



CUSTOMER RESOURCE

How TOPO ONE Works

A customer guide to authorized, evidence-backed cybersecurity analysis

Topology (TOPO) One is a RECON ONE cybersecurity analysis capability that transforms authorized network evidence into evidence-backed analysis of IT and OT environments. TOPO ONE helps identify assets and communications, potentially relevant vulnerabilities, configuration and security-policy concerns, network relationships and reachability, and potential attack paths - connecting findings to the evidence needed to understand what matters and why.

For security leaders, engineers, vulnerability-management teams, network and OT practitioners, infrastructure operators, school districts, critical infrastructure organizations, and procurement or security reviewers.

At a glance

COMMERCIAL ROLE

TOPO ONE by RECON ONE is a proprietary, analyst-operated capability used within scoped Vulnerability & Architecture Reviews and related assessments.

EVIDENCE BOUNDARY

Analysis uses customer-provided or otherwise authorized network evidence and approved technical context.

ANALYTICAL APPROACH

Observed evidence is kept distinct from inference, assumptions, constraints, and unresolved questions.

DELIVERY MODEL

TOPO ONE is not a self-service SaaS platform or public upload portal; scope and deliverables are defined for each engagement.

What TOPO ONE is

TOPO ONE is a proprietary RECON ONE cybersecurity analysis capability. RECON ONE analysts use it within scoped Vulnerability & Architecture Reviews and related assessments to connect network evidence with architecture, vulnerability, configuration, policy, reachability, and potential attack-path context.

Its current commercial role is analyst-operated assessment support. It is not presented as an independently purchased software product, a public upload service, or a self-service subscription platform. Human review remains part of the assessment and reporting process.

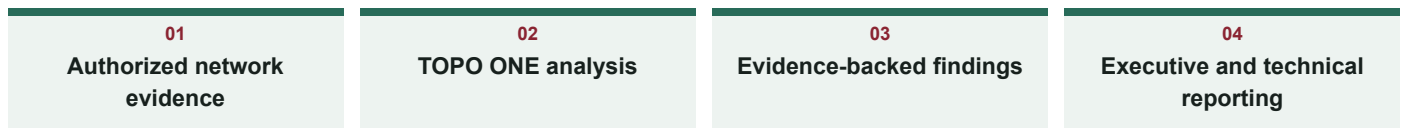
What evidence TOPO ONE analyzes

TOPO ONE can analyze authorized packet captures, including PCAP and PCAPNG, together with approved technical context when it is available. The evidence must be supplied by the customer or otherwise collected and provided under appropriate authorization.

Related context can help analysts interpret what the network evidence means. Its availability and quality affect the conclusions that can be supported.

- Captured network traffic from an agreed observation point and time period
- Architecture or network diagrams
- Asset or service inventories
- Approved site-policy, zone, or conduit assertions
- Relevant product, service, configuration, or vulnerability context
- Scope, authorization, handling, and retention requirements

The customer-facing analysis flow



Context connected during analysis



Passive analysis

TOPO ONE primarily derives insight from captured network evidence without requiring TOPO ONE itself to actively probe, exploit, or modify production systems. This can be useful where uptime, safety, fragile equipment, or change-control requirements make intrusive techniques undesirable, particularly in OT environments.

Passive does not mean complete or universally risk-free. Visibility depends on capture location, duration, traffic activity, encryption, network address translation, and the context supplied. Dormant systems and unobserved communications may not appear.

Understanding the environment

TOPO ONE helps characterize the environment represented by the available evidence. It can identify capture-visible endpoints, internal and external relationships, observed communications, services, protocols, and passive identity indicators. It can also support analysis of architecture, segmentation, IT/OT relationships, and communication boundaries.

The language matters: an item may be observed directly, inferred from supporting evidence, supplied by the customer, or left unresolved. A capture-derived view is not automatically a complete physical inventory or an authoritative CMDB.

- Observed assets, endpoints, services, protocols, and communication patterns
- Internal, external, multicast, and other group relationships visible in the evidence
- Product, platform, or role indicators supported by passive evidence
- Logical network relationships, segments, zones, conduits, and boundaries
- Evidence gaps, contradictions, and areas requiring customer or analyst validation

Vulnerability analysis in environment context

When observed product or service evidence and approved offline vulnerability intelligence support the analysis, TOPO ONE can identify potentially relevant vulnerabilities and help assess their applicability in the observed environment. Product, platform, version, feature, and traffic evidence can strengthen or weaken a candidate association.

A CVE association is not proof that a vulnerability is present or exploitable. Passive evidence may not establish an exact product version, enabled feature, or patch state. TOPO ONE retains uncertainty and opposing evidence instead of converting an incomplete match into certainty.

Where relevant intelligence is available, analysts may consider sources such as known-exploited-vulnerability status or exploitation-likelihood context alongside the environment evidence. Those signals support prioritization; they do not replace applicability review or prove compromise.

- Connect observed products and services with candidate vulnerability information
- Evaluate supporting and opposing applicability evidence
- Identify missing version, platform, feature, or patch-state evidence
- Relate vulnerability context to exposure, architecture, services, and reachability
- Produce conditional recommendations that state what should be validated next

Configuration and security-policy analysis

TOPO ONE can identify configuration-related and network-hygiene concerns supported by observed behavior, such as exposed or legacy services, unexpected communications, inappropriate relationships, segmentation concerns, and IT/OT boundary issues.

When an approved site policy is supplied, the analysis can compare observed flows with asserted zones and conduits and identify supported policy conflicts or gaps. TOPO ONE does not automatically read every device configuration. Analysts distinguish behavior observed in traffic, configuration or policy evidence actually supplied, and conclusions inferred from that evidence.

- Exposed, cleartext, legacy, or management-service concerns visible in traffic
- Unexpected communications or relationships that warrant validation
- Segmentation and architecture concerns
- Observed-flow conflicts with approved zone or conduit policy
- Configuration observations that remain conditional until corroborated

Reachability and segmentation

TOPO ONE builds an evidence-backed, capture-local view of which systems or services communicate or may be able to communicate. Relationships can be directly observed, inferred from available context, described as permitted or denied by supplied policy, left unknown, or marked contradictory when evidence conflicts.

This view supports service-aware path, boundary, exposure, and segmentation analysis. It remains bounded by the evidence: absence of observed traffic does not prove isolation, and potential reachability does not prove authentication success or exploitability.

Potential attack paths

TOPO ONE can analyze potential attack paths by combining available reachability, service, product, vulnerability, architecture, segmentation, policy, prerequisite, assumption, and constraint context.

A potential attack path is an analytical model of conditions that may matter. It is not proof that an attacker is present, exploitation occurred, credentials work, or compromise exists. A path may be incomplete, constrained, contradicted, or dependent on evidence that still requires validation, and the analysis does not claim to discover every possible path.

Evidence-backed findings

TOPO ONE is designed to connect material findings with supporting evidence and analytical context rather than produce unexplained scores. Findings can preserve confidence, provenance, assumptions, constraints, contradictory evidence, incomplete evidence, and the reasoning needed for analyst and customer review.

Public reporting describes these concepts at a useful customer level. Proprietary graph-construction rules, scoring or weighting logic, correlation methods, internal schemas, data-store design, rule identifiers, and performance gates are intentionally not exposed.

IT and OT analysis

TOPO ONE supports evidence-backed analysis across IT and OT environments, including architecture, communications, protocols and services, segmentation, vulnerability context, configuration and policy concerns, reachability, and potential attack paths.

For OT, industrial protocol and identity indicators can help characterize observed devices and relationships. Results are qualified by the available traffic and customer assertions. TOPO ONE does not claim definitive identification of every device, complete native protocol coverage, authoritative Purdue placement from every capture, or a complete OT asset inventory.

What customers receive

Scope and deliverables are established for each engagement. TOPO ONE supports a shared evidence base for leadership decisions, practitioner investigation, and remediation planning.

Executive reporting

- Significant findings and architecture or exposure concerns
- Potentially relevant vulnerabilities and configuration or policy concerns
- Reachability and potential attack-path implications
- Prioritized remediation and validation concerns
- Important limitations, assumptions, and decisions needed

Technical reporting

- Observed assets, entities, communications, services, and protocols
- Identity and vulnerability context
- Configuration, architecture, segmentation, and policy findings
- Reachability and potential attack paths
- Supporting evidence, confidence, assumptions, constraints, and remediation guidance

Structured analysis

- Machine-readable analysis artifacts may support repeatability, traceability, reporting, and authorized downstream workflows
- Artifact contents and customer delivery formats remain engagement-specific

Relationship to Vulnerability & Architecture Reviews

RECON ONE uses TOPO ONE as an evidence-backed network-analysis layer within Vulnerability & Architecture Reviews and related assessments. It is not simply a graphing utility: its analysis helps connect observed communications and services with architecture, vulnerability, configuration, policy, reachability, and conditional path context.

RECON ONE analysts interpret the evidence, validate material conclusions, identify limitations, and translate the results into executive priorities and technical remediation guidance. Other assessment methods and customer context may be needed to answer questions that network evidence alone cannot resolve.

What TOPO ONE does not do

TOPO ONE provides bounded analysis, not a guarantee. Its conclusions should be read with the documented scope, evidence coverage, assumptions, and limitations.

- It does not actively exploit systems or automatically modify production devices.
- It does not guarantee complete topology, asset, communication, vulnerability, or attack-path visibility.
- It does not replace an authoritative CMDB or asset inventory.
- It does not replace vulnerability scanners or vulnerability-management platforms.
- It does not prove compromise, attacker presence, authentication success, or exploitability from a potential path.
- It does not guarantee security, compliance, prevention, operational safety, or remediation outcomes.
- It does not provide a public self-service evidence-upload or processing portal.

Authorization and data handling

Analysis uses customer-provided or otherwise authorized evidence. Do not send packet captures, credentials, private keys, customer data, or other sensitive technical evidence through general website or initial email channels.

RECON ONE establishes engagement-specific scope, authorization, transfer, access, retention, and deletion requirements before sensitive evidence is handled. Detailed requirements are governed by the RECON ONE Data Handling & Security Policy and the applicable customer agreements.

[Read the RECON ONE Data Handling & Security Policy](#)

A typical engagement flow

1. **Scope and authorization** Define the decision, systems, evidence, owners, boundaries, and permitted activity.
2. **Secure evidence transfer** Arrange an approved engagement-specific method; do not send captures in the first email.
3. **Evidence validation** Confirm format, integrity, coverage, context, and known limitations before analysis.

A typical engagement flow CONTINUED

4. **TOPO ONE analysis** Develop evidence-backed environment, vulnerability, configuration, policy, reachability, and potential path context.
5. **Analyst review** Evaluate evidence, inference, confidence, assumptions, contradictions, and validation needs.
6. **Executive and technical reporting** Translate supported findings into leadership priorities and practitioner detail.
7. **Findings discussion** Review decisions, remediation priorities, remaining questions, and appropriate next steps.

Start with the decision

Start with the decision you need to make and the environment you need to understand. RECON ONE will help define an authorized scope, determine whether the available evidence is suitable, and identify the right assessment path.

[Discuss an assessment with RECON ONE](#)



Cybersecurity analysis grounded in authorized evidence.