SYMBEEO

PUBLIC

REFERENCE ARCHITECTURE

Zero-trust access for a multi-site enterprise on 2025–26 platforms: two design models from builds published by NIST

CAPABILITY	DOCUMENT	VERSION	DATE
Security	SRA-SEC-001	1.6	Nov 7, 2026

WRITTEN BY

David Morgan, Principal Security Architect

© 2026 Symbeeo. All rights reserved.

Document control

Document	SRA-SEC-001	Version	1.6
Issued	Nov 7, 2026	Status	Issued by Symbeeo
Classification	Public	Supersedes	1.5, Oct 10, 2026
Capability	Security	Author	David Morgan
Role	Principal Security Architect		
Credentials	CCISO, CISSP, CISSP-ISSEP, CISM, CISA, CRISC, PMP, CCSP, Adopting Zero Trust (Forrester)		
Approval	Approved by Edwin Ozer, Founder, Oct 10, 2026 (version 1.5). Version 1.6 issued by Symbeeo, Nov 7, 2026.		
Sign-off	"The practice lead signs this document before any build proceeds under it."		

Contents

1 · Scope 3
2 · Requirements register 4
3 · Architecture overview 5
4 · Component design 5
5 · Options and platform choices 6
6 · Failure conditions 7
7 · Validation 8
8 · Operations and lessons learned 8
9 · Appendix 8

© 2026 Symbeeo. All rights reserved. · Public

CONVENTIONS

Source tags. [S] read Sep 7, 2026 and Sep 24, 2026: NIST SP 1800-35 Implementing a Zero Trust Architecture, final, June 2025 — builds E2B3 and E1B5 reproduced as the two design models · Palo Alto PA-5450 datasheet (end-of-sale record) · Fortinet FortiGate 200G datasheet · Cisco ISE performance and scalability guide (release 3.5) · Cisco IT's own deployment, Cisco Live 2026 BRKCOC-2376 · from the 2026 technology review (§9.2), read Sep 24, 2026: the PA-5500 series datasheet, the Palo Alto and Cisco end-of-sale notices and the Cisco SNS 3800 series data sheet. [A] typical-buyer assumption. A row with more than one tag is counted once: as a published figure if any tag is [S] or [S*], otherwise as an assumption if any tag is [A], otherwise as a design target.

Table 1. Revision history

Date	Version	Change
Sep 15, 2026	1.0	First issue.
Sep 21, 2026	1.1	Corrections to wording, figure numbering and citations.
Sep 27, 2026	1.2	Revised to current platform versions and the current document format.
Sep 29, 2026	1.3	NERC CIP-004 coverage corrected to partial: R11 covers interactive remote access; removal of physical access is outside this document.
Oct 7, 2026	1.4	One rule removed from the §9.3 table of industry rules.
Oct 10, 2026	1.5	Approval line now reads: approved by the Founder, issued by Symbeeo. David Morgan remains the author.
Nov 7, 2026	1.6	Wording correction: the two design models come from builds published by NIST. NIST does not certify, validate or endorse.

1 · Scope

Who it is for. The CISO or head of infrastructure who must retire network-wide VPN trust and show an auditor the architecture they moved to, on platforms that will still be current in 2028.

Typical buyer [A]. The SRA-NET-001 client: 1,500 users at HQ, 3 branches, 2 data centers, two hyperscalers, 30 % remote workforce, managed laptops plus BYOD phones plus OT devices.

What is in. One policy engine; enforcement at the data-center edge, on every access port and at a cloud security edge; identity, posture, certificates; logging; two design models from builds published by NIST. **What is out.** SOC staffing; application security; data-loss prevention.

Related documents. NIST SP 800-207 (citation floor; final, August 2020, no revision, read Sep 24, 2026) · NIST SP 1800-35 (the builds; final, June 2025, no newer revision, read Sep 24, 2026) [S] · PA-5500 series datasheet [S] · FortiGate 200G datasheet [S] · ISE performance and scalability guide (updated Sep 8, 2026) [S] · Cisco SNS 3800 series data sheet [S] · BRKCOC-2376 [S] · lifecycle notices and software releases read Sep 24, 2026, with URLs, in §9.2.

© 2026 Symbeeo. All rights reserved. · Public

2 · Requirements register

Table 2. Requirements register

#	Requirement	Value	Source
R1	Sites	HQ · 3 branches · 2 DCs; site models: Large-Site HA (HQ, DCs), Small-Site HA (branches)	[A]
R2	Identity	Active Directory / Entra ID as external identity; identity-source sequencing defined	[S] 1800-35
R3	MFA coverage	100 % of interactive access to enforcement points	[A]
R4	Device classes	managed · BYOD · OT, each with a posture rule	[S] 1800-35 use cases
R5	Endpoints in the policy engine	5,000 at issue (2026-09), 20,000 ceiling; ISE 3.5 large deployment on SNS-3815/3855/3895 supports 2,000,000 active sessions; a small (two-node) deployment on SNS-3895 supports 50,000 (the SNS 3795 is not used: end of sale Dec 30, 2025)	[A]; [S] ISE guide, read Sep 24, 2026
R6	DC edge firewall	≥ 189 Gbps threat-prevention throughput (floor: the PA-5450's figure) [A]; chosen PA-5570: 240 Gbps threat prevention and 300 Gbps firewall (appmix, measured on PAN-OS 12.2); 8 × 10/25G SFP28, 12 × 40/100G QSFP28, 8 × 100/400G QSFP-DD; post-quantum key exchange (ML-KEM, HQC) for TLS decryption	[S] PA-5500 datasheet, read Sep 24, 2026
R7	Branch firewall	FortiGate 200G: 9 Gbps IPS, 7 Gbps NGFW, 6 Gbps threat protection; 8 × 10GE SFP+, 8 × 5GE RJ45	[S] FortiGate 200G datasheet (© 2026), read Sep 24, 2026
R8	Certificate authority	present; device certificates for 802.1X and per-app access	[S] 1800-35
R9	Policy-engine fail behavior	fail-closed for new sessions; existing sessions time out at 30 min	[A]
R10	Log retention	12 months hot, 24 months archive	[A]
R11	Revocation time	identity disabled → access lost ≤ 5 min	[A]
R12	Use cases demonstrated at acceptance	discovery and identification · policy enforcement · posture · least privilege · lateral movement blocked	[S] 1800-35 §6

© 2026 Symbeeo. All rights reserved. · Public

3 · Architecture overview

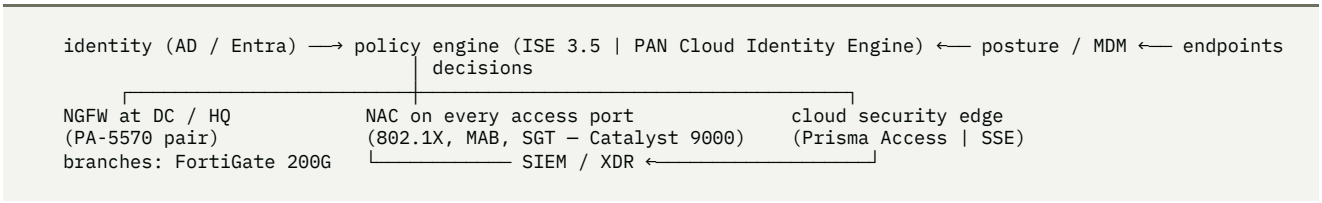


Figure 1. Policy engine and enforcement points

Model A uses the left and middle columns; Model B adds the right.

4 · Component design

Written as NIST build entries [S]. The two component lists below are NIST's, as built in SP 1800-35; they record what NIST built and are not edited. Where a product has since been renamed or has changed owner, the name current on Sep 24, 2026 follows each list (§9.2).

Model A · on-premises microsegmentation, from 1800-35 E2B3 (Cisco and Ping Identity as policy engines): products from Broadcom (VMware), Cisco Systems, IBM, Mandiant, Palo Alto Networks, Ping Identity, Radiant Logic, SailPoint, Tenable; certificates from DigiCert. Components: Cisco Duo, Cisco Identity Services Engine, Cisco network devices, Cisco Secure Endpoint, Cisco Secure Network Analytics, Cisco Secure Workload, DigiCert CertCentral, IBM Security QRadar XDR, Mandiant MSV, Palo Alto Networks NGFW, PingOne, RadiantOne, SailPoint IdentityIQ, Tenable.ad, Tenable.io, Tenable NNM, VMware Workspace ONE UEM and Access. **Names current on Sep 24, 2026 [S]:** VMware Workspace ONE UEM and Access → Omnissa Workspace ONE (Broadcom's end-user-computing business, now Omnissa under KKR since July 2024) · Tenable.ad → Tenable Identity Exposure · Tenable.io → Tenable Vulnerability Management · IBM Security QRadar XDR → IBM QRadar SIEM on premises (still supported by IBM); QRadar SaaS passed to Palo Alto Networks on Sep 4, 2024, with Cortex XSIAM as its migration path · Mandiant MSV → Mandiant Security Validation, Google Cloud, current (release 4.14.5.0, Feb 2026) · Cisco Secure Network Analytics current; its UCS M6 hardware appliances reach end of sale Dec 18, 2026, so none is quoted on M6 hardware (SDD-SEC-001 §9). 2026 platform instance: ISE 3.5 Patch 4 on SNS-3895 [S] (SNS 3795 not used: end of sale Dec 30, 2025), PA-5570 pair at each DC [S] (PA-5450 not used: end of sale Nov 22, 2026), FortiGate 200G pair at each branch [S], Catalyst 9000 enforcement on IOS XE 17.18.4 (SRA-NET-001 R15).

Model B · SASE, from 1800-35 E1B5 (Palo Alto Networks as policy engine): products from AWS, IBM, Mandiant, Okta, Palo Alto Networks, Radiant Logic, SailPoint, Tenable; certificates from DigiCert. Components: Panorama, PAN NGFW, Prisma Access, Prisma SASE (Prisma Access and Prisma SD-WAN), Cloud Delivered Security Services, Cloud Identity Engine, GlobalProtect, Strata Cloud Manager, Okta Identity Cloud, RadiantOne, SailPoint IdentityIQ, Okta Verify, QRadar XDR, Tenable.io, Tenable.ad, Tenable NNM, Mandiant MSV, DigiCert CertCentral, AWS IaaS. **Names current on Sep 24, 2026 [S]:** Tenable and Mandiant names as in Model A · QRadar XDR: in a Palo Alto-led model the QRadar SaaS path is Cortex XSIAM (above) · GlobalProtect is current and carries post-quantum remote access on the PA-5500 series (datasheet); the Prisma Agent is Palo Alto's newer agent for Prisma Access and coexists with GlobalProtect on the same endpoint and tenant. The Palo Alto NGFW in this model is a PA-5500 series appliance (PAN-OS 12.1 or later).

Substitution rule [A]. The policy engine and the DC NGFW are fixed per model; every other component is replaced by the client's incumbent where one exists and is supported.

© 2026 Symbeeo. All rights reserved. · Public

4.1 Policy engine.

Model A: ISE 3.5, deployment sized from the scalability guide (R5) [S], on SNS-3895 appliances, Cisco's named replacement for the SNS 3795 [S]. Model B: Cloud Identity Engine with Prisma Access. Design items: deployment architecture, node roles, authorization methods (dACL, VLAN, SGT), internal and external identity stores, identity-source sequencing, profiling, supplicant configuration, CA.

4.2 Enforcement points.

PA-5570 HA pair at each DC (R6); FortiGate 200G HA pair at each branch (R7); 802.1X on every access port (SRA-NET-001 R15); cloud edge for remote and SaaS (Model B).

4.3 Identity and certificates.

R2, R8; device certificates at enrollment; per-app access through a gateway rather than network-wide VPN — Cisco IT's control-plane / data-plane split [S] BRKCOC-2376.

4.4 Posture.

MDM/UEM feeds the policy engine; three device classes (R4).

4.5 Logging.

SIEM/XDR receives policy decisions, NGFW, NAC and cloud-edge logs; R10.

5 · Options and platform choices

Decision table. The option rows below the table give each option's fit and cost band, grouped under its decision. No row is decided by a published comparison, so no row carries [CMP].

Table 3. Options and platform choices

ID	Decision	Requirement	Alternatives considered	Decision taken	Rationale
D1	Design model	R4, R11, R12	(a) Model A, on-prem microsegmentation (E2B3): meets §2, cost licenses per node + NGFW · (b) Model B, SASE (E1B5): meets §2, cost per-user subscription · (c) VPN + flat network, hardened: fails R4, R11, R12, cost lowest	**(a) for DC-heavy clients, (b) for remote-heavy clients**	Both are builds published by NIST [S]; (c) is not zero trust. The typical buyer is DC-heavy, so SDD-SEC-001 applies (a) [A]
D2	DC edge firewall	R6	(a) PA-5570 pair: 240 Gbps threat prevention [S] · (b) PA-5560: 180 Gbps [S] · (c) PA-5580: 300 Gbps [S] · (d) PA-5450: end of sale Nov 22, 2026, announced May 22, 2026 [S] · (e) FortiGate at the DC: the 200G does not meet §2 (6 Gbps threat protection) [S]; larger FortiGate models were not evaluated in this set	**(a) PA-5570 HA pair per DC**	The DC NGFW vendor is fixed per model (§4 substitution rule): NIST builds E2B3 and E1B5 were built with Palo Alto NGFW [S]. Palo Alto names the PA-5500 series as the PA-5450's upgrade path [S]; (a) is the smallest PA-5500 model at or above the R6 floor; (b) is below it; (c) is oversized for a typical buyer [A]; (d) cannot be quoted (SDD-SEC-001 §9). Cost band: PAN higher than Fortinet

© 2026 Symbeeo. All rights reserved. · Public

ID	Decision	Requirement	Alternatives considered	Decision taken	Rationale
D3	Branch firewall	R7	(a) FortiGate 200G pair: 6 Gbps threat protection [S] · (b) Palo Alto at the branch: meets §2, cost higher	**(a) FortiGate 200G pair per branch**	Throughput class matches a branch [S]; current datasheet © 2026, no end-of-order notice found in public sources (§9.2, not verified in Fortinet's support portal)
D4	Policy-engine appliance (Model A)	R5	(a) SNS-3895: 50,000 endpoints in a small deployment, 2,000,000 in a large one [S] · (b) SNS-3855: same deployment limits, 128 GB RAM against 256 GB [S] · (c) SNS 3795: end of sale Dec 30, 2025, last date of support Dec 31, 2030 [S]	**(a) SNS-3895**	Cisco's named replacement for the SNS 3795 [S]; (b) meets R5 at lower cost and is the alternative if the client's ceiling stays at 20,000 [A]; (c) cannot be quoted
D5	Policy-engine fail behavior	R9	(a) fail-closed for new sessions · (b) fail-open: fails R9	**(a) fail-closed**	Decided in R9 [A]; signed by the client as SDD-SEC-001 P7

Option rows by decision.

Table 4. Options and platform choices

Decision	Option	Meets §2	Cost band	Chosen	Why
D1	Model A, on-prem microsegmentation (E2B3)	Y	licenses per node + NGFW	**Y** for DC-heavy clients	Build published by NIST [S]
D1	Model B, SASE (E1B5)	Y	per-user subscription	**Y** for remote-heavy clients	Build published by NIST [S]
D1	VPN + flat network, hardened	fails R4, R11, R12	lowest	N	Not zero trust
D2, D3	PA-5570 at DC vs FortiGate at DC	PA-5570 only	PAN higher	PAN at DC, Fortinet at branch	Throughput class (240 Gbps vs 6 Gbps threat protection) matches the site [S]; the 200G's 9 Gbps is its IPS figure (R7)
D5	Fail-open policy engine	fails R9	—	N	Decided in R9

6 · Failure conditions

Table 5. Failure conditions

#	Condition	What the user sees	Recovers by itself	Needs a hand	Time
F1	Policy-engine node down	none	PE cluster	replace node	0
F2	Policy-engine cluster down	new sessions refused (R9); existing continue to 30 min	no	restore	R9
F3	Identity store unreachable	new auth fails; cached sessions continue	no	restore directory	minutes
F4	DC NGFW member down	none	HA pair	replace	seconds

© 2026 Symbeeo. All rights reserved. · Public

#	Condition	What the user sees	Recovers by itself	Needs a hand	Time
F5	Branch firewall member down	none	HA pair	replace	seconds
F6	Cloud edge PoP down	reconnect to next PoP	yes	no	seconds
F7	CA unreachable	new enrollments fail; existing certificates valid	no	restore CA	hours

7 · Validation

None yet. Run 1800-35 functional demonstrations A (discovery and identification) and the lateral-movement case on the first build and record the results here.

8 · Operations and lessons learned

From Cisco IT [S]: map identities first; register devices and deploy certificates before enforcing; inventory everything; migrate VPN to per-app access in phases. Day 2: software baseline (ISE patch, PAN-OS, FortiOS, IOS XE) checked against the vendors' recommended releases each quarter and on the day of staging [A]. Symbeeo lessons: to be written by the signing engineer.

9 · Appendix

9.1 Components and references.

Component list per model (§4) · policy excerpts to be attached · references: SP 800-207, SP 1800-35, PA-5500 series datasheet, FortiGate 200G datasheet, ISE performance and scalability guide, SNS 3800 series data sheet, BRKCOC-2376, and the sources in §9.2.

9.2 2026 technology review, read Sep 24, 2026.

Every product, version, standard and date in this set checked against the owner's own page where one could be read. Kept where current; replaced where end-of-sale or superseded.

Table 6. 2026 technology review, read Sep 24, 2026

Item	Status read Sep 24, 2026	Action	Source
Palo Alto PA-5450	end of sale Nov 22, 2026 (announced May 22, 2026); support for 5 years after with a contract; upgrade path PA-5500 series	**replaced by PA-5570** (D2)	[S] `https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-sale`

© 2026 Symbeeo. All rights reserved. · Public

Item	Status read Sep 24, 2026	Action	Source
Palo Alto PA-5500 series	current; PA-5570 240 Gbps threat prevention, 300 Gbps firewall, ML-KEM and HQC key exchange in TLS decryption; figures measured on PAN-OS 12.2; no PA-5500 entry on the end-of-sale page	added	[S] `https://www.paloaltonetworks.com/resources/datasheets/pa-5500-series` (the vendor page gives a summary only; figures read from the vendor's datasheet PDF as hosted at `https://digitalscepter.com/assets/datasheets/pa-5500-series.pdf`)
PAN-OS	12.1 released Aug 28, 2025, end of life Aug 28, 2028; 12.2 released Jul 30, 2026; PA-5500 requires 12.x	baseline named: PAN-OS 12.1	[S] `https://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-life-summary`
Cisco SNS 3715/3755/3795	end of sale Dec 30, 2025, last date of support Dec 31, 2030; SNS 3795 → SNS-3895	**replaced by SNS-3895** (D4)	[S] `https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/secure-network-server-3715-3755-3795-eol.html`
Cisco SNS 3800 series	current (data sheet updated Apr 9, 2026); runs ISE 3.3 P7+, 3.4 P3+, 3.5; no notice on the ISE end-of-sale listing	added	[S] `https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/secure-network-server-3800-series-ds.html` · `https://www.cisco.com/c/en/us/products/security/identity-services-engine/eos-eol-notice-listing.html`
Cisco ISE 3.5	current; Patch 4 generally available Sep 14, 2026; no end-of-sale notice for 3.5 (3.1 and 3.2 announced Feb 23, 2026)	kept; baseline named: 3.5 Patch 4	[S] `https://www.cisco.com/c/en/us/td/docs/security/ise/3-5/release_notes/cisco-ise-release-notes-35.html`
ISE performance and scalability guide	updated Sep 8, 2026, covers 3.5 P3 onward; SNS 3800 figures in R5	kept	[S] `https://www.cisco.com/c/en/us/td/docs/security/ise/performance_and_scalability/b_ise_perf_and_scale.html`
Fortinet FortiGate 200G	current datasheet © 2026; no end-of-order date found in public sources; Fortinet's lifecycle page needs a support login	kept; **lifecycle not verified**	[S] `https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-200g-series.pdf`
FortiOS	8.0 released Apr 21, 2026; 7.6 supported to Jan 25, 2030; 7.2 support ends Sep 30, 2026	baseline named: 7.6, exact build per Fortinet's recommended release at staging [A]	secondary source `https://endoflife.date/fortios` (Fortinet's own page needs a login)

© 2026 Symbeeo. All rights reserved. · Public

Item	Status read Sep 24, 2026	Action	Source
Catalyst 9300X, IOS XE	no 9300X model on the 9300 end-of-sale listing; recommended IOS XE 17.18.4 and 17.15.6 (page updated Sep 4, 2026)	kept; baseline 17.18.4, as SRA-NET-001	[S] https://www.cisco.com/c/en/us/products/switches/catalyst-9300-series-switches/eos-eol-notice-listing.html · https://www.cisco.com/c/en/us/support/docs/switches/catalyst-9300-series-switches/214814-recommended-releases-for-catalyst-9200-9.html
NIST SP 1800-35	final, Jun 10, 2025; no newer revision	kept	[S] https://csrc.nist.gov/pubs/sp/1800/35/final
NIST SP 800-207	final, Aug 11, 2020; no revision or supersession	kept	[S] https://csrc.nist.gov/pubs/sp/800/207/final
NIST SP 800-88	Rev. 2 final, Sep 26, 2025 (cited in SDD-SEC-001 §9)	added	[S] https://csrc.nist.gov/pubs/sp/800/88/r2/final
Tenable.ad, Tenable.io	renamed Tenable Identity Exposure and Tenable Vulnerability Management (May 15, 2023)	current names recorded (§4)	[S] https://www.tenable.com/blog/tenable-product-name-changes-and-the-evolution-of-the-tenable-brand
VMware Workspace ONE	Broadcom's end-user-computing business sold to KKR, now Omnissa (closed July 2024)	current name recorded (§4)	[S] https://blogs.vmware.com/euc/2024/04/introducing-omnissa-the-former-vmware-end-user-computing-business.html
IBM QRadar XDR	QRadar SaaS assets sold to Palo Alto Networks, closed Sep 4, 2024, migration path Cortex XSIAM; on-prem QRadar keeps IBM support	status recorded (§4)	[S] https://www.paloaltonetworks.com/company/press/2024/palo-alto-networks--closes-acquisition-of-ibm-s-qradar-saas-assets
Mandiant MSV	current, Google Cloud; release 4.14.5.0 on Feb 19, 2026	kept	[S] https://security.googlecloudcommunity.com/security-validation-5/msv-4-14-5-0-product-release-february-19-2026-6858
Cisco Secure Network Analytics	product current; UCS M6 hardware appliances end of sale Dec 18, 2026	kept; M6 hardware excluded from quotes	[S] https://www.cisco.com/c/en/us/products/collateral/security/stealthwatch/ucs-m6-secure-network-analytics-hw-eol.html
GlobalProtect / Prisma Agent	both current (the vendor's page now names it Prisma Agent, read Sep 27, 2026); they coexist on an endpoint	kept; newer agent recorded (§4)	[S] https://docs.paloaltonetworks.com/prisma-access-agent/user-guide/prisma-access-agent-for-desktop-devices/switch-between-prisma-access-agent-and-gp-app

© 2026 Symbeeo. All rights reserved. · Public

Item	Status read Sep 24, 2026	Action	Source
Okta Identity Cloud, PingOne, RadiantOne, SailPoint IdentityIQ, DigiCert CertCentral, Cisco Duo, Secure Endpoint, Secure Workload, Panorama, Strata Cloud Manager, Prisma Access, Prisma SD-WAN, Cloud Identity Engine	not individually checked on Sep 24, 2026	kept as NIST's build names; **not verified**	—

9.3 · Industry rules this architecture helps a buyer meet.

Only rules linked to this document's requirements are listed; rules this document does not address are left out.

Table 7. Industry rules this architecture helps a buyer meet

Rule	Jurisdiction	What it asks of infrastructure	Requirements here	Coverage
FBI CJIS Security Policy v6.1 (Jun 25, 2026; supersedes v6.0)	US · criminal-justice agencies and their contractors	MFA and audit logging for access to criminal-justice information	R3, R10	partial
NYDFS 23 NYCRR Part 500, Second Amendment (Nov 2023; last phase in force Nov 1, 2025)	US · New York · DFS-regulated financial entities	§500.12 MFA for all access to information systems	R3 (§500.13 asset inventory: SRA-CON-001 R2)	full
PCI DSS v4.0.1 (Jun 2024)	Card schemes · any merchant or service provider	Req. 10.5.1: audit logs kept 12 months, 3 immediately available; Req. 1: segmentation of the cardholder data environment (scoping is the assessor's)	R10, R12	full
HIPAA Security Rule, 45 CFR Part 164 Subpart C (the January 2025 proposed update is not final)	US · covered entities and business associates	audit controls: activity in systems holding ePHI recorded and examined	R10	partial
NERC CIP-004-7 (enforceable; CIP-004-8 from Jul 1, 2028)	US and Canada · Bulk Electric System entities	unescorted physical and interactive remote access removed within 24 h of termination	R11 (interactive remote access; removal of unescorted physical access is not met by a network requirement and is outside this document)	partial
TSA Security Directive Pipeline-2021-02G (in force May 3, 2026 to May 2, 2027)	US · designated pipeline owners and operators	IT/OT segmentation so OT keeps running if IT is compromised; access control; continuous monitoring	R4, R12	partial
21 CFR Part 11 (electronic records; electronic signatures)	US · FDA-regulated records	system access limited to authorized individuals	R11	partial
EU GMP Annex 11 Computerized Systems (2011 revision in force; the 2025 revision draft is not final)	EU · medicinal-product manufacturers	access to computerized systems limited to authorized people	R11	partial

© 2026 Symbeeo. All rights reserved. · Public

Rule	Jurisdiction	What it asks of infrastructure	Requirements here	Coverage
MPA Content Security Best Practices v5.3.2, assessed through the Trusted Partner Network (TPN)	Studio contract requirement (US-led, applied worldwide)	content networks segmented from general networks	R12	partial

Naming a rule here is not a claim of compliance or certification: the buyer's assessor decides compliance, and Symbeeo holds no certification or authorization.

Sources for §9.3, read Sep 25, 2026: CJIS Security Policy v6.1 [S] `https://le.fbi.gov/file-repository/cjis_security_policy_v6-1_20260625.pdf` · 23 NYCRR 500 [S] `https://www.dfs.ny.gov/cybersecurity/23-NYCRR-Part-500` · amended text [S] `https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf` · PCI DSS v4.0.1 [S] `https://www.pcisecuritystandards.org/document_library/` (version); requirement numbers [S*] from secondary summaries, the standard sits behind a license click-through · HIPAA Security Rule; status of the proposed update, final action targeted July 2027 [S] `https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202510&RIN=0945-AA22` · NERC CIP-004-7 [S] `https://www.nerc.com/standards/reliability-standards/cip/cip-004-7` · TSA SD Pipeline-2021-02G [S] `https://www.tsa.gov/sd-and-ea` · 21 CFR Part 11 [S] `https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11` (text read on the eCFR) · EudraLex Volume 4, Annex 11 [S] `https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en` · MPA best practices and TPN [S] `https://www.trustedpartnernetwork.org/links-resources/` (v5.3.2 release date not stated on the page).

© 2026 Symbeeo. All rights reserved. · Public

SYMBEEO

Each vendor's tool shows you their option. We show you all of them against one requirement.

Compared. Then Delivered.

hello@symbeeo.com · symbeeo.com

© 2026 Symbeeo. All rights reserved.

Product and company names and logos are their owners' trademarks, shown only to identify the lines Symbeeo sources. Naming a vendor or showing its logo does not mean the vendor sponsors or approves Symbeeo's comparisons or any recommendation Symbeeo makes.

Figures are as published by their sources on the dates given in this document; figures marked [A] are assumptions.

SRA-SEC-001 · Version 1.6 · Nov 7, 2026