CrossConnect by Cybr IQ

THE CAPABILITY GUIDE · TEN AREAS, DRAWN OUT

Everything CrossConnect does. Drawn so you can see it.

One accurate record of your whole network, an assistant that cites every answer, and the analysis that tells you what to fix first, for the wired estate and the AV estate alike. This is the visual tour of all ten areas, with the proof behind every claim and not a single packet captured.

Runs on your own servers | Cites every answer | No packet capture | AV-native

An operator preview in active development. Everything shown here is **built and running today** against a real demo network.

WHAT YOU ARE LOOKING AT

One platform, ten areas, one source of truth.

CrossConnect keeps the authoritative record of your network and the live reality next to it, reconciles the two, and turns the difference into a ranked, evidence-backed list of what to do. The product is organized into ten areas. This guide walks every one of them.

10

capability areas, end to end

130+

individual capabilities

0

packets captured, ever

100%

answers cited or “I don't know”

THREE PROMISES UNDER EVERYTHING

Why you can trust what it tells you.

Documented vs. discovered

Every record is marked as something you recorded or something the network revealed. The two are reconciled, never silently merged, so you always know where a fact came from.

DOCUMENTED DISCOVERED

Confidence, never invented

Where CrossConnect infers something, it labels how sure it is and shows the next check instead of bluffing. No fake precision, anywhere.

Confirmed Inferred Unconfirmed

Read-only and advisory

It observes switch-derived signals only, no packet capture, no payloads. The assistant advises and cites; it never changes your network, and any write is confirm-before-commit.

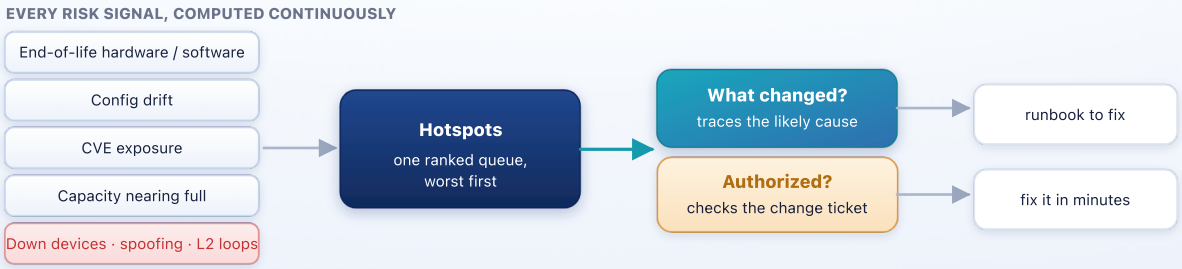
No packet capture

Confirm-before-commit

01 OVERVIEW & SITUATIONAL AWARENESS

Walk in, and know exactly what to do first.

No more staring at a dozen dashboards trying to guess what matters. Every risk the platform finds, aging gear, config drift, CVEs, capacity, outages, spoofing, becomes one ranked queue. Open any item and CrossConnect tells you whether a change caused it, and whether that change was even authorized.



Triage becomes one screen, not twelve. Every risk normalizes into a single severity-ranked queue, and every item explains itself.

Hotspots `/hotspots`

The ranked “act on this now” queue across every risk the platform computes, worst first, each with the evidence and the recommended next step.

What changed, likely cause `/hotspots`

Walks the tamper-evident audit trail to tell you whether a problem was caused by a change, and flags it when that change carried no authorizing ticket.

Topology `/topology`

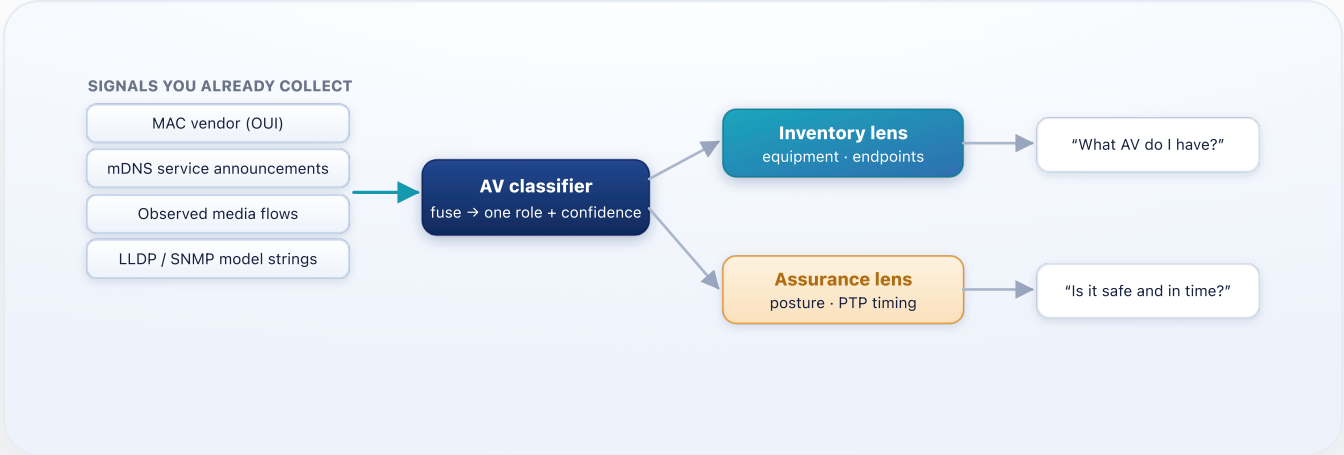
The live Layer-2 map built from discovered neighbors. Filter to one service to isolate just the devices and links that deliver it.

> **On a real day:** a CRITICAL “Device down: acc-stuA-12” sits above a MEDIUM “IP space at 78%,” and the drift hotspot reads “Likely caused by a change, VLAN 30 added yesterday, no change ticket.”

02 AV & MEDIA

The only network tool that treats AV as first-class.

Crestron, Q-SYS, Dante, NDI, cameras and codecs are not mysteries on your network anymore. CrossConnect identifies every AV device automatically, types each endpoint by role, proves it is properly walled off from the rest of the network, and verifies that the precision timing your audio and video lock to is healthy. All with zero extra data entry, and not one captured packet.



One set of signals, two answers. The same evidence powers an inventory of your AV fleet and an assurance check on whether it is segmented and correctly timed.

AV endpoints `/av-endpoints`

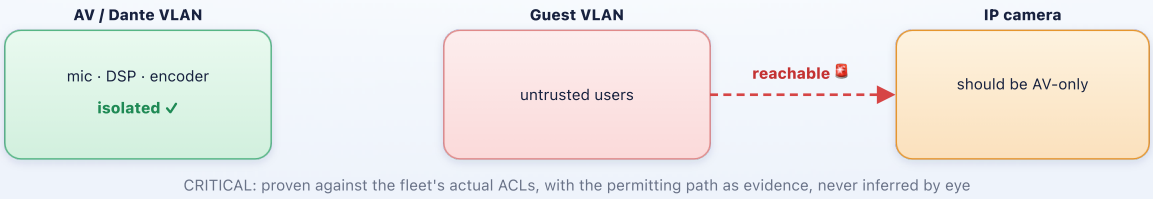
Every AV endpoint typed by role, codec, display, camera, mic, DSP, encoder/decoder, with a Confirmed / Inferred / Unconfirmed chip. Gear not in inventory is flagged as shadow AV.

AV posture `/av-posture`

A 0–100 segmentation score with ranked findings: a camera reachable from guest, a control port exposed, a shadow device on a sensitive segment, each proven by reachability, not guessed.

PTP / clock health `/ptp-health`

Scores whether the timing every Dante/AES67 stream locks to is resilient and in lock, and names the fix when a domain has no backup grandmaster.



CRITICAL: proven against the fleet's actual ACLs, with the permitting path as evidence, never inferred by eye

Proof, not guesswork. Findings are computed against your real configuration; when the analysis cannot decide, the answer is an honest “unconfirmed,” never a fabricated pass.

Example: a Shure Dante box announcing `_dante._tcp` and sourcing AES67 is typed av-microphone, Confirmed; the AV posture score reads 62/100 with one camera reachable from guest; clock health 70/100 flags a domain with no failover.

03 INVENTORY & FACILITIES

One record of physical reality, finally trustworthy.

Every device, the modules inside it, the rack it sits in, and the power feed that carries it, one connected chain instead of four spreadsheets that disagree. This is the foundation every other area reasons over, and discovery keeps it current on its own.

Inventory is a chain. Every device traces down to a rack position and the electrical feed that powers it, so power redundancy and headroom are computed, not estimated.

Devices `/devices`

Every switch, router, and AP with vendor, model, location, software, role, and status, sortable on every column, the object the rest of the platform hangs risk and connectivity off.

Network services `/network-services`

The intent layer: a named outcome (“Dante audio fabric”) with its devices, VLANs, and circuits bound to it, so health and impact roll up to the business outcome, not the box.

Racks & power chain `/rack`

Drag-to-place rack elevations with half-width mounting, and a power chain that traces every watt from device PSU through PDU outlet to feed.

Zero data entry to start, discovery fills it

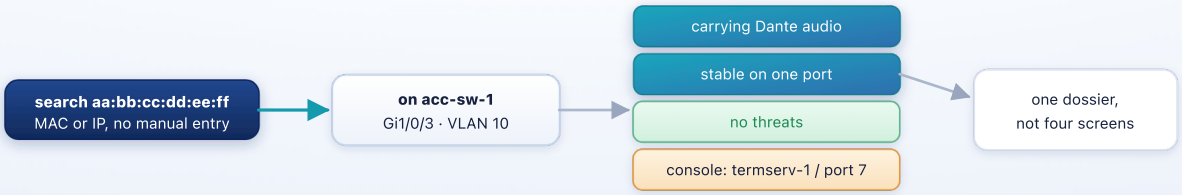
Half-width rack mounting modeled accurately

Service-level health, not just device-level

04 CONNECTIONS & TOPOLOGY

Trace any path. See what breaks before it does.

Type a MAC and find the exact switch port in one lookup, with the full story of what that endpoint is doing. Follow a VLAN across the fabric. And before you touch anything, ask “what loses connectivity if this device fails?” and get a real answer, simulated against the live network.



Where is it, and what is it doing? One lookup returns location, live traffic, move history, threats, and the out-of-band path to reach the switch when the network is down.

Locate a device `/locate`

The where-is-it lookup with no manual entry, plus the context you would otherwise gather from four separate screens.

Multicast: groups & map `/multicast-groups`

Every multicast group in plain language, as a list or a flow map, merged from real traffic and IGMP membership. No packet capture.

Failure impact `/failure-impact`

Pick a device; CrossConnect removes it from a copy of the live network and reports what loses connectivity and which services are at risk. Empty means verified redundancy.

> **Example:** if dist-hq-01 fails, 14 flows lose connectivity (no second path) and the Dante audio service is impacted, computed by simulation, not by eyeballing the diagram.

05 ADDRESSING (IPAM)

Your whole address plan, with utilization built in.

From the blocks a registry issued you down to the individual host, plus the VLANs, routing instances, and trust planes layered over them. Utilization, overlap, and next-free answers come for free, and purpose labels let the network read by intent instead of by number.

Segmentation you can read at a glance. Trust planes are derived from your VLANs; the matrix shows exactly where two planes meet on the same switch.

Prefixes `/prefixes`

CIDR blocks with status, utilization, overlap detection, and a next-free-subnet answer, the spreadsheet replaced by a working surface.

Network zones `/zones`

The estate grouped into trust planes derived from your VLANs, with a matrix showing where planes are bridged, the structure behind every segmentation check.

VLANs & IPAM roles `/vlans`

802.1Q VLANs with the devices that carry them, plus purpose labels (audio, video, control, guest) shared across prefixes and VLANs so intent is explicit.

Next-free subnet and IP, computed

Overlap detection out of the box

Reads by **intent**, not just by number

06 ASSURANCE & COMPLIANCE

Proof your network is correct, secure, and in policy.

Stop guessing from configs by eye. CrossConnect builds one formal model of your whole fleet and answers the hard questions: can guest reach the cameras, which change broke that flow, are you passing CIS and PCI, and which device should you fix first. Five overlapping risk lists become one decision per device.

Decide once per device, not five times. Worst-first, with the recommended action and the service it protects named, so you stop reconciling five dashboards.

Reachability & segmentation `/reach-check`

Verifies intended behavior against your real ACLs: does A reach B, and should it? Surfaces the leak nobody catches, isolated in policy but traffic observed.

Network black box `/black-box`

Name a flow that used to work; CrossConnect binary-searches the config history to find the exact change that broke it, with the diff and time window as proof.

Compliance `/compliance`

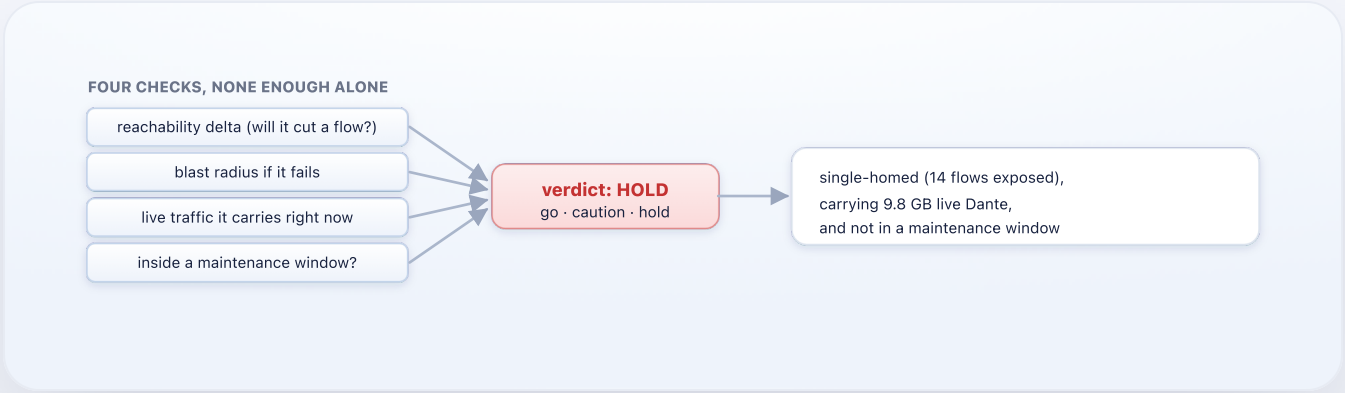
CIS, NIST-CSF, SOC 2, PCI, and ISO scored as data over evidence you already have, one reusable check satisfying many frameworks at once.

> **The black box, in action:** “Dante 10.10.10.0/24 → UDP 4440: healthy 48h ago, broken by an egress ACL added to Vlan20 on cor-bb-01 24h ago.” It names the cause; it never changes anything.

07 OPERATIONS

Run the network with both hands on the wheel.

Is the site ready? Where is capacity heading? Is this change safe to make right now? CrossConnect answers all three from telemetry it already has, then gives you the automation, maintenance windows, and reports to act. Change safety is the headline: four checks, none of which alone says “safe,” combined into one verdict.



Together, they catch what any single check misses. One GO / CAUTION / HOLD verdict before you push a change, with the reasons spelled out.

Service readiness `/readiness`

Device health rolled up to the groups that deliver service, by site or role, so you see whether the site is ready, not whether one switch is up.

Change safety `/change-safety`

A pre-flight cockpit that joins reachability, blast radius, live traffic, and the maintenance window into one verdict.

Capacity planning `/capacity`

Forecast-to-full across PoE, rack space, bandwidth, and IP, projected onto each network service so pressure reads against a business outcome.

No new agents to deploy, reuses telemetry

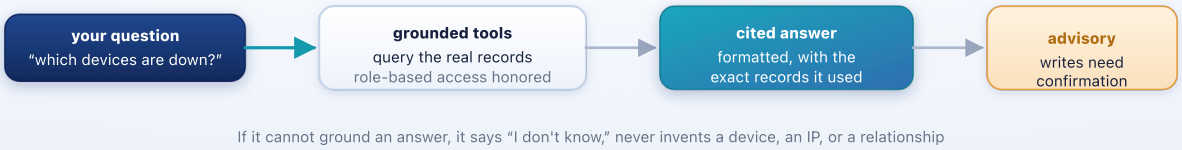
Service-scoped maintenance windows

Generated **Terraform / Ansible** for upgrades

08 AI ASSISTANT

Ask your network anything. Check every answer.

A conversational layer over your whole source-of-truth. Ask in plain English and get an answer drawn from your real records, with the records it used shown right there. It honors who is allowed to see what, says “I don't know” instead of bluffing, and never changes anything without your confirmation.



If it cannot ground an answer, it says “I don't know,” never invents a device, an IP, or a relationship

Grounded, cited, and safe. Every answer points at the records behind it; the assistant advises and explains, and never silently touches the network.

Assistant `/assistant`

Ask about your fleet and get cited, formatted answers from the live source-of-truth, with every prompt, retrieval, and output logged.

AI quality `/ai-quality`

An improvement loop: a quality score and a backlog of weak answers to work, each pointing at a tool to add or a record to fix.

Bring your own model `/ai-setup`

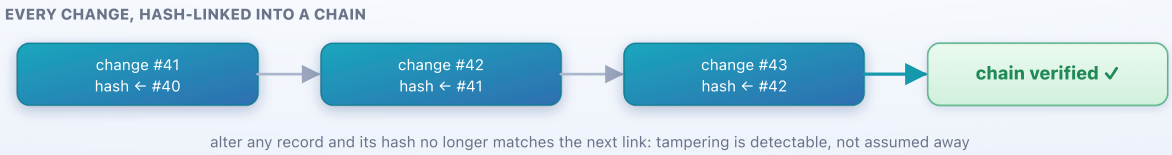
Provider, model, and an encrypted key per tenant, with a test-connection. Proposed write actions wait in a queue for your approval.

> **Example:** “Which devices are down and who owns them?” returns the list with the owning contact, every row linked to its record, so you can verify the answer in one click.

09 ADMINISTRATION & GOVERNANCE

Safe to operate, built to be trusted.

Tenant isolation, roles, an encrypted secrets vault, and a record of every change that cannot be quietly rewritten. Connectors stay dormant until you turn them on, and inbound data passes through a trust gate before it ever becomes truth. This is what lets an auditor, or your insurer, take the platform's word for it.



A history that cannot be quietly rewritten. Records are chained by hash, so the audit trail either verifies or it does not, the integrity behind every compliance claim.

Tamper-evident audit chain `/recent-events`

Every change hash-linked and verifiable, the guarantee behind the “what changed” traces and the compliance evidence.

Inbound review `/inbound-review`

External assertions arrive as proposals, resolved and confidence-scored, for you to confirm or dismiss. Nothing inbound silently becomes truth.

Happy Auditor `/happy-auditor`

A one-click, control-mapped evidence pack an auditor or cyber-insurer accepts, assembled live with an integrity verdict on the chain itself.

Dormant by default, no port open until configured

50+ signed webhook event types

Tenant **isolation** on every record

10 LEARN & ONBOARDING

Up to speed in an afternoon, not a quarter.

A guided front door reads your real network and draws its shape, so a newcomer builds a mental model without typing anything. From there, single-job workflows and end-to-end playbooks walk every common task, and a full API reference and data-provenance map back it all up.

Learning that scales with you. Orient with the Atlas, follow one workflow, or chain workflows into a full journey like onboarding a whole new site.

Start here, the Atlas `/start`

Reads your real estate and draws its shape, then previews every operational feature read-only against your own network, so it teaches the product and the network at once.

Workflows & playbooks `/workflows`

A searchable library of step-by-step jobs, chained into end-to-end journeys like “onboard a site” or “pass an audit.”

API & data provenance `/learn/api-catalog`

The full REST and webhook reference with copy-paste examples, plus a provenance map of where every piece of data comes from.

> **Day one:** open `/start` to see “your network in 60 seconds,” click the AV-fleet tile to see your Crestron and Q-SYS gear, then follow the clickable first-week path, all read-only, nothing at risk.

THE WHOLE PICTURE

See your network the way it really is.

CrossConnect holds the authoritative record of your network and the live reality beside it, reconciles the two, and hands you a ranked, evidence-backed list of what to fix, for the wired estate and the AV estate alike, without touching a single packet.

CrossConnect