSON. Threat-intelligence lookups and login-page detection are off until the customer switches them on, and each is listed with what it sends in Section 11.

Finding	Evidence kept on the appliance	State
Vulnerable public service	The service banner and the version it announced	Confirmed or Needs review
Exposed file or directory	The server's reply: status, type, size and an excerpt with secrets masked	Reported only when the reply proves it
Weak mail authentication	The published SPF and DMARC records as read	Policy stated: reject, quarantine or report only
Open cloud storage	The response to an anonymous read	Exposed only if the read succeeds
Leaked-secret candidate	The public code location	Candidate, for a person to verify
Attack path	The findings it is built from	Never built from assumptions

Table 6. Attack Surface findings and the evidence behind each.

IN THE BOARD MEETING ILLUSTRATIVE

Somebody asks whether the organization is exposed to the vulnerability that was in the news. The answer Specto+ supports: "Two machines match, and we have confirmed both; they will be patched by Thursday. Eleven we could not check, and here is why."

5 Phantom Bait PROFESSIONAL

Decoys inside the network: machines that nobody has a legitimate reason to touch. Any contact is worth investigating first.

BUILDING A DECOY



WHEN SOMETHING TOUCHES IT

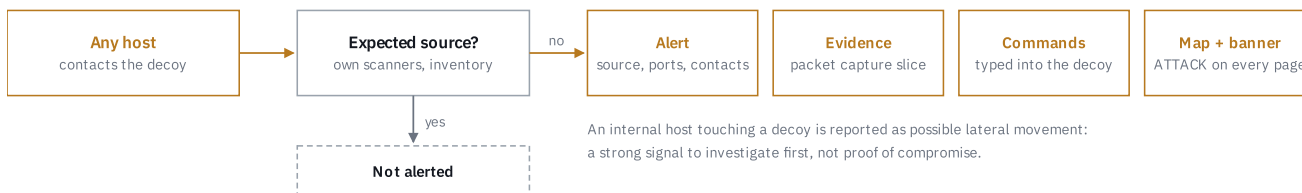


Figure 7. Phantom Bait. A decoy is cloned from a real machine; contact from anything other than an expected source raises an alert with evidence.

LEAVES THE APPLIANCE Nothing. With several sites, decoy contacts go to the customer's own main appliance.

The administrator selects a real machine. Specto+ copies its open ports and service responses and builds a decoy with its own network identity, so that it appears on the network as a separate machine rather than part of the appliance. Anything typed into a decoy is recorded.

Once the organization's own scanners and inventory tools are listed as expected sources, any other contact raises an alert naming the source, keeps a slice of the network traffic as evidence, marks the contact on the network map, and shows an attack marker on every page while the contact continues.

There is no fixed number of decoys; each uses part of the appliance's memory. Because each decoy has its own hardware address, the hypervisor must allow MAC address changes, forged transmits and promiscuous mode on the appliance's adapter. Decoys operate only on the network the appliance is attached to. They are never deployed on fully OT networks, never copied from an OT device, and never placed on the internet side.

MONDAY MORNING ILLUSTRATIVE

One entry in the decoy alert list: a laptop in accounts made contact with the decoy file server on Saturday at 02:14. The record shows which laptop, when, and exactly what it sent. Nobody in accounts works on Saturdays, and nobody outside IT knows that server exists.

What a decoy records

When something touches a decoy	What is kept as evidence
The source	The address that made contact, named against the inventory when it is known
Commands	Everything typed into the decoy
Ports	The ports touched and the time of each contact
Traffic	A slice of the real packet capture, downloadable as evidence
Alert	One per source unless the source is expected; a marker on the map and on every page while contact continues

Table 7. The evidence a decoy keeps.

6 SOC Drills and Executive Readiness PROFESSIONAL

SOC Drills

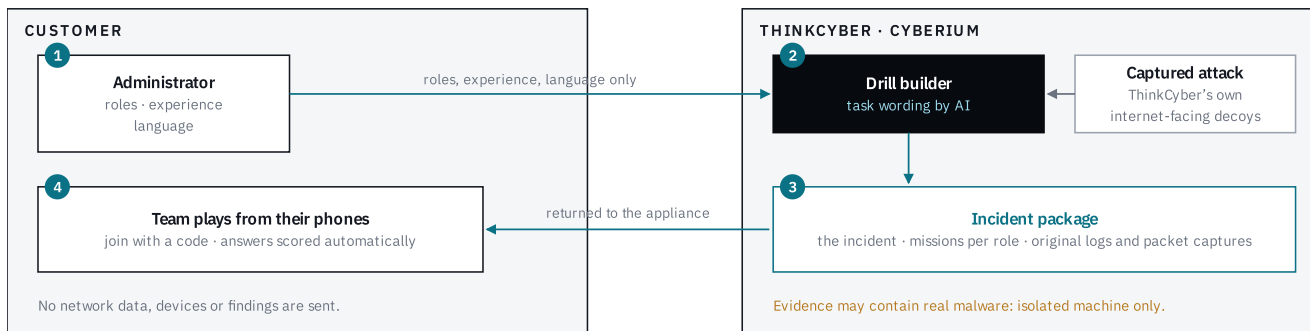


Figure 8. SOC Drills. Only roles, experience and language leave the customer; the drill comes back with its original evidence.

LEAVES THE APPLIANCE Roles, experience in months, language and an anonymous identifier. No network data.

The administrator selects roles (SOC Tier 1, 2, 3 and Incident Response), experience level and language. ThinkCyber's Cyberium platform builds the drill from an attack captured on ThinkCyber's own internet-facing decoys and returns the incident, missions for each role and the original evidence: logs and packet captures. Only the task wording is written by AI.

Players join from their phones with a code, and answers are scored automatically. Only roles, experience and language are sent to ThinkCyber; no customer network data is sent. Drills are unlimited under a Professional licence. Findings on the customer's network are not converted into drills.

Drill evidence can contain real malware samples; downloads require confirming handling on an isolated machine, and the confirmation is recorded.

Executive Readiness

A tabletop exercise for the management team, built from this network's own findings.



Figure 9. Executive Readiness. The scenario is generated by the customer's configured AI model from the appliance's own findings.

LEAVES THE APPLIANCE A summary of the security posture and the participants' answers, to the customer's chosen AI provider only.

Executive Readiness turns what the appliance has found on this network (its devices, vulnerabilities and exposure) into a crisis scenario. The CISO reveals the crisis turn by turn; each role records its decisions; the exercise closes with a scored after-action report listing strengths, gaps and recommendations, downloadable as PDF.

Because the scenario starts from real findings, the discussion is about the organization's own systems rather than a generic case. The exercise uses the customer's own AI model.

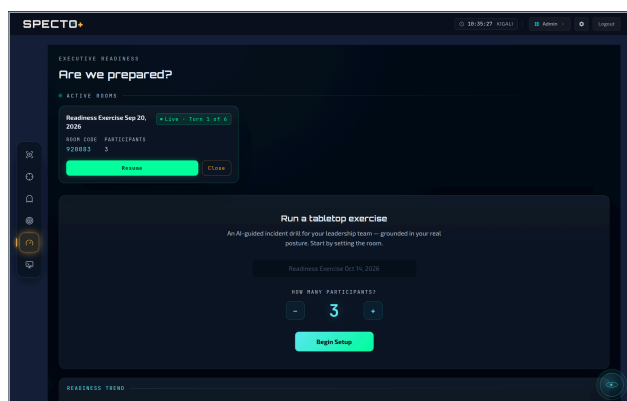


Figure 10. Specto+ 1.7.6, Executive Readiness: an exercise room in progress and the setup for a new tabletop exercise.

7 Cy, the AI advisor ALL EDITIONS

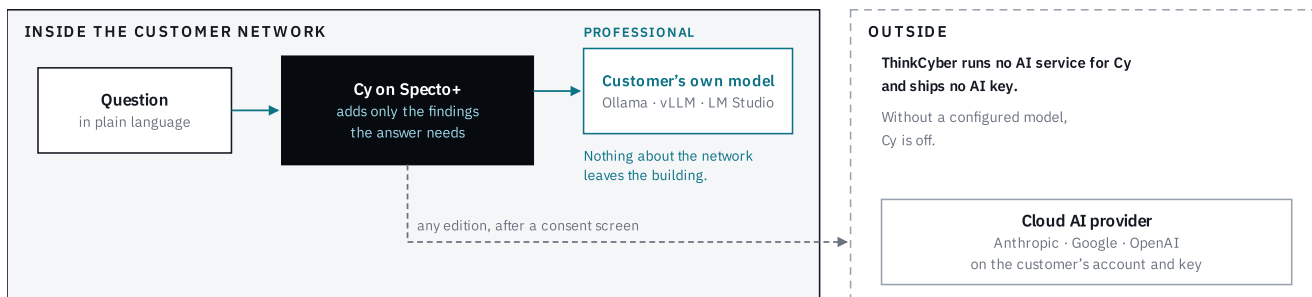


Figure 11. Cy data path. The model is chosen by the customer; ThinkCyber is not on the path.

LEAVES THE APPLIANCE With a cloud provider, the question and its context (addresses, alerts, vulnerabilities), to that provider. With a model on the customer's network, nothing.

Cy answers questions about the network in plain language, using what the appliance has found. It uses whichever model the customer points it to and has no other destination. On the Free edition Cy uses the customer's own key for a cloud provider (Anthropic, Google or OpenAI), after a consent screen that states what will be sent. A Professional licence also allows a model the customer runs on its own network through an OpenAI-compatible endpoint, such as Ollama, vLLM or LM Studio; in that configuration nothing about the network leaves the building. With a cloud provider, the question and the context needed to answer it (addresses, alerts and vulnerabilities) go to that provider.

ThinkCyber runs no AI service for Cy, charges nothing for AI use, and ships no AI key in the product. Without a configured model, Cy is off.

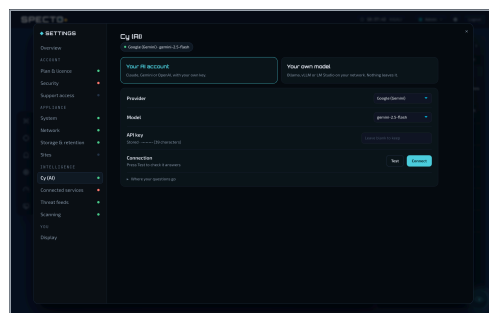


Figure 12. Specto+ 1.7.6, Cy settings: the customer's own AI account or the customer's own model, with the provider and model in use.

8 Endpoint Control PROFESSIONAL

Finding the problem is half of it. Endpoint Control is how you act on the machine itself, from the same screen, with an account you provide and nothing installed on it.

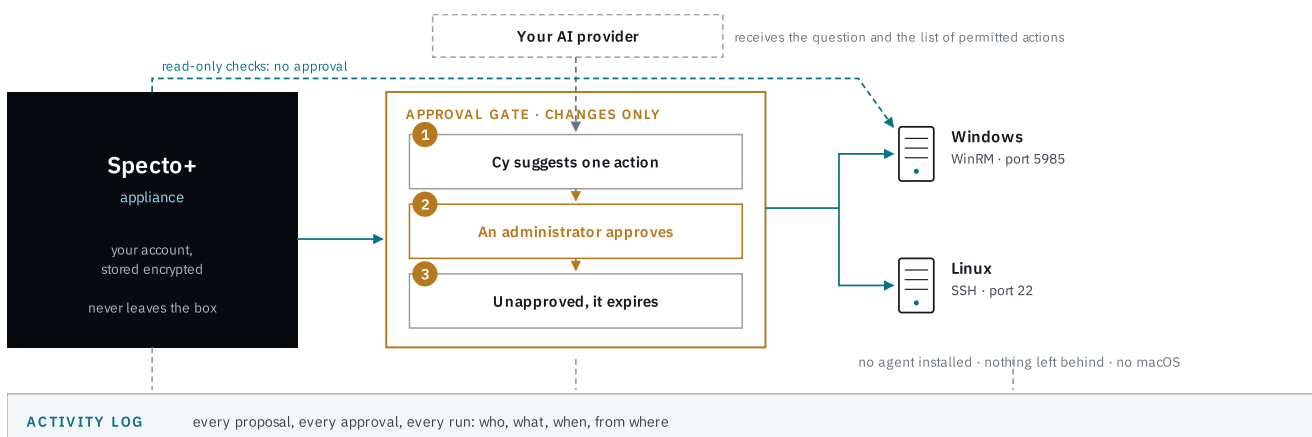


Figure 13. Endpoint Control. Read-only checks run without approval. Every change passes the approval gate, one action at a time, and everything is written to the Activity Log.

LEAVES THE APPLIANCE When Cy proposes an action, the question and the list of actions it may choose from go to the AI provider you chose. With a model on your own network, nothing leaves. Your sign-in account and everything the appliance reads never leave.

8 ENDPOINT CONTROL, CONTINUED

What it reads	What it can do: one action at a time, approved by a person
Hardware and operating system	Check, restart or stop a service
Installed programs and services	Find a file by name or hash; check that a file is present
Security state: disk encryption, firewall, antivirus, restart pending	Show who is logged on
Local administrators; shares and who can open them	Remove software
Startup items and scheduled tasks	Remove a browser add-on; install an approved one (Chrome and Edge, from the vendor store only)
Browser add-ons, USB history, who is logged on	Isolate a machine, and release it

Table 8. Endpoint Control. What the account cannot read is shown as “could not read”, never as clean. There is no free-form command.

Isolating a machine

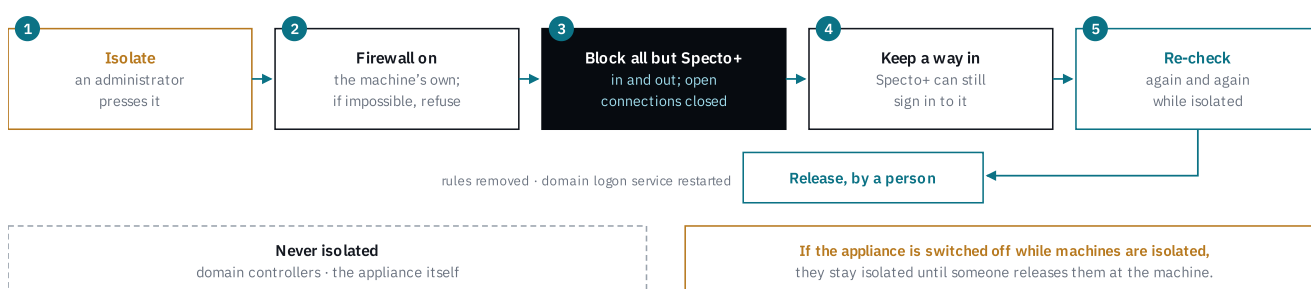


Figure 14. Isolation. It never ends by itself, and only the appliance can still reach an isolated machine.

On Windows, the machine’s own firewall is switched on first; if it cannot be, Specto+ refuses and says the machine cannot be cut off. Everything in and out is then blocked except the appliance, and connections that are already open are closed. On Linux the same is done with the machine’s own firewall. Only Specto+ can still reach the machine; an administrator cannot, from their own PC.

On a domain machine, Specto+ first makes sure it can still sign in without the domain controller.

Isolation never ends by itself. A person presses Release, and until then the appliance keeps re-checking the machine. Release removes the rules and restarts the domain logon service. Domain controllers are on a never-isolate list, and the appliance can never isolate itself.

PLAN FOR THIS

If the appliance is switched off while machines are isolated, they stay isolated until someone releases them at the machine.

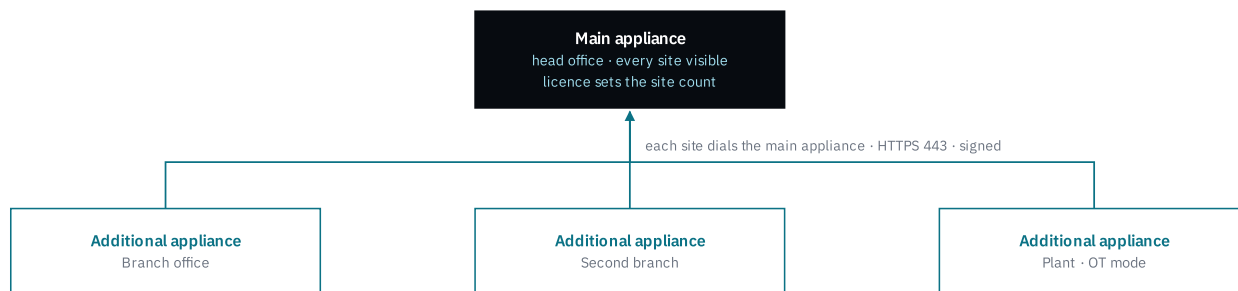
The account it uses

Account the customer provides	What it gives
A normal user	The inventory
Local Administrators (Windows) or sudo (Linux)	Full detail
Administrator or root	Isolation

Table 9. Account levels. Specto+ never needs a Domain Admin account. Use a dedicated account; it is stored encrypted on the appliance and never leaves it.

9 Sites, industrial networks and operations

Multiple sites PROFESSIONAL



Without the main appliance a site keeps full features for seven days, then continues monitoring as the Free edition until contact returns.

Figure 15. Multiple sites. One appliance per network; additional appliances report to one main appliance.

Additional appliances connect to one main appliance, from which every site is visible. Each site dials the main appliance over HTTPS 443; nothing connects into a site. The link is certificate-pinned and every report is signed. Sites send alerts, the device inventory, fingerprints and decoy contacts; packet captures and logs stay on the site. The licence sets how many may connect, and all renew together. A site that loses contact with the main appliance keeps full features for seven days and keeps monitoring after that. A site removed on the main appliance becomes read-only with its data kept. If the main appliance fails, it receives a new code and each site re-pairs with a pairing code, keeping its data.

Industrial and sensitive networks

Subnets can be declared passive zones and single devices marked OT. Neither is actively probed; both are listed as not assessed rather than counted as safe. A full OT mode builds no decoys. Factory floors, medical equipment and controllers that must not be touched are excluded by the customer, not inferred by the product.

Server health

The appliance monitors its own disk, memory, scans and sensors. A sensor that is running but receiving nothing is reported as a problem, not as healthy.

Data retention

Traffic recordings are kept in a size-bounded ring: 5 GB on the Free edition, and up to half the disk, set by the customer, on Professional. Recordings tied to alerts or decoy contacts are retained as evidence. Other records are kept until an administrator enables clean-up.

Updates

The appliance refuses any update it cannot verify. Update checks are off until the customer enables them, and air-gapped sites install updates from a file. Software and vulnerability-data updates are included in every edition.

Who does what

Customer	ThinkCyber partner	ThinkCyber
Provides the hypervisor and a bridged adapter	Installation and first-run setup	Software releases and vulnerability-data updates
Declares passive zones, OT devices and expected sources	Switch, VLAN and hypervisor configuration	Licences and 30-day evaluations
Declares and authorises Attack Surface assets	Connection of additional sites	SOC Drill content, from ThinkCyber's captures
Approves every Endpoint Control change	Endpoint Control onboarding	Support, through support access the customer switches on
Chooses the AI model for Cy	Monitoring and on-site support	Team training through the Cyberium platform
Remediates findings	Custom exercises and services	

Table 10. Operating responsibilities.

10 Security of the appliance

A tool that holds an inventory of the network, its weaknesses and credentials for its machines is itself a target. These are the controls on the appliance.

Area	Control
Access roles	Two roles: administrator and client.
Audit trail	Every login and every action is recorded with user, time and source address.
Recovery	A recovery key created during setup restores owner access and ends all open sessions.
Support access	Off by default. An administrator switches it on, re-enters the password and chooses 4 hours, 24 hours or 3 days; it ends by itself. The appliance opens the tunnel outward to ThinkCyber's relay on port 443; no inbound port is opened. An engineer connects back only with a short-lived signed certificate (no password works) and receives a root shell on the appliance: full rights on the box, fully recorded. Everything typed and shown is saved to a file on the appliance readable only by the system, and each session is entered in the activity log. A banner shows on every page while access is on, and "End now" cuts it at once.
Software integrity	Signed updates; the appliance refuses an update it cannot verify.
Licence	Signed licence, verified on the appliance. Revoking a licence never switches the appliance off.
Change control	Endpoint Control changes require a person's approval and are written to the audit log.
Scope control	Passive zones and OT marking exclude devices from active probing. Attack Surface scans require an administrator's authorisation.
Web interface	HTTPS by default, with a certificate generated by each appliance at first boot; plain HTTP redirects to HTTPS.
Multi-factor authentication	An authenticator code is required for every administrator. Any other user who sets one up is always asked for it. The one exception is a site's emergency account, kept as the last way in.
Stored secrets	Endpoint Control accounts, AI keys and Attack Surface keys and logins are encrypted at rest (AES-256) with a key unique to each appliance, which is never included in backups.
Backup	Automatic daily backup on the appliance's own disk, kept 14 days; an appliance that was off at backup time catches up at next boot. A backup downloaded from Server Health, encrypted with a passphrase the customer chooses, is the off-appliance copy for disaster recovery.
Restore	Restores devices, findings, history, alerts, drill and exercise results, and user accounts. Secrets never leave the appliance they were entered on: after restoring onto new hardware, re-enter Endpoint Control sign-ins, AI keys, scan logins and API keys, re-apply the licence code, and re-pair an additional site with its main appliance. The new appliance keeps its own identity and keys.
Support policy	Update cadence, support channels and end-of-life policy: ThinkCyber will confirm.

Table 11. Appliance security controls.

Endpoint Control accounts

Endpoint Control acts with the rights of the account the customer provides; use a dedicated one. On Windows, membership of the local Administrators group gives full detail and isolation. On Linux, a normal user is enough for inventory, read-only sudo gives full detail, and root is needed only for isolation. Specto+ never needs a Domain Admin account.

Authorised use

Attack Surface examines only domains and addresses the customer declares. Each declaration records the customer's confirmation that it owns the asset or is authorised to scan it, and scanning checks for that confirmation before it runs.

11 Data handling: what leaves the network

Device records, findings and captured traffic are stored on the appliance. The appliance starts every external connection itself, and each one is listed below with what it carries. ThinkCyber cannot reach the appliance unless the customer's administrator turns on support access, for a time limit the administrator chooses.

Organizations with a policy against cloud processing can run the Professional edition with Cy pointed at a model inside their own network, leave threat-intelligence lookups and login-page detection off, and keep update checks off, installing updates from a file. In that configuration and with SOC Drills not requested, the remaining outbound connections are the vulnerability feeds, which carry no customer data, and the one-time licence activation.

The location of outside addresses is looked up in a local, offline database; nothing is sent for it unless an administrator turns on enrichment. Attack Surface reaches out by nature: it scans the organization's own public addresses and queries public sources about its domains. It is switched on per asset by an administrator.

Connection	When	What is sent	Destination
Vulnerability data	Default	Requests for feed updates. The device list is not sent.	NIST NVD and CISA KEV
Software updates	When enabled	An update check.	ThinkCyber
Licence activation	When a code is entered	The activation code. One contact; there is no scheduled check-in.	ThinkCyber
Cy, cloud model	When a key is added	The question and the findings needed to answer it, after a consent screen.	The AI provider the customer chose, on the customer's account
Cy, own model	Professional	The question and the findings needed to answer it.	The customer's own endpoint
Attack Surface	When enabled	Scans of the customer's public addresses; public certificate, subdomain, ownership and cloud-storage lookups.	The customer's assets; public sources
Threat-intel lookups	When enabled	A public address or domain.	The lookup service, via ThinkCyber or the customer's key
GitHub search	With a token	Search terms for the organization.	GitHub
Login-page detection	When enabled	The login page fingerprint.	ThinkCyber relay
SOC Drills	When requested	Roles, experience and language. No network data.	ThinkCyber
Webhook alerts	When configured	Attack Surface alerts.	The customer's receiver
Location enrichment	Off by default	Outside addresses, to add company name and hostname. Basic location uses a local database and sends nothing.	ipinfo.io
Support access	Only while switched on (4 hours, 24 hours or 3 days)	An encrypted tunnel opened by the appliance; an engineer connects back through it with a short-lived signed certificate.	ThinkCyber relay, port 443
Additional sites	Professional	Alerts, device inventory, fingerprints and decoy contacts, signed by the site. No packet captures or logs.	The main appliance, HTTPS 443, dialled by the site

Table 12. Outbound connections. No port is opened from the internet; inside the network, administrators reach the web interface on HTTPS 443. Destinations are listed in Table 5.

12 Standards alignment

Specto+ produces evidence that supports specific safeguards in common frameworks. The table maps capabilities to CIS Critical Security Controls v8 safeguards and NIST Cybersecurity Framework 2.0 categories. Supporting a safeguard is not the same as satisfying it: process, ownership and remediation remain with the organization, and no product makes an organization compliant by itself.

Capability	CIS Controls v8 safeguard	NIST CSF 2.0
Device discovery and inventory	1.1 Establish and maintain a detailed enterprise asset inventory 1.3 Utilize an active discovery tool	ID.AM Asset Management
Internal vulnerability matching	7.5 Perform automated vulnerability scans of internal enterprise assets	ID.RA Risk Assessment
Attack Surface	7.6 Perform automated vulnerability scans of externally-exposed enterprise assets 9.5 Implement DMARC	ID.RA Risk Assessment
Intrusion engine; decoys support detection	13.3 Deploy a network intrusion detection solution	DE.CM Continuous Monitoring DE.AE Adverse Event Analysis
Endpoint Control isolation	–	RS.MI Incident Mitigation
SOC Drills, Executive Readiness	17.7 Conduct routine incident response exercises	PR.AT Awareness and Training ID.IM Improvement

Table 13. Indicative mapping to CIS Controls v8 safeguards and NIST CSF 2.0 categories.

13 Design boundaries

A security product that overstates what it knows is worse than having none. The following limits are part of the design and are stated so that they can be planned around.

- **One vantage point.** The intrusion engine sees the traffic that reaches the appliance's connection. The appliance has one adapter; what does not pass it is not seen.
- **No network-wide blocking.** The appliance blocks on its own firewall and can isolate a managed endpoint. It does not push rules to network firewalls.
- **TCP only.** Port scanning covers the full TCP range; UDP is not scanned.
- **Version evidence, not exploitation.** Confirmed findings are version matches, which a person reviews before acting.
- **No automatic patching.** Remediation is performed by the organization; Endpoint Control actions require a person's approval.
- **Integrations.** Attack Surface alerts go to a webhook. There is no SIEM or syslog connector.
- **Platforms.** Endpoint Control supports Windows and Linux. macOS is not supported.
- **Deployment.** Specto+ is self-hosted only. There is no cloud-hosted version.

14 Editions, ordering and specifications

The Free edition has no time limit and no device limit, and requires no registration, email address or licence code. Professional is a yearly licence per appliance, never per device. A 30-day evaluation of every Professional capability is available, with one 30-day extension; at the end of an evaluation the appliance returns to the Free edition with its data intact. Moving from Free or an evaluation to Professional keeps all data on the same appliance, with no reinstallation.

Feature	Free	Evaluation	Professional
Internal Visibility, intrusion engine, reports	•	•	•
Attack Surface	–	•	•
Phantom Bait	–	•	•
SOC Drills (unlimited)	–	•	•
Executive Readiness	–	•	•
Endpoint Control	–	•	•
Cy with the customer's cloud AI key	•	•	•
Cy with a model the customer runs	–	•	•
Additional sites	–	–	Per licence
Traffic recording storage	5 GB	Up to half the disk	Up to half the disk
Device limit	None	None	None
Term	Unlimited	30 days (+30)	Yearly

Table 14. Edition comparison. Software and vulnerability-data updates are included in every edition.

REVOKING OR ENDING A LICENCE

Revoking a licence never switches an appliance off; it prevents the code from being reused and stops ThinkCyber services such as SOC Drills. When a Professional licence ends, everything keeps working for 30 days. After that, the Free capabilities continue, the Professional modules stop, and their data stays readable. Routine traffic recordings are reduced to the Free allowance; evidence recordings are kept. Decoys stop after the 30 days and return on renewal without being set up again.

Ordering and support

Specto+ is sold by ThinkCyber partners and by ThinkCyber directly. A Professional licence covers one main appliance for one year; additional sites are added to the same licence and renew on the same date. Evaluations are issued by ThinkCyber.

Activation is a single online call when a code is entered. The appliance then verifies its signed licence locally; sites without internet open access briefly to activate or renew.

Partners provide the services around the appliance: installation, switch and VLAN configuration, connection of additional sites, Endpoint Control onboarding, monitoring, and on-site support. Custom exercises and team training are available through ThinkCyber's Cyberium platform.

Software releases and vulnerability-data updates are included for the term of the licence, in every edition.

Specifications

Item	Specification
Form factor	Virtual appliance, single OVA image
Hypervisor	ThinkCyber will confirm
Compute	Sized with the customer for the network; ThinkCyber will confirm
Network adapter	Bridged onto the monitored network (not NAT)
Decoys	Hypervisor must allow MAC address changes and forged transmits on the adapter
Network adapter	One bridged adapter, shared by scanning, the intrusion engine and decoys
Addressing	DHCP or fixed IP; optional HTTP proxy with bypass list
Port scanning	Frequent quick scan of common ports; full TCP scan per device
Vulnerability data	NIST NVD, CISA KEV
Intrusion engine	Built in, on traffic reaching the appliance
Endpoint protocols	WinRM, port 5985 (Windows); SSH, port 22 (Linux); agentless
AI	Anthropic, Google, OpenAI (customer key); OpenAI-compatible local endpoint (Professional)
Exports and alerts	PDF, CSV; webhook (Slack, Microsoft Teams, JSON)
Access control	Administrator and client roles; MFA for administrators; HTTPS; full audit trail; recovery key
Updates	Signed; online (opt-in) or from file for air-gapped sites

Table 15. Specifications. Describes release 1.7.6.

Glossary

Term	Meaning in this document
Appliance	One Specto+ virtual machine attached to one network.
Passive zone	A subnet the customer has excluded from active scanning. Its devices are reported as not assessed.
Decoy	A machine created by Phantom Bait that copies the ports and responses of a real machine and has no legitimate users.
Expected source	A scanner or inventory tool the customer has declared, whose contact with a decoy does not raise an alert.
Confirmed	A vulnerability whose affected version range contains the exact version a service announced.
Needs review	A possible vulnerability that depends on an approximate version and requires a person's judgement.
KEV	The CISA Known Exploited Vulnerabilities catalog: vulnerabilities with evidence of exploitation by attackers.

Table 16. Terms used in this data sheet.

SPECTO+

HOW TO EVALUATE SPECTO+

Request a 30-day evaluation

A 30-day evaluation includes every Professional capability on the customer's own network. Request it at

thinkcybergroup.com/specto-plus or through a ThinkCyber partner. The Free edition download will be announced on the same page.

ThinkCyber partners provide installation, network and VLAN work, multi-site connection, Endpoint Control onboarding, monitoring services and on-site support.

FOR MORE INFORMATION

ThinkCyber

ThinkCyber develops Specto+ and Cyberium, a hands-on cybersecurity training platform. The SOC Drills in Specto+ are built by Cyberium from attacks captured on ThinkCyber's own internet-facing decoys.

thinkcybergroup.com