

**CMP-005**

# Modern Private Networking

Overlay networks, identity-aware access and private application fabrics



## 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.

# Modern Private Networking

Overlay networks, identity-aware access and private application fabrics

DOCUMENT ID

CMP-005

VERSION

1.2.0-candidate

STATUS

Candidate Comparative Evaluation

PUBLICATION DATE

2026-09-17

SCHEDULED REVIEW

2026-12-16

CANONICAL ROUTE

/library/evaluations/cmp-005/

4

CANDIDATES

9

MANDATORY GATES

E2

CURRENT MAX EVIDENCE

18

ATOMIC CRITERIA

3

WORKLOAD PROFILES

CURRENT DECISION BOUNDARY

No universal private-networking winner. The products continue to optimize different authority, hosting, access, and routing models. Reproduce identity, relay, route convergence, self-host, outage, export, and migration behavior for the target profile.

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.

Tailscale

v1.102.4 / 2026-09-10

REFRESH TRIGGER

Client and Kubernetes-operator work continues to improve connectivity, scale, IPv6, and multi-cluster operations.

NetBird

v0.78.2 / 2026-09-14

REFRESH TRIGGER

Rapid self-hosted and policy-management evolution keeps sovereignty attractive but increases upgrade/revalidation importance.

Cloudflare One

Cloud service updates through 2026-09-15

REFRESH TRIGGER

Tagged infrastructure targets, fresh-auth controls, DLP discovery, and route-management improvements broaden the access fabric.

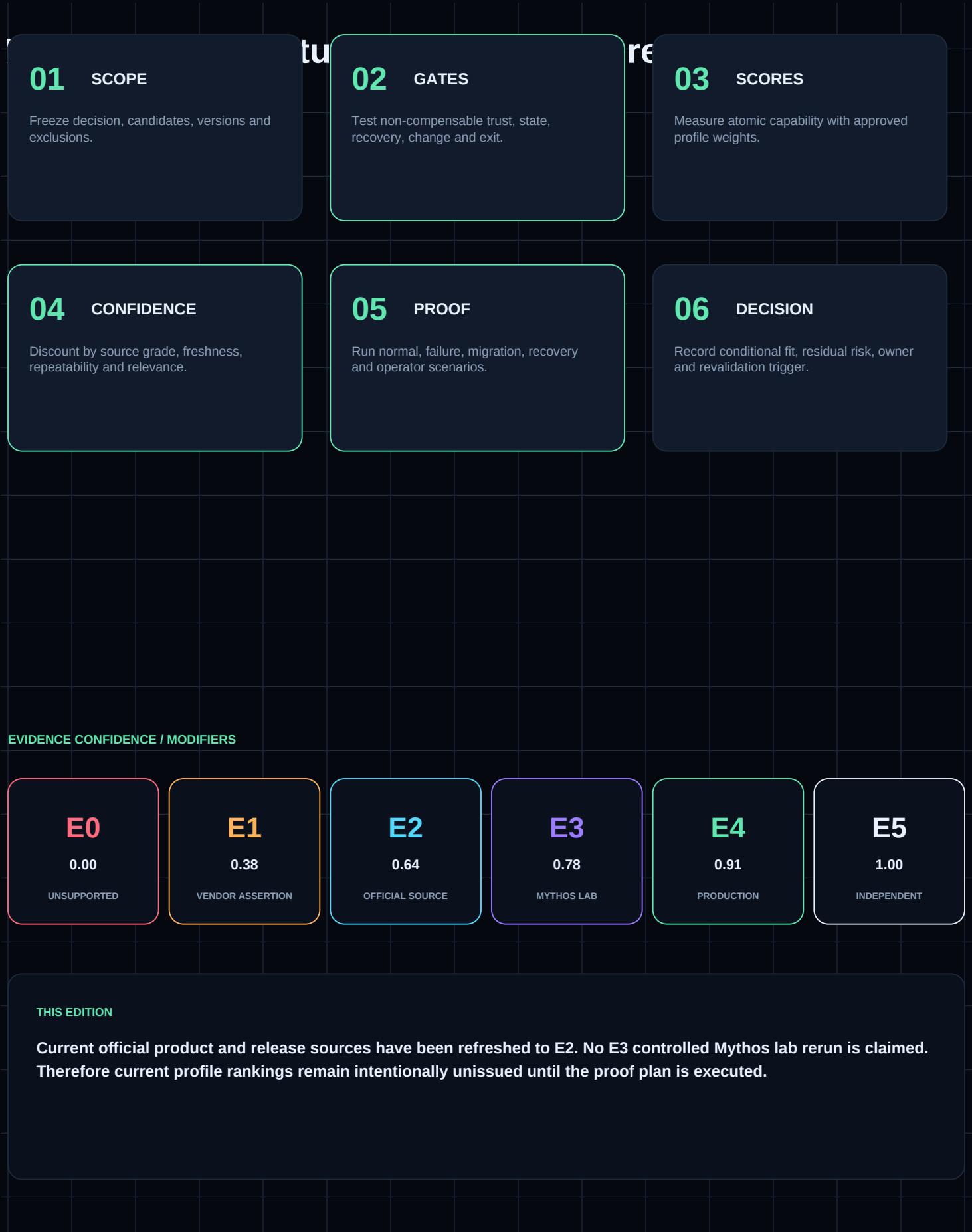
ZeroTier

ZeroTier One 1.16.2 / New Central Jun 2026

REFRESH TRIGGER

New Central API v2, webhooks and full custom Flow Rules materially strengthen automation and policy management.

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.

|                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div><div>Tailscale</div><div>v1.102.4 / 2026-09-10</div><div>MATERIAL DELTA</div><div>Client and Kubernetes-operator work continues to improve connectivity, scale, IPv6, and multi-cluster operations.</div><div>CRITERIA TOUCHED</div><div>C01 / C07 / C08 / C09 / C14</div><div>LOW REVALIDATION</div></div>                                                  | <div><div>NetBird</div><div>v0.78.2 / 2026-09-14</div><div>MATERIAL DELTA</div><div>Rapid self-hosted and policy-management evolution keeps sovereignty attractive but increases upgrade/revalidation importance.</div><div>CRITERIA TOUCHED</div><div>C01 / C03 / C05 / C13 / C14 / C16</div><div>MODERATE REVALIDATION</div></div>          |
| <div><div>Cloudflare One</div><div>Cloud service updates through 2026-09-15</div><div>MATERIAL DELTA</div><div>Tagged infrastructure targets, fresh-auth controls, DLP discovery, and route-management improvements broaden the access fabric.</div><div>CRITERIA TOUCHED</div><div>C01 / C02 / C03 / C05 / C07 / C14</div><div>MODERATE REVALIDATION</div></div> | <div><div>ZeroTier</div><div>ZeroTier One 1.16.2 / New Central Jun 2026</div><div>MATERIAL DELTA</div><div>New Central API v2, webhooks and full custom Flow Rules materially strengthen automation and policy management.</div><div>CRITERIA TOUCHED</div><div>C01 / C03 / C05 / C07 / C12 / C14</div><div>MODERATE REVALIDATION</div></div> |

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               | TAILSCALE | NETBIRD | CLOUDFLARE ONE | ZEROTIER |
|------------------------------|-----------|---------|----------------|----------|
| C01 Functional coverage      | RETEST    | RETEST  | RETEST         | RETEST   |
| C02 Security / trust         | E2        | E2      | RETEST         | E2       |
| C03 Governance / approval    | E2        | RETEST  | RETEST         | RETEST   |
| C04 State integrity          | E2        | E2      | E2             | E2       |
| C07 Observability / evidence | RETEST    | E2      | RETEST         | RETEST   |
| C09 Resilience / continuity  | RETEST    | LAB     | LAB            | LAB      |
| C11 Change safety / rollback | LAB       | LAB     | LAB            | LAB      |
| C16 Portability / exit       | LAB       | RETEST  | 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

Tailscale

E2 REFRESHED

Historical adjusted confidence: 58.2%

E3 LAB: NOT REPRODUCED

NetBird

E2 REFRESHED

Historical adjusted confidence: 58.2%

E3 LAB: NOT REPRODUCED

Cloudflare One

E2 REFRESHED

Historical adjusted confidence: 58.2%

E3 LAB: NOT REPRODUCED

ZeroTier

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.

|                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div><div>Tailscale</div><div>LOW REVALIDATION</div><div>Client and Kubernetes-operator work continues to improve connectivity, scale, IPv6, and multi-cluster operations.</div><div>RETEST: C01 / C07 / C08 / C09 / C14</div></div>                               |
| <div><div>NetBird</div><div>MODERATE REVALIDATION</div><div>Rapid self-hosted and policy-management evolution keeps sovereignty attractive but increases upgrade/revalidation importance.</div><div>RETEST: C01 / C03 / C05 / C13 / C14 / C16</div></div>          |
| <div><div>Cloudflare One</div><div>MODERATE REVALIDATION</div><div>Tagged infrastructure targets, fresh-auth controls, DLP discovery, and route-management improvements broaden the access fabric.</div><div>RETEST: C01 / C02 / C03 / C05 / C07 / C14</div></div> |
| <div><div>ZeroTier</div><div>MODERATE REVALIDATION</div><div>New Central API v2, webhooks and full custom Flow Rules materially strengthen automation and policy management.</div><div>RETEST: C01 / C03 / C05 / C07 / C12 / C14</div></div>                       |

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

Connect workforce endpoints, servers, containers, mobile devices, sites, and overlapping networks.

02

CONTROLLED SCENARIO

Test direct, relayed, site-to-site, subnet-router, exit-node, application, SSH, and DNS flows.

03

CONTROLLED SCENARIO

Exercise identity outage, relay loss, controller loss, route conflict, key rotation, and revoked-device behavior.

04

CONTROLLED SCENARIO

Measure connection establishment, throughput, latency, roaming, and recovery.

05

CONTROLLED SCENARIO

Validate policy-as-code, posture, logging, API, and incident response.

06

CONTROLLED SCENARIO

Export or reconstruct all routes, policies, devices, identities, and operational evidence.

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 private-networking winner. The products continue to optimize different authority, hosting, access, and routing models. Reproduce identity, relay, route convergence, self-host, outage, export, and migration behavior for the target profile.

CURRENT RANKING: NOT REISSUED / CONTROLLED LAB REQUIRED

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

|                     |               |               |
|---------------------|---------------|---------------|
| Tailscale           | E2 / OFFICIAL |               |
| Tailscale changelog |               | tailscale.com |

|                                    |               |                 |
|------------------------------------|---------------|-----------------|
| NetBird                            | E2 / OFFICIAL |                 |
| NetBird documentation and releases |               | docs.netbird.io |

|                          |               |                           |
|--------------------------|---------------|---------------------------|
| Cloudflare One           | E2 / OFFICIAL |                           |
| Cloudflare One changelog |               | developers.cloudflare.com |

|                    |               |                   |
|--------------------|---------------|-------------------|
| ZeroTier           | E2 / OFFICIAL |                   |
| ZeroTier changelog |               | docs.zerotier.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 | Identity-aware private networking and application-access coverage    | 5      | YES  | Feature documentation, APIs, configuration exports, and scenario demonstration.                  |
| C02 | Peer identity, key management, policy, relay, 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 | Identity, device, route, policy, and key-state 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 | Peer, route, site, policy, and relay 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 | SaaS, self-hosted, hybrid, and sovereign control-plane 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                                                                | TAILSCALE | NETBIRD | CLOUDFLARE | ZEROTIER |
|--------------------------------------------------------------------------|-----------|---------|------------|----------|
| C01 Identity-aware private networking and application-access coverage    | 4.7       | 4.4     | 4.5        | 4.3      |
| C02 Peer identity, key management, policy, relay, and trust architecture | 4.6       | 4.4     | 4.6        | 4.1      |
| C03 Governance and approval controls                                     | 4.4       | 4.1     | 4.4        | 3.9      |
| C04 Identity, device, route, policy, and key-state integrity             | 4.3       | 4.2     | 4.2        | 4.2      |
| C05 Automation and API quality                                           | 4.7       | 4.4     | 4.6        | 4.2      |
| C06 Integration ecosystem                                                | 4.5       | 4.2     | 4.8        | 4.0      |
| C07 Observability and evidence                                           | 4.4       | 4.1     | 4.5        | 4.0      |
| C08 Peer, route, site, policy, and relay scale                           | 4.5       | 4.0     | 4.7        | 4.3      |
| C09 Resilience and continuity                                            | 4.3       | 4.0     | 4.5        | 4.1      |
| C10 Usability and operator cognition                                     | 4.8       | 4.4     | 4.5        | 3.8      |
| C11 Change safety and rollback                                           | 4.3       | 4.2     | 4.2        | 4.1      |
| C12 Extensibility and programmability                                    | 4.2       | 4.3     | 4.0        | 4.2      |
| C13 SaaS, self-hosted, hybrid, and sovereign control-plane options       | 3.0       | 4.9     | 2.8        | 4.7      |
| C14 Lifecycle and upgrade discipline                                     | 4.4       | 4.0     | 4.3        | 3.9      |
| C15 Economics and cost predictability                                    | 4.0       | 4.4     | 3.6        | 4.4      |
| C16 Portability and exit                                                 | 3.7       | 4.6     | 3.2        | 4.5      |
| C17 Vendor and ecosystem risk                                            | 3.8       | 4.0     | 3.4        | 3.8      |
| C18 Assurance confidence                                                 | 3.6       | 3.4     | 3.5        | 3.4      |

### WEIGHTED BASELINE / 100

**Tailscale**
**85.2**
**NetBird**
**84.0**
**Cloudflare**
**83.5**
**ZeroTier**
**81.8**

# EVIDENCE-ADJUSTED SCORECARD

## CAPABILITY DISCOUNTED BY CURRENT EVIDENCE CONFIDENCE

| CANDIDATE  | RAW  | EVIDENCE CONFIDENCE | ADJUSTED | CURRENT STATE          |
|------------|------|---------------------|----------|------------------------|
| Tailscale  | 85.2 | 58.2%               | 50.1     | CONTROLLED LAB PENDING |
| NetBird    | 84.0 | 58.2%               | 49.4     | CONTROLLED LAB PENDING |
| Cloudflare | 83.5 | 58.2%               | 49.0     | CONTROLLED LAB PENDING |
| ZeroTier   | 81.8 | 58.2%               | 48.0     | 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

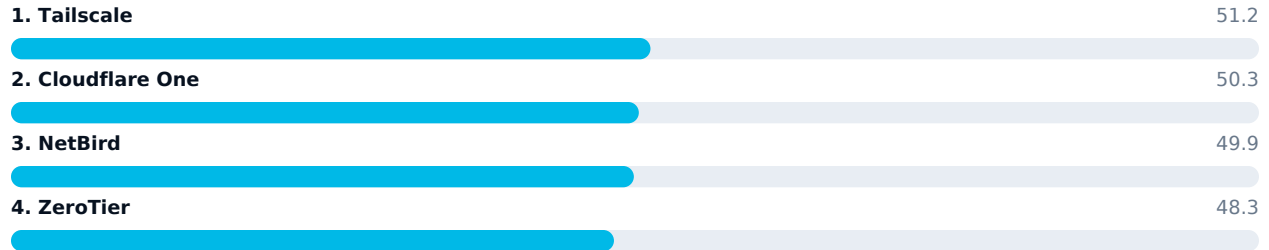
Most candidate criteria are supported at E2: official documentation or source evidence. Environment-specific laboratory, production, and independent evidence remain future gates.

# PROFILE-SPECIFIC RANKINGS

## EVIDENCE-ADJUSTED SENSITIVITY ANALYSIS

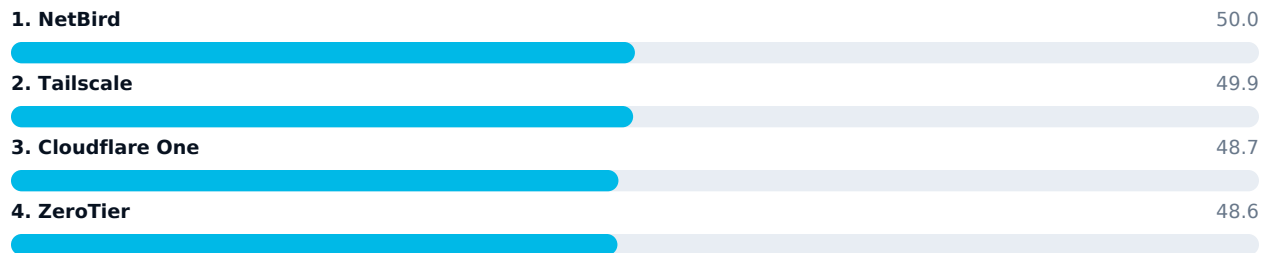
### IDENTITY-AWARE WORKFORCE ACCESS

Prioritizes user experience, identity policy, posture, application access, audit, and rapid deployment.



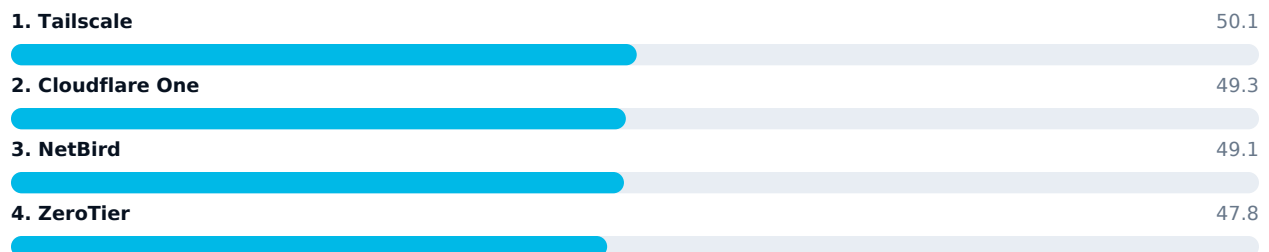
### SOVEREIGN PRIVATE NETWORK

Prioritizes self-hosting, key and route control, exportability, offline tolerance, and reduced external dependency.



### MULTI-SITE APPLICATION AND NETWORK FABRIC

Prioritizes sites, routes, application publishing, relay performance, global operations, and policy.



#### 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

## TAILSCALE

### OPERATING MODEL

Managed WireGuard-based tailnet with identity integration, grants, device posture, routing, and application-layer access extensions.

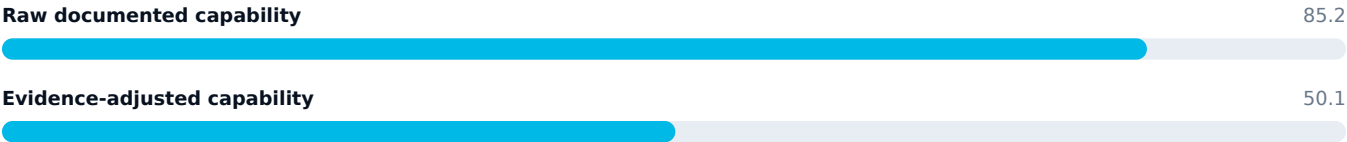
### DOCUMENTED STRENGTHS

- Excellent operator and end-user experience.
- Strong identity-aware policy and modern grants model.
- Broad endpoint support and rapid deployment.
- Mature managed coordination and operational simplicity.

### CAUTIONS AND PROOF OBLIGATIONS

- Managed control-plane dependency is material.
- Advanced routing and application patterns require careful architecture.
- Sovereignty and full exit requirements must be validated explicitly.

### BASELINE SCORE PROFILE



### GATE DISPOSITION

PASS - workforce and rapid-deployment profile | CONDITIONAL - control-plane and exit boundaries

# CANDIDATE DEEP DIVE / 02

## NETBIRD

### OPERATING MODEL

WireGuard-based private-network platform available as managed SaaS or self-hosted control plane with groups, policies, posture, routes, and relays.

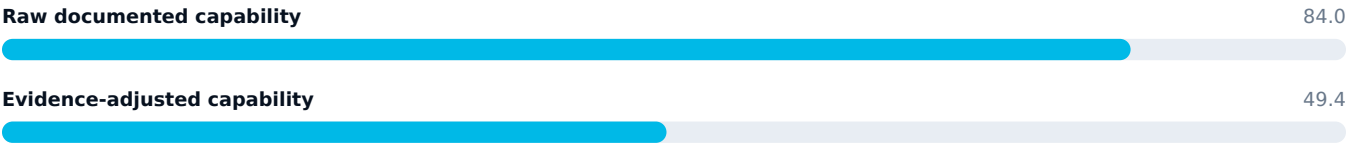
### DOCUMENTED STRENGTHS

- Self-hosted and managed deployment options.
- Identity-aware access policies and posture checks.
- Open-source transparency and growing integration surface.
- Strong fit for sovereign or hybrid operating models.

### CAUTIONS AND PROOF OBLIGATIONS

- Self-hosting transfers reliability and security responsibility to the operator.
- Ecosystem maturity and scale must be proven for large estates.
- Upgrade, relay, identity, and database operations require disciplined ownership.

### BASELINE SCORE PROFILE



### GATE DISPOSITION

PASS - sovereign and hybrid profile | CONDITIONAL - self-hosted operations and scale

# CANDIDATE DEEP DIVE / 03

## CLOUDFLARE ONE

### OPERATING MODEL

Cloud-delivered connectivity and access platform using Tunnel, Mesh, Access, global network services, and policy.

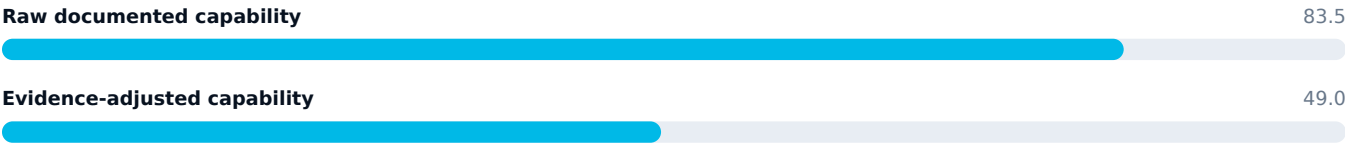
### DOCUMENTED STRENGTHS

- Strong application publishing and identity-aware access.
- Global network and managed connector operations.
- Outbound-only tunnel model reduces inbound exposure.
- Converges application, private-network, and broader security services.

### CAUTIONS AND PROOF OBLIGATIONS

- Cloudflare dependency and service coupling are significant.
- Peer-mesh and site-routing requirements must be tested carefully.
- Exit, routing behavior, logging, and pricing require profile-specific validation.

### BASELINE SCORE PROFILE



### GATE DISPOSITION

PASS - application access and global managed fabric | CONDITIONAL - platform coupling and route behavior

# CANDIDATE DEEP DIVE / 04

## ZEROTIER

### OPERATING MODEL

Virtual Ethernet networking platform with controllers, roots, distributed rules engine, routing, bridging, and enterprise deployment options.

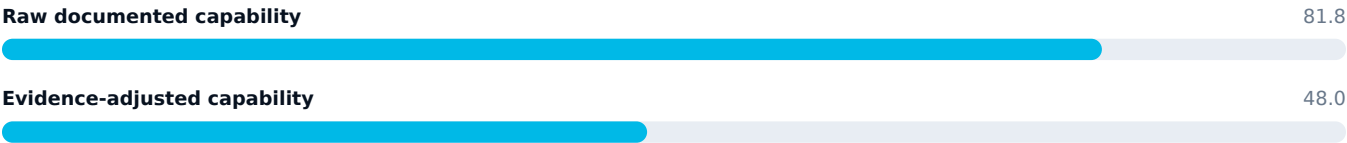
### DOCUMENTED STRENGTHS

- Layer-2 and Layer-3 virtual networking flexibility.
- Distributed rules engine and network virtualization model.
- Self-hosting and private-root options support sovereignty.
- Useful for complex device, site, lab, and embedded networking.

### CAUTIONS AND PROOF OBLIGATIONS

- Identity-aware application access is less turnkey.
- Operational model and troubleshooting can be more network-centric.
- Policy, controller, and route design require specialized engineering.

### BASELINE SCORE PROFILE



### GATE DISPOSITION

PASS - virtual network and sovereign network profile | CONDITIONAL - identity and operational model

# ARCHITECTURE AND INTEGRATION FIT

## THE PRODUCT IS ONLY ONE PART OF THE OPERATING SYSTEM

### REFERENCE OPERATING LAYERS

**01** Identity, device enrollment, and key authority

**02** Coordination, discovery, relay, and routing control plane

**03** Peer or connector data plane

**04** Policy, posture, application access, and segmentation

**05** Telemetry, evidence, lifecycle, recovery, and exit

### INTEGRATION BOUNDARIES

- Identity providers and device management
- DNS and service discovery
- Endpoint security and posture
- Cloud, datacenter, branch, home, lab, and embedded networks
- SIEM, ITSM, and automation
- Application proxies, SSH, RDP, database, and web 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 | A proof of connectivity is mistaken for proof of policy, resilience, and operations.      | PREVENT / DETECT / RECOVER / EVIDENCE |
| R-02 | HIGH     | Relay dependence or route asymmetry causes hidden latency and failure.                    | PREVENT / DETECT / RECOVER / EVIDENCE |
| R-03 | HIGH     | Identity or posture outages lock out critical operations.                                 | PREVENT / DETECT / RECOVER / EVIDENCE |
| R-04 | HIGH     | Self-hosted control planes are deployed without HA, patching, backup, and monitoring.     | PREVENT / DETECT / RECOVER / EVIDENCE |
| R-05 | MEDIUM   | Application publishing bypasses segmentation or origin hardening.                         | PREVENT / DETECT / RECOVER / EVIDENCE |
| R-06 | MEDIUM   | Exit testing reveals that device, route, policy, and key state cannot be migrated safely. | 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

Connect workforce endpoints, servers, containers, mobile devices, sites, and overlapping networks.

### TEST 02

Test direct, relayed, site-to-site, subnet-router, exit-node, application, SSH, and DNS flows.

### TEST 03

Exercise identity outage, relay loss, controller loss, route conflict, key rotation, and revoked-device behavior.

### TEST 04

Measure connection establishment, throughput, latency, roaming, and recovery.

### TEST 05

Validate policy-as-code, posture, logging, API, and incident response.

### TEST 06

Export or reconstruct all routes, policies, devices, identities, and operational evidence.

### 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

- Choose the dominant access pattern before ranking candidates.
- Test direct and relayed behavior from representative geographies and restricted networks.
- Treat identity, DNS, relay, and control-plane failure as mandatory scenarios.
- Revalidate quarterly and after material routing, policy, or pricing changes.

| CANDIDATE  | ADJ. SCORE | GATE POSITION                                                                                           | LAB STATE |
|------------|------------|---------------------------------------------------------------------------------------------------------|-----------|
| Tailscale  | 50.1       | PASS - workforce and rapid-deployment profile; CONDITIONAL - control-plane and exit boundaries          | PENDING   |
| NetBird    | 49.4       | PASS - sovereign and hybrid profile; CONDITIONAL - self-hosted operations and scale                     | PENDING   |
| Cloudflare | 49.0       | PASS - application access and global managed fabric; CONDITIONAL - platform coupling and route behavior | PENDING   |
| ZeroTier   | 48.0       | PASS - virtual network and sovereign network profile; CONDITIONAL - identity and operational model      | 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 |
| TAILSCALE-GRANTS  | Tailscale  | Tailscale Grants                                                        | 2026-07-24 |
| TAILSCALE-POLICY  | Tailscale  | Tailnet Policy File Syntax                                              | 2026-07-24 |
| NETBIRD-ACCESS    | NetBird    | NetBird Access Control                                                  | 2026-07-24 |
| NETBIRD-SELFHOST  | NetBird    | NetBird Self-Hosting Guide                                              | 2026-07-24 |
| CLOUDFLARE-TUNNEL | Cloudflare | Cloudflare Tunnel Documentation                                         | 2026-07-24 |
| CLOUDFLARE-MESH   | Cloudflare | Cloudflare Mesh Routes                                                  | 2026-07-24 |
| ZEROTIER          | ZeroTier   | ZeroTier Enterprise Deployment Guide                                    | 2026-07-24 |
| ZEROTIER-RULES    | ZeroTier   | ZeroTier Rules Engine                                                   | 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.