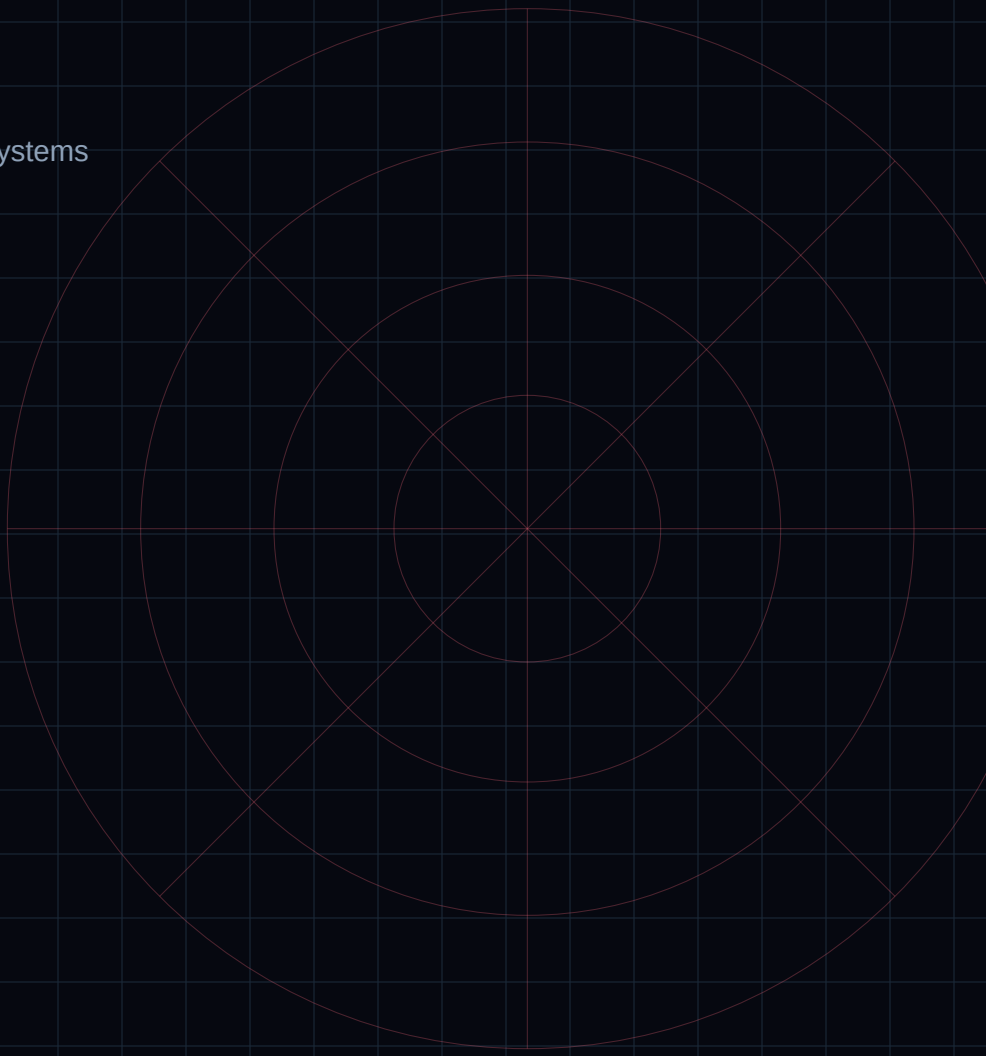
COMPARATIVE EVALUATION / EVIDENCE REFRESH

CMP-002

Enterprise NGFW Platforms

Enterprise firewall and centralized policy systems



CURRENT EVIDENCE SNAPSHOT

Official product sources refreshed through 2026-09-17

Controlled Mythos laboratory rerun: NOT ASSERTED

BENCHMARK DOCTRINE

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

VERSION 1.2.0-candidate

CANDIDATE COMPARATIVE EVALUATION / PUBLIC

Enterprise NGFW Platforms

Enterprise firewall and centralized policy systems

DOCUMENT ID
CMP-002
VERSION
1.2.0-candidate
STATUS
Candidate Comparative Evaluation
PUBLICATION DATE
2026-09-17
SCHEDULED REVIEW
2026-12-16
CANONICAL ROUTE
/library/evaluations/cmp-002/

4
CANDIDATES

18
ATOMIC CRITERIA

9
MANDATORY GATES

3
WORKLOAD PROFILES

E2
CURRENT MAX EVIDENCE

CURRENT DECISION BOUNDARY

No universal NGFW winner is defensible. The July ordering is historical only. Current major-version and management-plane changes require profile-specific policy, HA, upgrade, rollback, logging, automation, and migration proof.

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.

Palo Alto Networks

PAN-OS 12.2 / SCM 3.0

REFRESH TRIGGER

PAN-OS 12.2 and Strata Cloud Manager 3.0 expand management, routing coexistence, audit, and modern TLS/PQC surfaces.

Check Point

R82.10 SC Build 428 / 2026-09-09

REFRESH TRIGGER

R82.10 SmartConsole remains active with current fixes and change-report updates.

Fortinet

FortiOS 7.6.7 / 2026-06-02

REFRESH TRIGGER

7.6.7 adds operational and network features while retaining upgrade/known-issue considerations; 8.0 documentation is also present.

Cisco Secure Firewall

Threat Defense 10.0.2 / 2026-09-15

REFRESH TRIGGER

Version 10 is on a new release numbering/cadence with active 7.x maintenance streams alongside it.

FINAL BENCHMARK SYSTEM / DECISION ARCHITECTURE

01 SCOPE

Freeze decision, candidates, versions and exclusions.

02 GATES

Test non-compensable trust, state, recovery, change and exit.

03 SCORES

Measure atomic capability with approved profile weights.

04 CONFIDENCE

Discount by source grade, freshness, repeatability and relevance.

05 PROOF

Run normal, failure, migration, recovery and operator scenarios.

06 DECISION

Record conditional fit, residual risk, owner and revalidation trigger.

EVIDENCE CONFIDENCE / MODIFIERS

E0	E1	E2	E3	E4	E5
0.00	0.38	0.64	0.78	0.91	1.00
UNSUPPORTED	VENDOR ASSERTION	OFFICIAL SOURCE	MYTHOS LAB	PRODUCTION	INDEPENDENT

THIS EDITION

Current official product and release sources have been refreshed to E2. No E3 controlled Mythos lab rerun is claimed. Therefore current profile rankings remain intentionally unissued until the proof plan is executed.

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.

Palo Alto Networks

PAN-OS 12.2 / SCM 3.0

MATERIAL DELTA

PAN-OS 12.2 and Strata Cloud Manager 3.0 expand management, routing coexistence, audit, and modern TLS/PQC surfaces.

CRITERIA TOUCHED

C02 / C03 / C07 / C11 / C14

MODERATE REVALIDATION

Check Point

R82.10 SC Build 428 / 2026-09-09

MATERIAL DELTA

R82.10 SmartConsole remains active with current fixes and change-report updates.

CRITERIA TOUCHED

C03 / C07 / C11 / C14

MODERATE REVALIDATION

Fortinet

FortiOS 7.6.7 / 2026-06-02

MATERIAL DELTA

7.6.7 adds operational and network features while retaining upgrade/known-issue considerations; 8.0 documentation is also present.

CRITERIA TOUCHED

C01 / C09 / C11 / C14

HIGH REVALIDATION

Cisco Secure Firewall

Threat Defense 10.0.2 / 2026-09-15

MATERIAL DELTA

Version 10 is on a new release numbering/cadence with active 7.x maintenance streams alongside it.

CRITERIA TOUCHED

C01 / C09 / C11 / C14

HIGH REVALIDATION

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	PALO ALTO NETWO	CHECK POINT	FORTINET	CISCO SECURE FI
C01 Functional coverage	E2	E2	RETEST	RETEST
C02 Security / trust	RETEST	E2	E2	E2
C03 Governance / approval	RETEST	RETEST	E2	E2
C04 State integrity	E2	E2	E2	E2
C07 Observability / evidence	RETEST	RETEST	E2	E2
C09 Resilience / continuity	LAB	LAB	RETEST	RETEST
C11 Change safety / rollback	RETEST	RETEST	RETEST	RETEST
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

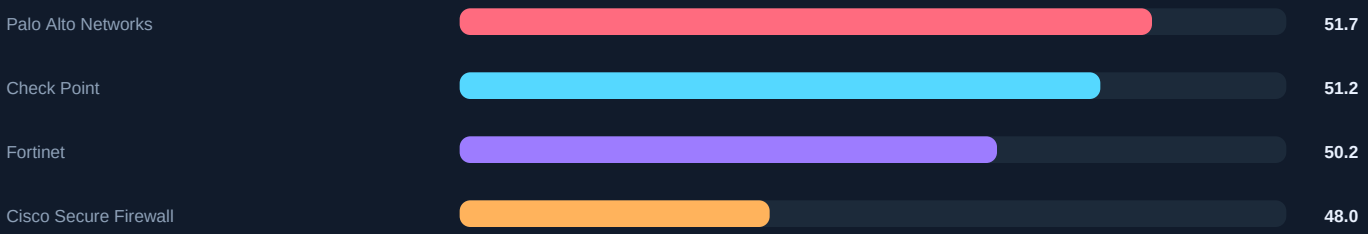
HOLD decision gate remains closed

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.

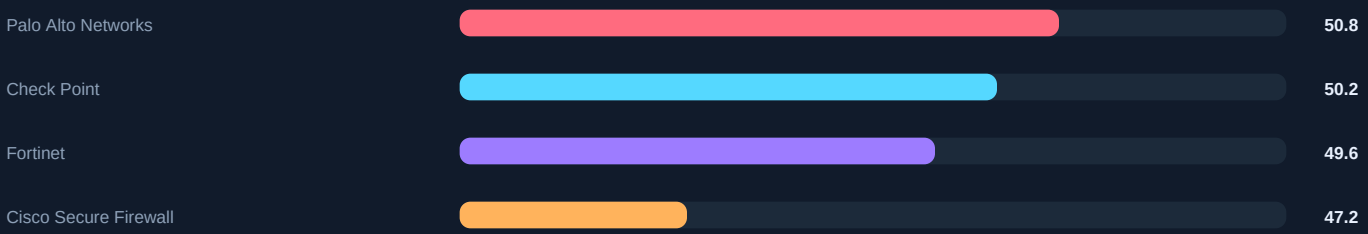
HIGH-ASSURANCE ENTERPRISE SECURITY

BASELINE SPREAD 3.7 PTS



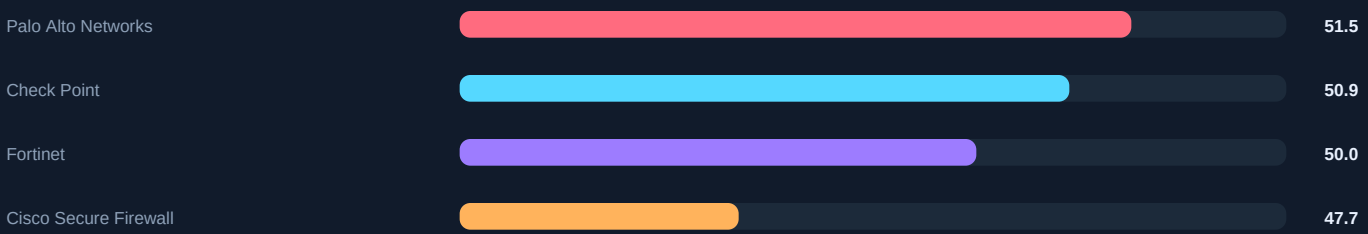
DISTRIBUTED BRANCH AND CAMPUS

BASELINE SPREAD 3.6 PTS



MULTI-DOMAIN SERVICE PROVIDER

BASELINE SPREAD 3.8 PTS



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

Palo Alto Networks — E2 REFRESHED
Historical adjusted confidence: 58.2%
E3 LAB: NOT REPRODUCED

Check Point — E2 REFRESHED
Historical adjusted confidence: 58.2%
E3 LAB: NOT REPRODUCED

Fortinet — E2 REFRESHED
Historical adjusted confidence: 58.2%
E3 LAB: NOT REPRODUCED

Cisco Secure Firewall — 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.

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.

Palo Alto Networks

MODERATE REVALIDATION

PAN-OS 12.2 and Strata Cloud Manager 3.0 expand management, routing coexistence, audit, and modern TLS/PQC surfaces.

RETEST: C02 / C03 / C07 / C11 / C14

Check Point

MODERATE REVALIDATION

R82.10 SmartConsole remains active with current fixes and change-report updates.

RETEST: C03 / C07 / C11 / C14

Fortinet

HIGH REVALIDATION

7.6.7 adds operational and network features while retaining upgrade/known-issue considerations; 8.0 documentation is also present.

RETEST: C01 / C09 / C11 / C14

Cisco Secure Firewall

HIGH REVALIDATION

Version 10 is on a new release numbering/cadence with active 7.x maintenance streams alongside it.

RETEST: C01 / C09 / C11 / 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

Import a representative policy estate and compare rule intent, objects, NAT, VPN, routing, and segmentation.

02

CONTROLLED SCENARIO

Exercise high availability, management loss, log loss, backup, restore, and rollback.

03

CONTROLLED SCENARIO

Measure policy installation, session scale, inspection throughput, and logging under representative traffic.

04

CONTROLLED SCENARIO

Validate API-driven object and policy lifecycle with approval and evidence.

05

CONTROLLED SCENARIO

Test decryption, certificate lifecycle, exception handling, and privacy controls.

06

CONTROLLED SCENARIO

Conduct controlled migration with semantic review and post-cutover validation.

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

No universal NGFW winner is defensible. The July ordering is historical only. Current major-version and management-plane changes require profile-specific policy, HA, upgrade, rollback, logging, automation, and migration proof.

CURRENT RANKING: NOT REISSUED / CONTROLLED LAB REQUIRED

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

Palo Alto Networks	E2 / OFFICIAL	
Palo Alto Networks Aug 2026 new features		docs.paloaltonetworks.com
Check Point	E2 / OFFICIAL	
Check Point R82.10 SmartConsole Build 428		sc1.checkpoint.com
Fortinet	E2 / OFFICIAL	
FortiOS 7.6.7 release notes		docs.fortinet.com
Cisco Secure Firewall	E2 / OFFICIAL	
Cisco Secure Firewall Version 10 release notes		www.cisco.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	Enterprise NGFW and centralized-management coverage	5	YES	Feature documentation, APIs, configuration exports, and scenario demonstration.
C02	Policy, inspection, segmentation, 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	Configuration, object, policy, and log 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	Gateway, tenant, policy, and log 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	Usability and operator 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, sovereign, and disconnected deployment 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	PALO ALTO	CHECK POINT	FORTINET	CISCO
C01 Enterprise NGFW and centralized-management coverage	4.8	4.7	4.6	4.3
C02 Policy, inspection, segmentation, and trust architecture	4.8	4.7	4.5	4.4
C03 Governance and approval controls	4.5	4.7	4.3	4.2
C04 Configuration, object, policy, and log integrity	4.5	4.5	4.3	4.1
C05 Automation and API quality	4.6	4.2	4.5	4.2
C06 Integration ecosystem	4.6	4.3	4.5	4.4
C07 Observability and evidence	4.6	4.5	4.3	4.3
C08 Gateway, tenant, policy, and log scale	4.6	4.5	4.6	4.2
C09 Resilience and continuity	4.5	4.6	4.3	4.2
C10 Usability and operator cognition	4.4	4.2	4.2	4.0
C11 Change safety and rollback	4.5	4.5	4.3	4.1
C12 Extensibility and programmability	4.4	4.1	4.3	3.9
C13 Cloud, on-premises, sovereign, and disconnected deployment options	4.0	4.2	4.4	4.0
C14 Lifecycle and upgrade discipline	4.3	4.2	4.0	3.8
C15 Economics and cost predictability	3.4	3.5	4.2	3.7
C16 Portability and exit	3.7	3.8	3.9	3.6
C17 Vendor and ecosystem risk	3.7	3.8	3.7	3.6
C18 Assurance confidence	3.6	3.6	3.5	3.4

WEIGHTED BASELINE / 100

Palo Alto	Check Point	Fortinet	Cisco
86.8	85.9	85.0	80.8

EVIDENCE-ADJUSTED SCORECARD

CAPABILITY DISCOUNTED BY CURRENT EVIDENCE CONFIDENCE

CANDIDATE	RAW	EVIDENCE CONFIDENCE	ADJUSTED	CURRENT STATE
Palo Alto	86.8	58.2%	51.2	CONTROLLED LAB PENDING
Check Point	85.9	58.2%	50.6	CONTROLLED LAB PENDING
Fortinet	85.0	58.2%	49.9	CONTROLLED LAB PENDING
Cisco	80.8	58.2%	47.5	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

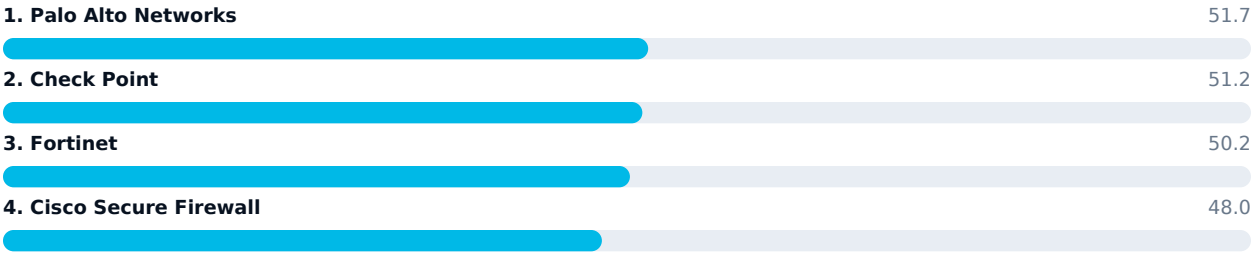
Most candidate criteria are supported at E2: official documentation or source evidence. Environment-specific laboratory, production, and independent evidence remain future gates.

PROFILE-SPECIFIC RANKINGS

EVIDENCE-ADJUSTED SENSITIVITY ANALYSIS

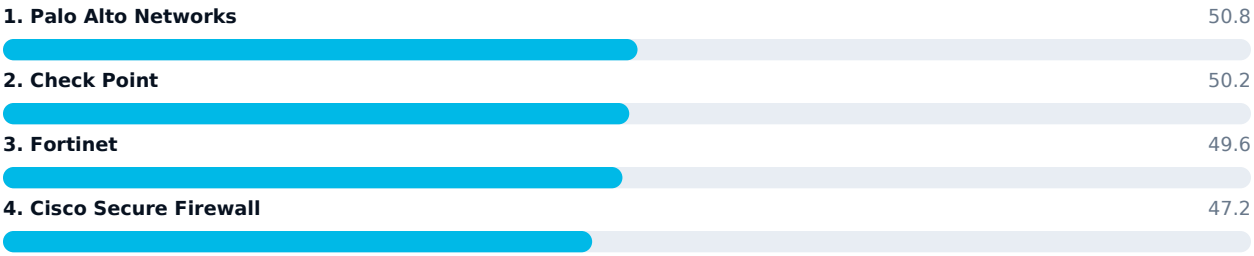
HIGH-ASSURANCE ENTERPRISE SECURITY

Prioritizes inspection depth, policy governance, segmentation, audit, resilience, and controlled change.



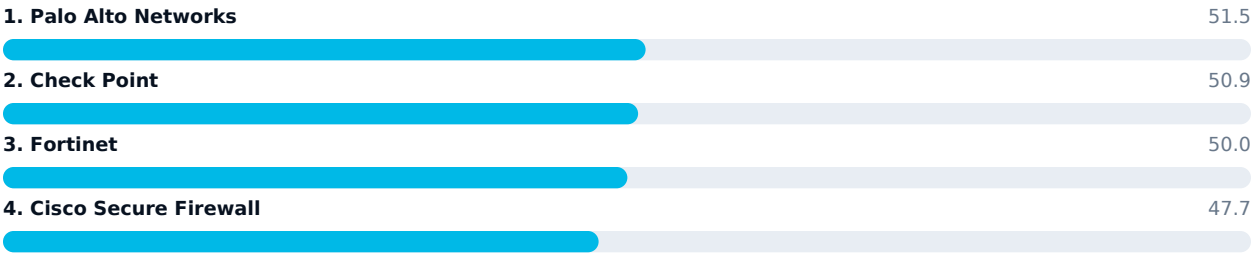
DISTRIBUTED BRANCH AND CAMPUS

Prioritizes appliance breadth, centralized operations, SD-WAN adjacency, economics, and remote lifecycle.



MULTI-DOMAIN SERVICE PROVIDER

Prioritizes delegation, tenancy, scale, policy isolation, automation, evidence, and lifecycle governance.



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

PALO ALTO NETWORKS

OPERATING MODEL

Application- and identity-aware NGFW ecosystem with Panorama and Strata Cloud Manager management paths.

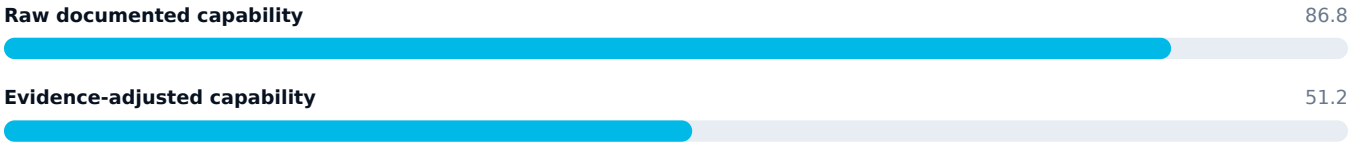
DOCUMENTED STRENGTHS

- Rich application, threat-prevention, decryption, and policy capabilities.
- Strong centralized management and cloud-delivered evolution.
- Broad automation, telemetry, and ecosystem integration.
- Mature enterprise operating patterns.

CAUTIONS AND PROOF OBLIGATIONS

- Commercial complexity and feature licensing require careful modeling.
- Panorama and cloud-management trajectories require explicit architecture decisions.
- Policy quality still depends on disciplined objects, ownership, and cleanup.

BASELINE SCORE PROFILE



GATE DISPOSITION

PASS - high-assurance enterprise profile | CONDITIONAL - commercial and management-path validation

CANDIDATE DEEP DIVE / 02

CHECK POINT

OPERATING MODEL

Management-centric security architecture with SmartConsole, Security Management, MDSM, gateways, and software blades.

DOCUMENTED STRENGTHS

- Deep centralized policy and object management.
- Strong multi-domain and delegated-management patterns.
- Mature clustering, logging, and enterprise control-plane architecture.
- Granular rulebase and security-blade integration.

CAUTIONS AND PROOF OBLIGATIONS

- Operational expertise is specialized and upgrades require careful planning.
- Architecture can become complex across domains, gateways, and management layers.
- Automation and cloud-management fit must be validated for each workflow.

BASELINE SCORE PROFILE

Raw documented capability 85.9

Evidence-adjusted capability 50.6

GATE DISPOSITION

PASS - management-centric and multi-domain profile | CONDITIONAL - specialized operational capability required

CANDIDATE DEEP DIVE / 03

FORTINET

OPERATING MODEL

Security Fabric ecosystem with FortiGate gateways and FortiManager-centered centralized operations.

DOCUMENTED STRENGTHS

- Broad appliance and platform coverage.
- Strong price-performance potential and integrated Security Fabric.
- Central management and automation options across the estate.
- Flexible branch, campus, datacenter, and service-provider deployment.

CAUTIONS AND PROOF OBLIGATIONS

- Feature and licensing boundaries require precise validation.
- Cross-product integration can increase ecosystem coupling.
- Operational consistency depends on firmware and management discipline.

BASELINE SCORE PROFILE

Raw documented capability 85.0

Evidence-adjusted capability 49.9

GATE DISPOSITION

PASS - distributed and value-sensitive profile | CONDITIONAL - firmware and ecosystem coupling controls

CANDIDATE DEEP DIVE / 04

CISCO SECURE FIREWALL

OPERATING MODEL

Secure Firewall Threat Defense managed through Firewall Management Center and integrated with the Cisco security ecosystem.

DOCUMENTED STRENGTHS

- Strong fit for Cisco-heavy enterprises and integrated security telemetry.
- Central management, policy, health, and migration tooling.
- Broad enterprise support and hardware options.
- Potential consolidation with existing Cisco identity and security investments.

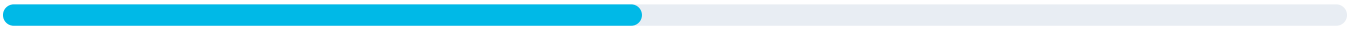
CAUTIONS AND PROOF OBLIGATIONS

- Operational experience and feature behavior must be validated carefully.
- Migration from ASA or other platforms can expose policy translation gaps.
- Management and release complexity require strict lab qualification.

BASELINE SCORE PROFILE

Raw documented capability 80.8

Evidence-adjusted capability 47.5



GATE DISPOSITION

CONDITIONAL - Cisco-aligned estate | CONTROLLED POC REQUIRED - migration and operations

ARCHITECTURE AND INTEGRATION FIT

THE PRODUCT IS ONLY ONE PART OF THE OPERATING SYSTEM

REFERENCE OPERATING LAYERS

01 Central management and policy authority

02 Gateway and inspection enforcement plane

03 Identity, endpoint, cloud, and threat-intelligence integrations

04 Logging, analytics, and evidence plane

05 Change, upgrade, backup, and recovery control system

INTEGRATION BOUNDARIES

- Identity and NAC
- SIEM, SOAR, and data lake
- Endpoint and cloud security
- DNS, DHCP, IPAM, and certificate services
- ITSM, Git, CI/CD, and automation
- SASE and remote-access services

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	Feature scores conceal mandatory policy or recovery failures.	PREVENT / DETECT / RECOVER / EVIDENCE
R-02	HIGH	Licensing assumptions make the preferred architecture economically invalid.	PREVENT / DETECT / RECOVER / EVIDENCE
R-03	HIGH	Management failure or compromise creates estate-wide exposure.	PREVENT / DETECT / RECOVER / EVIDENCE
R-04	HIGH	Decryption deployment causes application outage or privacy violations.	PREVENT / DETECT / RECOVER / EVIDENCE
R-05	MEDIUM	Upgrade paths are accepted without representative HA, VPN, routing, and policy tests.	PREVENT / DETECT / RECOVER / EVIDENCE
R-06	MEDIUM	Migration tools translate syntax but not intent, exceptions, or operational knowledge.	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

Import a representative policy estate and compare rule intent, objects, NAT, VPN, routing, and segmentation.

TEST 02

Exercise high availability, management loss, log loss, backup, restore, and rollback.

TEST 03

Measure policy installation, session scale, inspection throughput, and logging under representative traffic.

TEST 04

Validate API-driven object and policy lifecycle with approval and evidence.

TEST 05

Test decryption, certificate lifecycle, exception handling, and privacy controls.

TEST 06

Conduct controlled migration with semantic review and post-cutover validation.

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

- Use profile-specific shortlists rather than a universal rank.
- Require a production-representative firewall lab and migration rehearsal.
- Model five-year license, support, staffing, logging, and hardware costs.
- Revalidate quarterly and before any major release or management-plane transition.

CANDIDATE	ADJ. SCORE	GATE POSITION	LAB STATE
Palo Alto	51.2	PASS - high-assurance enterprise profile; CONDITIONAL - commercial and management-path validation	PENDING
Check Point	50.6	PASS - management-centric and multi-domain profile; CONDITIONAL - specialized operational capability required	PENDING
Fortinet	49.9	PASS - distributed and value-sensitive profile; CONDITIONAL - firmware and ecosystem coupling controls	PENDING
Cisco	47.5	CONDITIONAL - Cisco-aligned estate; CONTROLLED POC REQUIRED - migration and operations	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
CIS-CONTROLS	Center for Internet Security	CIS Critical Security Controls v8.1	2026-07-24
PAN-SCM	Palo Alto Networks	Strata Cloud Manager Documentation	2026-07-24
PAN-PANORAMA	Palo Alto Networks	Panorama Administrator Documentation	2026-07-24
CP-R82-MGMT	Check Point	R82 Security Management Administration Guide	2026-07-24
CP-R82-MDSM	Check Point	R82 Multi-Domain Security Management Guide	2026-07-24
FORTIMANAGER	Fortinet	FortiManager 8.0 Documentation	2026-07-24
CISCO-FMC	Cisco	Cisco Secure Firewall Management Center Administration Guide	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.