

CMP-006

Campus Networking Platforms

Wired, wireless, assurance and campus
operations



CURRENT EVIDENCE SNAPSHOT

Official product sources refreshed through 2026-09-17

Controlled Mythos laboratory rerun: NOT ASSERTED

VERSION 1.2.0-candidate

CANDIDATE COMPARATIVE EVALUATION / PUBLIC

BENCHMARK DOCTRINE

Gates before scores. Evidence before
certainty. Profile fit before universal ranking.

Campus Networking Platforms

Wired, wireless, assurance and campus operations

DOCUMENT ID

CMP-006

VERSION

1.2.0-candidate

STATUS

Candidate Comparative Evaluation

PUBLICATION DATE

2026-09-17

SCHEDULED REVIEW

2026-12-16

CANONICAL ROUTE

/library/evaluations/cmp-006/

4

CANDIDATES

9

MANDATORY GATES

E2

CURRENT MAX EVIDENCE

18

ATOMIC CRITERIA

3

WORKLOAD PROFILES

CURRENT DECISION BOUNDARY

Reopen the cloud-native assurance and mixed-vendor profile. Mist support for selected AOS-CX switches changes the candidate boundary. Current versions require lab proof on provisioning, assurance, NAC, upgrade, failure, and rollback before any portfolio preference is asserted.

NO CURRENT UNIVERSAL WINNER IS PUBLISHED FROM THIS REFRESH.

July 24 baseline scores are preserved as lineage and sensitivity evidence, not silently reissued as September laboratory results.

Cisco Catalyst Center

3.3.1 / 2026-09-09

REFRESH TRIGGER

3.3.1 refreshes integrations and operations across the Catalyst management surface.

HPE Aruba Networking Central

Cloud updates through 2026-08-18

REFRESH TRIGGER

Central continues rapid cloud delivery across configuration, NAC, assurance, and Copilot-oriented operations.

Juniper Mist

2026-09-09 update

REFRESH TRIGGER

Mist now onboards, configures, monitors, upgrades, and troubleshoots selected HPE AOS-CX switches, materially changing mixed-vendor fit.

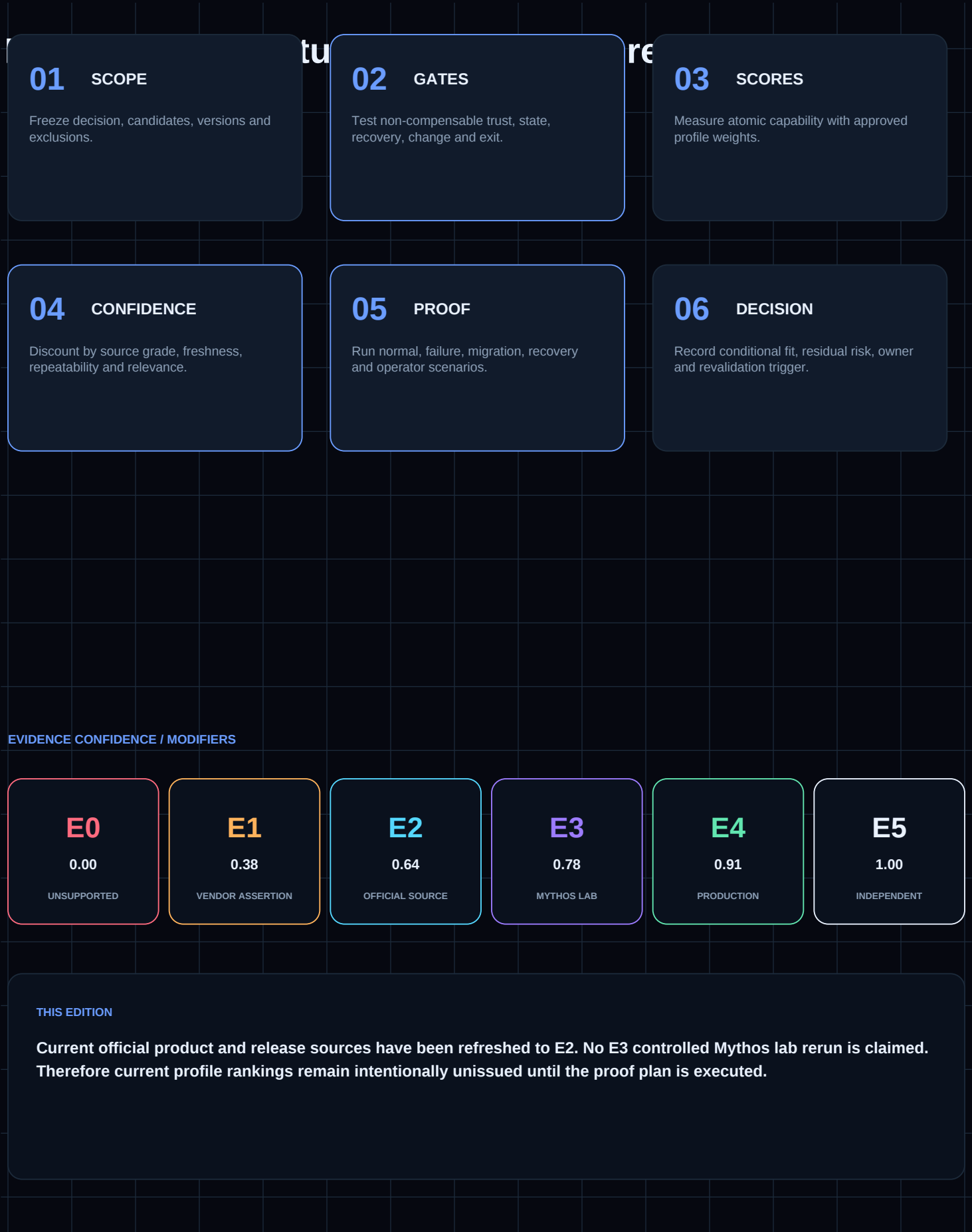
Fortinet Campus and Branch

FortiManager 7.6.7 / FortiOS 7.6.7

REFRESH TRIGGER

Current management and FortiOS lines continue security-converged branch/campus development with explicit upgrade constraints.

FINAL BENCHMARK SYSTEM / DECISION ARCHITECTURE



What changed since the July benchmark snapshot

Changes below are sourced from current official release documentation. They identify revalidation triggers; they are not translated into new numeric scores without controlled proof.

Cisco Catalyst Center 3.3.1 / 2026-09-09 MATERIAL DELTA 3.3.1 refreshes integrations and operations across the Catalyst management surface. CRITERIA TOUCHED C01 / C05 / C06 / C07 / C14 MODERATE REVALIDATION	HPE Aruba Networking Central Cloud updates through 2026-08-18 MATERIAL DELTA Central continues rapid cloud delivery across configuration, NAC, assurance, and Copilot-oriented operations. CRITERIA TOUCHED C01 / C03 / C07 / C10 / C14 MODERATE REVALIDATION
Juniper Mist 2026-09-09 update MATERIAL DELTA Mist now onboards, configures, monitors, upgrades, and troubleshoots selected HPE AOS-CX switches, materially changing mixed-vendor fit. CRITERIA TOUCHED C01 / C05 / C06 / C08 / C10 / C14 MATERIAL REVALIDATION	Fortinet Campus and Branch FortiManager 7.6.7 / FortiOS 7.6.7 MATERIAL DELTA Current management and FortiOS lines continue security-converged branch/campus development with explicit upgrade constraints. CRITERIA TOUCHED C01 / C02 / C05 / C09 / C14 MODERATE REVALIDATION

MANDATORY GATES / CURRENT REVALIDATION POSTURE

Mandatory gates remain non-compensable

No current release is marked PASS solely from documentation. E2 means the official source supports the capability path; LAB and RETEST identify proof still required. HOLD blocks a current decision.

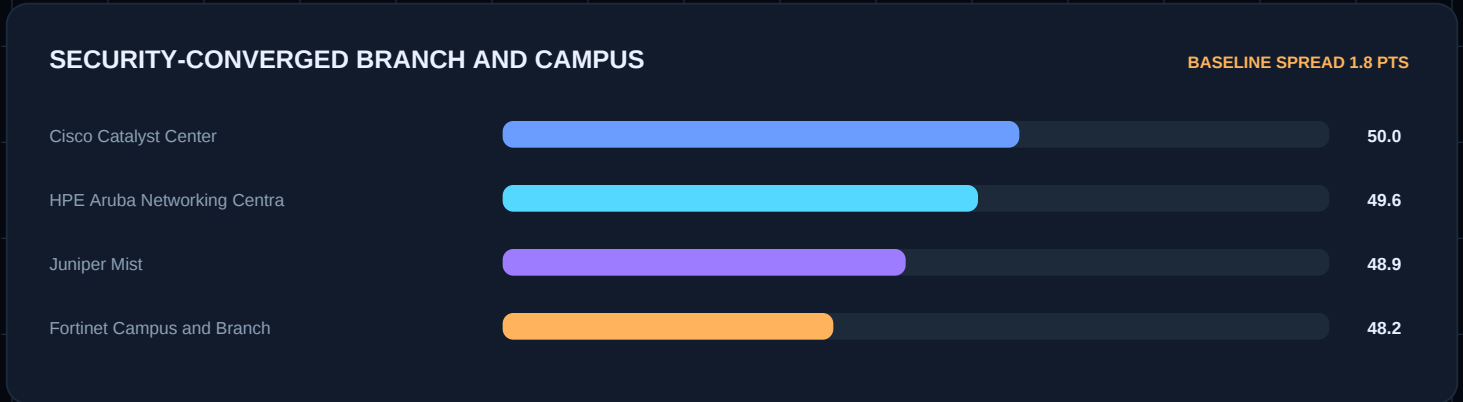
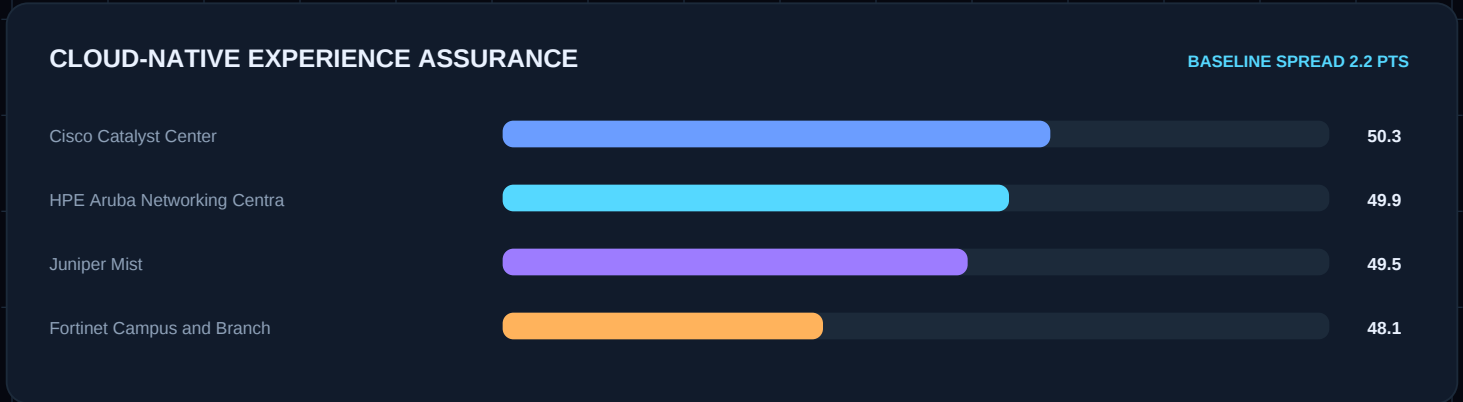
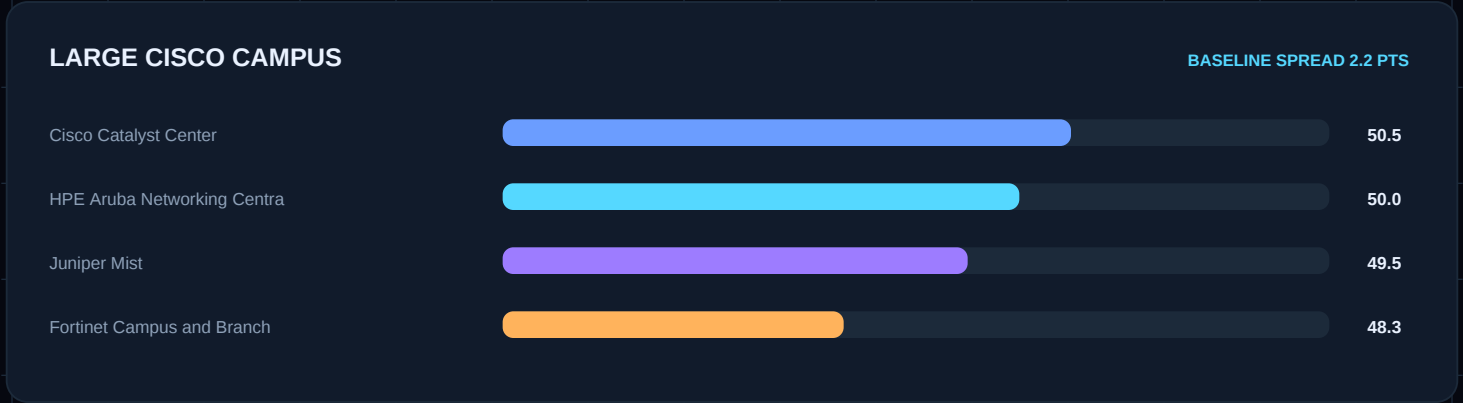
MANDATORY GATE	CISCO CATALYST	HPE ARUBA NETWO	JUNIPER MIST	FORTINET CAMPUS
C01 Functional coverage	RETEST	RETEST	RETEST	RETEST
C02 Security / trust	E2	E2	E2	RETEST
C03 Governance / approval	E2	RETEST	E2	E2
C04 State integrity	E2	E2	E2	E2
C07 Observability / evidence	RETEST	RETEST	E2	E2
C09 Resilience / continuity	LAB	LAB	LAB	RETEST
C11 Change safety / rollback	LAB	LAB	LAB	LAB
C16 Portability / exit	LAB	LAB	LAB	LAB
C18 Assurance confidence	HOLD	HOLD	HOLD	HOLD

LEGEND

E2	official-source support only	LAB	controlled proof required	RETEST	release delta touches this gate	HOLD	decision gate remains closed
----	------------------------------	-----	---------------------------	--------	---------------------------------	------	------------------------------

Historical profile sensitivity - preserved, not reissued

Values below are the 2026-07-24 evidence-adjusted baseline. They show sensitivity to operating-model weights. The September refresh does not recompute rank because E3 lab proof has not been reproduced.



CURRENT RANK STATUS: WITHHELD PENDING CONTROLLED PROOF.

Evidence confidence is separate from capability

E5

Independent repeatable validation

confidence modifier 1.00

E4

Production evidence in adopting environment

confidence modifier 0.91

E3

Controlled Mythos laboratory result

confidence modifier 0.78

E2

Official documentation / release / source

confidence modifier 0.64

E1

Vendor assertion or marketing

confidence modifier 0.38

E0

Unsupported or unverified

confidence modifier 0.00

CURRENT EVIDENCE STATE

Cisco Catalyst Center

E2 REFRESHED

Historical adjusted confidence: 58.2%

E3 LAB: NOT REPRODUCED

HPE Aruba Networking Central

E2 REFRESHED

Historical adjusted confidence: 58.2%

E3 LAB: NOT REPRODUCED

Juniper Mist

E2 REFRESHED

Historical adjusted confidence: 58.2%

E3 LAB: NOT REPRODUCED

Fortinet Campus and Branch

E2 REFRESHED

Historical adjusted confidence: 58.2%

E3 LAB: NOT REPRODUCED

ASSURANCE RULE

A current release note can change capability context, but it cannot raise assurance beyond E2. Current recommendation strength is therefore bounded until the test plan produces reproducible artifacts.

MIGRATION, LIFECYCLE AND IRREVERSIBLE-COMMITMENT RISK

Lifecycle risk is evaluated independently of features

The benchmark models migration, upgrade, compatibility, support, staffing, data/state export, downtime and exit. Current release changes below are explicit proof triggers.

Cisco Catalyst Center MODERATE REVALIDATION 3.3.1 refreshes integrations and operations across the Catalyst management surface. RETEST: C01 / C05 / C06 / C07 / C14
HPE Aruba Networking Central MODERATE REVALIDATION Central continues rapid cloud delivery across configuration, NAC, assurance, and Copilot-oriented operations. RETEST: C01 / C03 / C07 / C10 / C14
Juniper Mist MATERIAL REVALIDATION Mist now onboards, configures, monitors, upgrades, and troubleshoots selected HPE AOS-CX switches, materially changing mixed-vendor fit. RETEST: C01 / C05 / C06 / C08 / C10 / C14
Fortinet Campus and Branch MODERATE REVALIDATION Current management and FortiOS lines continue security-converged branch/campus development with explicit upgrade constraints. RETEST: C01 / C02 / C05 / C09 / C14

IRREVERSIBLE COMMITMENT GATE

Before migration or procurement lock-in, prove rollback, state portability, operational reconstruction, and supplier-exit assumptions.

Controlled proof is the next decision-producing step

REPRODUCTION STATE / NOT EXECUTED IN THIS EVIDENCE-REFRESH RELEASE

01

CONTROLLED SCENARIO

Deploy a representative wired and wireless site hierarchy with users, guests, IoT, voice, and critical applications.

02

CONTROLLED SCENARIO

Measure discovery, provisioning, configuration compliance, telemetry completeness, and client-assurance accuracy.

03

CONTROLLED SCENARIO

Inject DHCP, DNS, RADIUS, RF, roaming, PoE, VLAN, routing, WAN, and certificate failures.

04

CONTROLLED SCENARIO

Exercise software upgrade, rollback, device replacement, site outage, and management-plane loss.

05

CONTROLLED SCENARIO

Validate API, webhooks, ITSM, source-of-truth, SIEM, and automated-remediation controls.

06

CONTROLLED SCENARIO

Compare operator time-to-diagnose and time-to-recover using blinded scenarios.

EVIDENCE PACKAGE

Preserve exact versions, architecture, configuration, scenario, expected result, instrumentation, raw output, timing, failures, operator actions, deviations, acceptance state, owner, and artifact hashes.

Current decision posture

Reopen the cloud-native assurance and mixed-vendor profile. Mist support for selected AOS-CX switches changes the candidate boundary. Current versions require lab proof on provisioning, assurance, NAC, upgrade, failure, and rollback before any portfolio preference is asserted.

CURRENT RANKING: NOT REISSUED / CONTROLLED LAB REQUIRED

CURRENT OFFICIAL-SOURCE REGISTER / CHECKED 2026-09-17

Cisco Catalyst Center	E2 / OFFICIAL	
Cisco Catalyst Center 3.3.1 release notes		www.cisco.com
HPE Aruba Networking Central	E2 / OFFICIAL	
HPE Aruba Networking Central release notes		arubanetworking.hpe.com
Juniper Mist	E2 / OFFICIAL	
Juniper Mist Sep 9 2026 update		www.juniper.net
Fortinet Campus and Branch	E2 / OFFICIAL	
FortiManager 7.6.7 release notes		docs.fortinet.com

REVISION LINEAGE

1.2.0-candidate / 2026-09-17 - current-source evidence refresh; no lab rescore issued.

1.1.0-candidate / 2026-07-24 - baseline benchmark using the final comparative evaluation system.

Trigger earlier review after major release, acquisition, licensing change, critical vulnerability, material outage, failed PoC, or workload change.

BASELINE ANALYTIC RECORD CONTINUES ON PAGE 11 FOR TRACEABILITY.

ATOMIC CRITERIA MODEL

WEIGHTED CAPABILITY WITH EXPLICIT MINIMUM EVIDENCE

ID	CRITERION	WEIGHT	GATE	MINIMUM EVIDENCE
C01	Campus wired, wireless, policy, assurance, and lifecycle coverage	5	YES	Feature documentation, APIs, configuration exports, and scenario demonstration.
C02	Security and trust architecture	5	YES	Threat model, identity flows, RBAC tests, audit records, and security configuration.
C03	Governance and approval controls	5	YES	Approval workflow, policy controls, separation-of-duties tests, and decision records.
C04	Inventory, topology, intent, configuration, and telemetry integrity	5	YES	Backup, restore, rollback, drift, and corruption-recovery evidence.
C05	Automation and API quality	4	NO	API specifications, authentication tests, rate limits, event samples, and automation runs.
C06	Integration ecosystem	4	NO	Supported integrations, connector tests, failure behavior, and lifecycle ownership.
C07	Observability and evidence	4	YES	Logs, traces, metrics, reports, export tests, and evidence-retention controls.
C08	Site, device, client, event, and telemetry scale	4	NO	Controlled load tests, topology scale, saturation behavior, and capacity model.
C09	Resilience and continuity	5	YES	Failure injection, HA tests, recovery timing, degraded-mode operation, and runbooks.
C10	Network-operator and service-desk cognition	3	NO	Task observation, error-rate measures, navigation tests, and operator interviews.
C11	Change safety and rollback	5	YES	Plan or preview output, canary tests, rollback execution, and post-change verification.
C12	Extensibility and programmability	3	NO	Plugin, module, provider, workflow, or code-extension tests and upgrade impact analysis.
C13	Cloud, on-premises, hybrid, and disconnected management options	3	NO	Deployment architecture, data-flow mapping, residency evidence, and offline tests.
C14	Lifecycle and upgrade discipline	4	NO	Release notes, upgrade test, compatibility matrix, support policy, and migration plan.
C15	Economics and cost predictability	3	NO	Bill-of-materials, licensing model, staffing estimates, metering, and sensitivity analysis.
C16	Portability and exit	4	YES	Export tests, format analysis, replacement workflow, and decommission evidence.
C17	Vendor and ecosystem risk	3	NO	License analysis, roadmap evidence, bus-factor indicators, and dependency inventory.
C18	Assurance confidence	5	YES	Source provenance, lab artifacts, production evidence, independent replication, and review date.

SCORE SCALE

0 absent; 1 materially deficient; 2 partial; 3 adequate with limits; 4 strong; 5 leading for the defined profile. Scores remain provisional until the required evidence grade is achieved.

RAW CAPABILITY SCORECARD

DOCUMENTED CAPABILITY BEFORE EVIDENCE DISCOUNT

CRITERION	CATALYST CENTER	ARUBA CENTRAL	MIST	FORTINET
C01 Campus wired, wireless, policy, assurance, and lifecycle coverage	4.8	4.7	4.6	4.3
C02 Security and trust architecture	4.4	4.4	4.4	4.5
C03 Governance and approval controls	4.3	4.2	4.1	4.1
C04 Inventory, topology, intent, configuration, and telemetry integrity	4.4	4.3	4.2	4.1
C05 Automation and API quality	4.6	4.5	4.5	4.4
C06 Integration ecosystem	4.5	4.4	4.4	4.4
C07 Observability and evidence	4.7	4.6	4.8	4.2
C08 Site, device, client, event, and telemetry scale	4.7	4.5	4.6	4.4
C09 Resilience and continuity	4.4	4.3	4.4	4.2
C10 Network-operator and service-desk cognition	4.4	4.4	4.7	4.0
C11 Change safety and rollback	4.4	4.3	4.2	4.2
C12 Extensibility and programmability	4.3	4.2	4.2	4.0
C13 Cloud, on-premises, hybrid, and disconnected management options	3.8	4.3	3.0	4.1
C14 Lifecycle and upgrade discipline	4.1	4.0	4.3	3.9
C15 Economics and cost predictability	3.3	3.6	3.5	4.1
C16 Portability and exit	3.5	3.7	3.4	3.6
C17 Vendor and ecosystem risk	3.6	3.7	3.5	3.6
C18 Assurance confidence	3.5	3.5	3.4	3.4

WEIGHTED BASELINE / 100

Catalyst Cen

84.8

Aruba Centra

84.3

Mist

83.0

Fortinet

81.9

EVIDENCE-ADJUSTED SCORECARD

CAPABILITY DISCOUNTED BY CURRENT EVIDENCE CONFIDENCE

CANDIDATE	RAW	EVIDENCE CONFIDENCE	ADJUSTED	CURRENT STATE
Catalyst Center	84.8	58.2%	49.9	CONTROLLED LAB PENDING
Aruba Central	84.3	58.2%	49.6	CONTROLLED LAB PENDING
Mist	83.0	58.2%	48.8	CONTROLLED LAB PENDING
Fortinet	81.9	58.2%	48.1	CONTROLLED LAB PENDING

EVIDENCE SCALE

E0 / 0.00

Unsupported or unverified

E1 / 0.38

Vendor assertion or marketing statement

E2 / 0.64

Official documentation, release notes, or source repository

E3 / 0.78

Controlled Mythos laboratory result

E4 / 0.91

Production evidence from the adopting environment

E5 / 1.00

Independent repeatable validation

CURRENT CONFIDENCE BOUNDARY

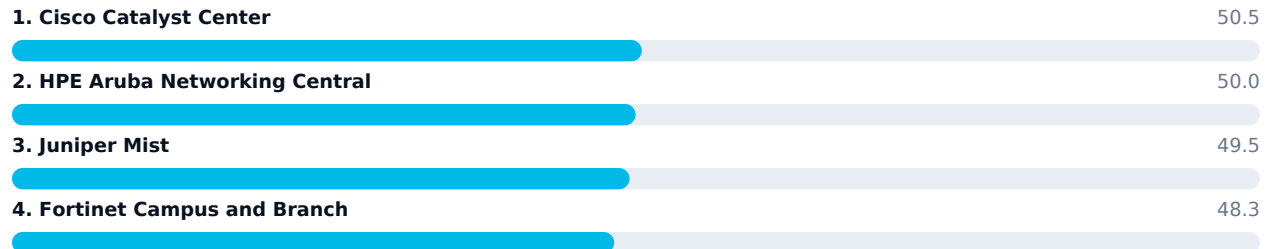
Most candidate criteria are supported at E2: official documentation or source evidence. Environment-specific laboratory, production, and independent evidence remain future gates.

PROFILE-SPECIFIC RANKINGS

EVIDENCE-ADJUSTED SENSITIVITY ANALYSIS

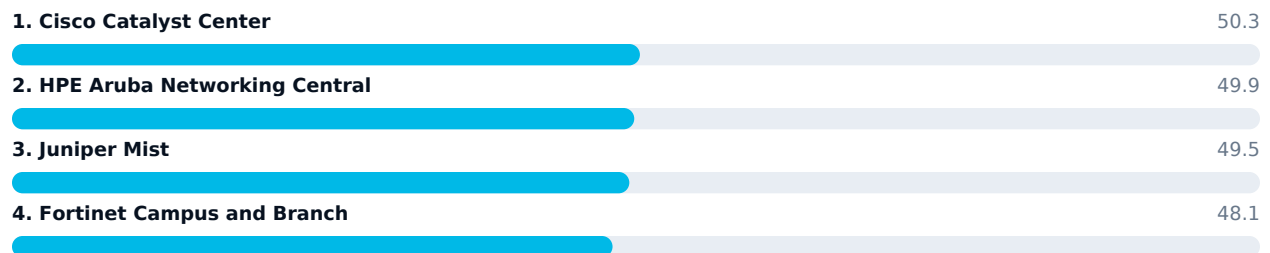
LARGE CISCO CAMPUS

Prioritizes Cisco design, provisioning, SD-Access, assurance, inventory, and enterprise integration.



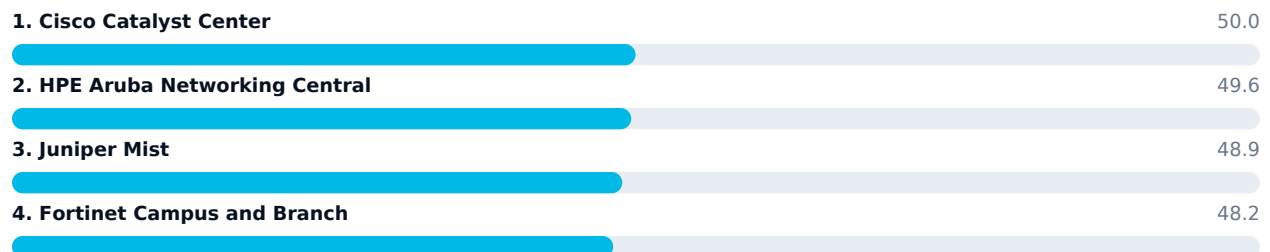
CLOUD-NATIVE EXPERIENCE ASSURANCE

Prioritizes client experience, wired/wireless assurance, API operations, rapid feature delivery, and service cognition.



SECURITY-CONVERGED BRANCH AND CAMPUS

Prioritizes security integration, branch, SD-WAN adjacency, central lifecycle, economics, and appliance breadth.



RANK SENSITIVITY

Small score differences are not decision certainty. Treat near-ties as a requirement for deeper PoC, commercial, migration, and operating-model evidence.

CANDIDATE DEEP DIVE / 01

CISCO CATALYST CENTER

OPERATING MODEL

Cisco campus management, design, provisioning, policy, automation, inventory, topology, and assurance platform.

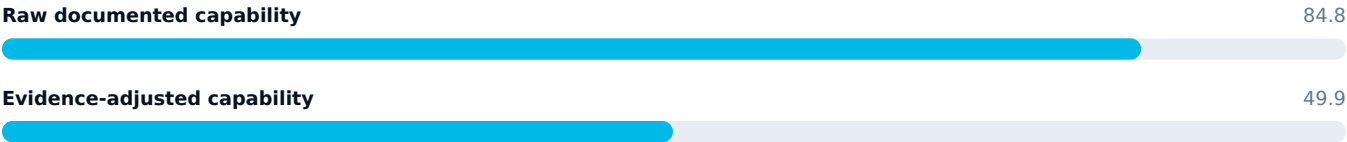
DOCUMENTED STRENGTHS

- Deep Cisco campus integration.
- Rich inventory, design, provisioning, assurance, and SD-Access workflows.
- Broad API and platform integration.
- Strong fit for large Cisco wired and wireless estates.

CAUTIONS AND PROOF OBLIGATIONS

- Platform and appliance lifecycle can be substantial.
- Best value depends on Cisco-centric infrastructure and licensing.
- Assurance quality depends on telemetry, design, and operational discipline.

BASELINE SCORE PROFILE



GATE DISPOSITION

PASS - large Cisco campus profile | CONDITIONAL - platform lifecycle and licensing

CANDIDATE DEEP DIVE / 02

HPE ARUBA NETWORKING CENTRAL

OPERATING MODEL

Cloud or on-premises network-management and operations platform for Aruba wired, wireless, gateway, branch, and policy ecosystems.

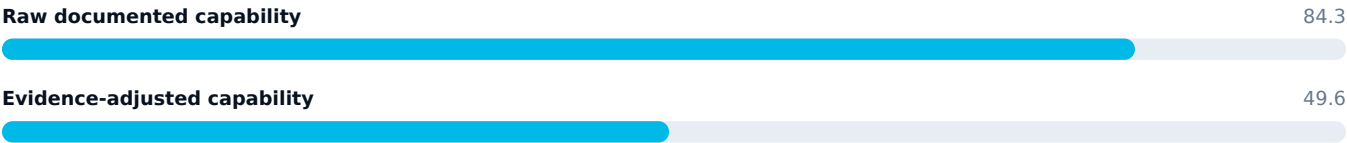
DOCUMENTED STRENGTHS

- Strong Aruba wired and wireless integration.
- Cloud and on-premises options.
- Broad campus, branch, policy, and operations coverage.
- Validated solution guidance and mature enterprise networking heritage.

CAUTIONS AND PROOF OBLIGATIONS

- Classic and new Central transitions require architecture and feature validation.
- Licensing and feature parity must be verified per deployment model.
- Cross-version and device-family operations require disciplined testing.

BASELINE SCORE PROFILE



GATE DISPOSITION

PASS - Aruba campus and deployment-flexibility profile | CONDITIONAL - platform-generation parity

CANDIDATE DEEP DIVE / 03

JUNIPER MIST

OPERATING MODEL

Cloud-native AI-driven wired, wireless, access-assurance, location, and operations platform.

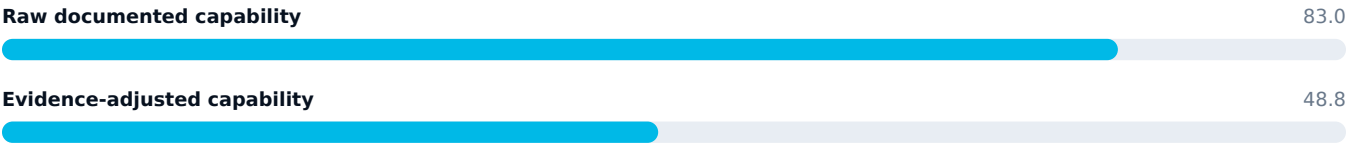
DOCUMENTED STRENGTHS

- Strong experience and assurance orientation.
- Cloud-native operational model and Marvis-assisted troubleshooting.
- Wired, wireless, and access assurance convergence.
- Modern APIs and microservices delivery.

CAUTIONS AND PROOF OBLIGATIONS

- Cloud-service dependency and subscription model are material.
- Best fit depends on Juniper and Mist ecosystem alignment.
- AI-driven recommendations require transparent operational validation.

BASELINE SCORE PROFILE



GATE DISPOSITION

PASS - cloud-native experience-assurance profile | CONDITIONAL - cloud dependency and ecosystem fit

CANDIDATE DEEP DIVE / 04

FORTINET CAMPUS AND BRANCH

OPERATING MODEL

FortiGate, FortiSwitch, FortiAP, FortiManager, and Security Fabric operating model for converged campus, branch, and security.

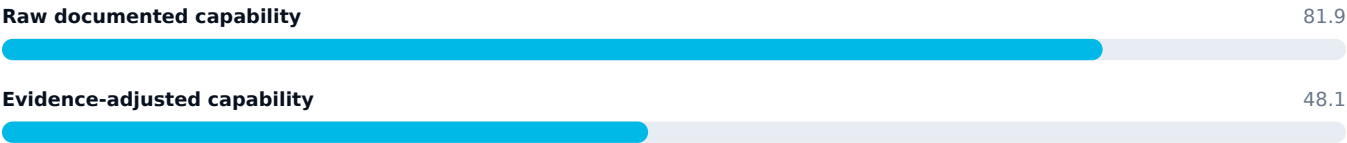
DOCUMENTED STRENGTHS

- Converged security and network operations.
- Broad branch and campus appliance ecosystem.
- Potential commercial and operational consolidation.
- Central management and automation within the Security Fabric.

CAUTIONS AND PROOF OBLIGATIONS

- Campus assurance depth must be tested against requirements.
- Ecosystem coupling and firmware discipline are central risks.
- Network and security ownership boundaries must be designed deliberately.

BASELINE SCORE PROFILE



GATE DISPOSITION

PASS - security-converged branch profile | CONDITIONAL - campus assurance and firmware governance

ARCHITECTURE AND INTEGRATION FIT

THE PRODUCT IS ONLY ONE PART OF THE OPERATING SYSTEM

REFERENCE OPERATING LAYERS

01 Intent, site, policy, and inventory authority

02 Wired, wireless, gateway, access, and identity infrastructure

03 Telemetry, assurance, analytics, and incident workflows

04 Provisioning, automation, software, and configuration lifecycle

05 Evidence, recovery, integration, and service management

INTEGRATION BOUNDARIES

- Identity, NAC, PKI, DHCP, DNS, and IPAM
- ITSM, collaboration, and incident command
- SIEM, NDR, endpoint, and security platforms
- Cloud, WAN, SD-WAN, branch, and datacenter
- APIs, event streaming, automation, and source of truth

ARCHITECTURE GATE

Every external dependency requires an owner, identity boundary, failure mode, evidence path, version policy, recovery procedure, and exit strategy.

SECURITY, OPERATIONS, LIFECYCLE, ECONOMICS, AND EXIT

CROSS-DOMAIN DECISION RECORD

SECURITY AND AUTHORITY

Identity, credentials, secrets, roles, privileged actions, signing, approvals, isolation, audit, and incident response must be tested as an integrated system.

RELIABILITY AND RECOVERY

Control-plane, data-plane, dependency, region, database, queue, network, and operator failures require defined degraded modes and recovery objectives.

CHANGE AND LIFECYCLE

Version, compatibility, migration, canary, rollback, content, plugin, provider, firmware, and decommission procedures are part of product fitness.

ECONOMICS AND CAPACITY

Licenses, metering, data, compute, hardware, storage, support, staffing, training, integration, migration, and opportunity cost require sensitivity analysis.

SOVEREIGNTY AND PRIVACY

Data location, support access, telemetry, subprocessors, encryption, key control, disconnected operation, and legal obligations must align with policy.

PORTABILITY AND EXIT

Configuration, policy, data, state, evidence, workflows, identities, and operational knowledge must be exportable and reconstructable.

DECISION OWNERSHIP

Architecture, security, operations, finance, procurement, legal, data, and service owners jointly accept the final profile, evidence, residual risk, and exit obligations.

RISK AND FAILURE REGISTER

SCENARIOS THAT CAN INVALIDATE A FEATURE-BASED SELECTION

ID	SEVERITY	FAILURE SCENARIO	REQUIRED TREATMENT
R-01	CRITICAL	A polished dashboard conceals incomplete telemetry or weak root-cause accuracy.	PREVENT / DETECT / RECOVER / EVIDENCE
R-02	HIGH	Cloud or management loss removes essential operations without a degraded mode.	PREVENT / DETECT / RECOVER / EVIDENCE
R-03	HIGH	Templates and intent drift from deployed device configuration.	PREVENT / DETECT / RECOVER / EVIDENCE
R-04	HIGH	Automated remediation changes service without sufficient approval or rollback.	PREVENT / DETECT / RECOVER / EVIDENCE
R-05	MEDIUM	Licensing or hardware constraints invalidate the target operating model.	PREVENT / DETECT / RECOVER / EVIDENCE
R-06	MEDIUM	Platform migration breaks inventory, policy, maps, telemetry, historical baselines, and runbooks.	PREVENT / DETECT / RECOVER / EVIDENCE

RISK RULE

A candidate with an unresolved critical failure path cannot advance because optional capability, market position, or commercial discount cannot compensate for missing safety or recovery evidence.

CONTROLLED PROOF-OF-CAPABILITY PLAN

REPEATABLE SCENARIOS, INSTRUMENTATION, AND ACCEPTANCE

TEST 01

Deploy a representative wired and wireless site hierarchy with users, guests, IoT, voice, and critical applications.

TEST 02

Measure discovery, provisioning, configuration compliance, telemetry completeness, and client-assurance accuracy.

TEST 03

Inject DHCP, DNS, RADIUS, RF, roaming, PoE, VLAN, routing, WAN, and certificate failures.

TEST 04

Exercise software upgrade, rollback, device replacement, site outage, and management-plane loss.

TEST 05

Validate API, webhooks, ITSM, source-of-truth, SIEM, and automated-remediation controls.

TEST 06

Compare operator time-to-diagnose and time-to-recover using blinded scenarios.

EVIDENCE PACKAGE

Preserve versions, architecture, configuration, data set, scenario, expected result, instrumentation, raw output, timing, failures, operator actions, deviations, acceptance state, owner, and artifact hashes.

CONDITIONAL RECOMMENDATION AND REVALIDATION

DECISION RECORD, ACCEPTANCE, AND NEXT EVIDENCE

RECOMMENDATION POSITION

- Shortlist by installed estate and target operating model.
- Use identical client and service-failure scenarios in a controlled lab.
- Measure actual operator cognition and recovery time.
- Revalidate quarterly and before major cloud, licensing, appliance, or controller transitions.

CANDIDATE	ADJ. SCORE	GATE POSITION	LAB STATE
Catalyst Center	49.9	PASS - large Cisco campus profile; CONDITIONAL - platform lifecycle and licensing	PENDING
Aruba Central	49.6	PASS - Aruba campus and deployment-flexibility profile; CONDITIONAL - platform-generation parity	PENDING
Mist	48.8	PASS - cloud-native experience-assurance profile; CONDITIONAL - cloud dependency and ecosystem fit	PENDING
Fortinet	48.1	PASS - security-converged branch profile; CONDITIONAL - campus assurance and firmware governance	PENDING

REVALIDATION SCHEDULE

Review no later than 2026-10-24. Review earlier after a major release, commercial change, critical vulnerability, material outage, architecture transition, failed acceptance test, or change to the target workload profile.

SOURCE AUTHORITY AND REVISION

CURRENT EVIDENCE SNAPSHOT AND PUBLICATION HISTORY

SOURCE ID	PUBLISHER	TITLE	CHECKED
NIST-CSF-20	NIST	Cybersecurity Framework 2.0	2026-07-24
NIST-SP800-53	NIST	Security and Privacy Controls for Information Systems and Organizations	2026-07-24
CATALYST-CENTER	Cisco	Cisco Catalyst Center User Guide	2026-07-24
CATALYST-ASSURANCE	Cisco	Cisco Catalyst Assurance User Guide	2026-07-24
ARUBA-CENTRAL	HPE Aruba Networking	HPE Aruba Networking Central Documentation	2026-07-24
ARUBA-VSG	HPE Aruba Networking	Aruba Validated Solution Guides	2026-07-24
MIST-WIRED	HPE Juniper Networking	Juniper Mist Wired Assurance Guide	2026-07-24
FORTI-CAMPUS	Fortinet	FortiManager 8.0 Operations	2026-07-24

SOURCE POSITION

Official documentation and source repositories support the current capability model. Source records preserve publisher, title, URL, purpose, and review date in the machine-readable authority register. Commercial terms, performance, and environment-specific behavior remain unverified until controlled proof.

REVISION HISTORY

1.1.0-candidate / 2026-07-24 - permanent-publication rebuild using the final benchmark system, profile-specific rankings, evidence adjustment, mandatory gates, and controlled PoC requirements.