Sales Enablement Kit: NetRoute Module

Motadata Unified Observability Platform

Module Overview: What is NetRoute?

NetRoute is a network path analysis module within the Motadata AIOps Unified Observability Platform, designed to visualize and monitor end-to-end network routes. It graphically maps the path from a source to a destination through each hop (router or node in between), providing a **topological view of the entire route**. NetRoute actively tracks route changes and multi-path traffic in real time, highlighting the active path and any deviations or alternate routes. By evaluating each hop's performance (latency, packet loss, etc.), it quickly identifies bottlenecks or points of failure in the network path. NetRoute maintains a historical record of path performance, allowing teams to **"replay" network routes over time** for troubleshooting past incidents and spotting recurring issues. Alerts are integrated into the route view – if a hop or entire path has issues, it's indicated with severity-based color codes for instant visibility. In short, NetRoute gives IT teams a **hop-by-hop insight** into network connectivity, from the user's vantage point to the destination, all within a unified observability dashboard.

Value Proposition:

Motadata NetRoute provides enhanced network path analysis featuring detailed routing visualization, hop-by-hop performance insights, and even predictive outage detection. By combining severity-based alerts with comprehensive path history, NetRoute streamlines troubleshooting and optimizes network efficiency.

In under 100 words:

NetRoute helps you instantly pinpoint **"where the network breaks"** by showing every hop between users and services, flagging problem spots, and enabling fast root-cause isolation – even across the public internet.

Elevator Pitch

- **30-Second Pitch (Customer-Facing):**

  "Modern IT users don't care why *the network is slow – they just need it fixed fast. With Motadata's NetRoute module, our observability platform literally draws you a map from your users to their apps, highlighting every hop and pinpointing where issues occur. Think of it as traceroute on steroids: always-on, historical, and correlated with your alerts. NetRoute means no more finger-pointing between teams – you'll see exactly where the network is breaking and solve issues before users even notice."*

- **30-Second Pitch (Partner-Facing):**

  "Motadata NetRoute gives you a competitive edge to offer your clients. It's an advanced network path monitoring add-on that others charge a premium for – but we deliver it unified in our platform. In seconds, NetRoute visualizes the entire path from an end-user to a service, even through the cloud or ISP. For you as a partner, it's a differentiator – you can solve the 'invisible network issue' complaints with a proven tool that maps issues hop-by-hop. It helps you drive value and showcase innovative solutions, without complex setup."

- **1-Minute Pitch (Customer-Facing):**

  "Every minute of outage or slow performance, you're losing productivity and credibility. Traditional network monitoring tells you if a device is up, but not which route *a user's traffic took or where it got stuck. That's where NetRoute shines. In one view, you get the entire route from the user to the application – whether it's on-prem or in the cloud – with each hop's health indicated. Imagine being able to click on a user complaint and instantly see that the slowdown is at the third hop, maybe a misconfigured ISP router or a congested link. NetRoute not only shows current paths but lets you roll back in time to see yesterday's route when things were working fine, so you can identify what changed. It's like having x-ray vision for network paths, built right into your observability workflow. The outcome? Faster root-cause analysis (often* minutes*, not hours), proactive detection of routing issues, and proof to hold providers accountable to SLAs. In short, fewer escalations and happier users – because you solve problems before they escalate."*

- **1-Minute Pitch (Partner-Facing):**

  "Let's talk about giving your customers so mmething extra. Many IT teams struggle with issues that aren't within their four walls – the problem could be an ISP or a cloud route, and their tools go blind beyond the datacenter. NetRoute fixes that. It's an integrated module in Motadata AIOps that performs end-to-end route tracing with intelligence. For you, as our partner, this means you can offer a solution that others might need a separate product for (like ThousandEyes or fancy add-ons). With NetRoute, you can demonstrate to clients how you'll provide visibility not just into their devices, but the actual network paths their traffic takes. It's agent-based plus agentless: deploy a lightweight probe on any critical endpoint or branch, and map out to any destination – cloud, SaaS, you name it. The system will alert on path breaches, automatically correlate with other events, and even predict outages using AI. As a partner, you'll differentiate your proposal with this capability, drive additional service revenue (through deployment and tuning of NetRoute), and most importantly, help your clients drastically cut down their MTTR for network issues. It's a win-win: they see more value in the Motadata platform, and you build trust as the provider who brings cutting-edge yet practical solutions."

Pain-Solution-Value Narrative: The elevator pitches above follow a simple narrative – start with the **pain** ("we can't see where the network breaks, traceroute is too manual"), introduce the **solution** (NetRoute's automated, visual hop-by-hop tracing with alerts), and end with the **value** (faster troubleshooting, proactive issue prevention, better SLA management, happier users, etc.). The idea is to quickly convey that *we understand the common network pains* and that *Motadata NetRoute is the purpose-built answer* to those pains, delivering tangible outcomes.

Core Capabilities Cheat Sheet

Feature	What It Does	Customer Benefit	Demo Highlight
Hop-by-Hop Visualization	Graphically maps each network hop from source to destination in real time. Highlights the path taken by traffic with visual indicators on each hop.	Fast root-cause isolation – instantly see which hop is causing a slowdown or failure. Makes troubleshooting intuitive ("follow the red node").	Show the live topology of a sample route; click through each hop to see latency. Emphasize how a problematic hop turns red, guiding the engineer's eyes immediately.
Dynamic Entity Resolution	Automatically resolves IP addresses to meaningful entities (hostnames, device roles, locations). Updates labels as devices are identified.	Provides context at a glance – engineers see "Firewall – New York" or "ISP Router – AT&T" instead of just IPs. This rich context means faster analysis and less guesswork.	Point out how an IP in the path auto-resolves to a known device name. Correlate that with inventory info. Shows how alerts on that hop are correlated with the device's info.
Historical Route Playback	Maintains a timeline of route data and allows replaying the network path as it was at a past timestamp. You can compare current vs. past routes.	Troubleshoot intermittent or past issues ("what changed since yesterday when it worked?") and verify if routing changes caused an incident. Proves SLA compliance by showing evidence of when/where failures occurred.	Use the timeline slider on a route visualization to switch between last week's route and today's route. Show that a hop that was green last week is red or taking a different path today. This elicits the "aha" moment linking a change to the outage.
AS-based Grouping	Automatically identifies and groups public network hops by their Autonomous System (AS) or service provider. For internet routes, clusters hops that belong to the	Enables third-party dependency analysis – e.g., see which ISP or cloud provider is causing latency. Simplifies complex internet paths by collapsing multiple nodes owned by one	Show an internet route where several consecutive hops are within the same ISP (e.g., AS 7018 for AT&T) – the UI groups them and maybe labels the group "AT&T backbone."

Feature	What It Does	Customer Benefit	Demo Highlight
	same ISP or carrier network.	provider into a single logical group for clarity.	Demonstrate toggling the group open/closed. Highlight how this immediately shows if a particular provider's network is the bottleneck.
Route-from-Agent Support	Allows path tracing initiated from remote agents (e.g., a lightweight Motadata agent on a branch PC or cloud VM) towards any target. Essentially, you can start a route test from *anywhere* – not just from the central server – giving last-mile visibility.	Last-mile and user perspective coverage. For example, simulate a remote user's connectivity to a SaaS app by launching NetRoute from the user's location. This provides insight into issues that occur *after* the traffic leaves the core network (e.g., local ISP or home network issues).	In the demo, pick an agent representing a branch office as the source and a cloud application as the destination. Initiate a NetRoute. Show how the path starts at the branch's agent, goes through local ISP nodes, and reaches the cloud service – something traditional NPM tools wouldn't easily show. If possible, demonstrate deploying an agent live (if time permits) and immediately getting a path trace.
Policy-based Alerting	Lets you define performance thresholds and SLA policies on routes or even individual hops (e.g., packet loss > X% on any hop, or end-to-end latency > Y ms). NetRoute policies generate alerts with severity levels when these conditions are met. Alerts are	Proactive network management – catch and fix routing issues before users complain. Ensures you meet uptime and performance SLAs by monitoring path KPIs, not just device health. Hop-level alerting means even a third-party outage (like an ISP router down) can	Show an example policy where if any hop's latency exceeds 100 ms or packet loss > 5%, an alert is triggered. Then in the demo, simulate a high latency on a hop (if possible) or use a recorded scenario – watch the hop turn yellow/red on the

Feature	What It Does	Customer Benefit	Demo Highlight
	overlaid on the route map with color-coded severities and can trigger notifications via the usual channels.	trigger an actionable alert.	map. Open the alert view to show that NetRoute pinpoints **which hop** violated the policy. This is a wow factor compared to generic "ping failed" alerts.

In summary, NetRoute's core features work in harmony: it visualizes the path, enriches it with context (names, AS details), retains history, and ties into alerting to not only display but also proactively notify when something's off. Each of these capabilities can be a deciding factor for customers who need faster and smarter network troubleshooting.

Customer Pain Points Solved

Many network issues hide between traditional monitoring silos. Here are common pain points we hear – and how NetRoute addresses them:

- **"We don't know where the network breaks."**
  NetRoute solution: Provides end-to-end **path maps** that clearly mark where a packet fails or gets delayed. Instead of guessing, you can **see the exact hop** where the failure occurs (e.g., the third hop in the path is down). No more blind spots – whether the issue is in your LAN, at your ISP, or in the cloud, NetRoute shows you where the break is.

- **"User complaints can't be traced to root cause."**
  NetRoute solution: Transforms vague "the app is slow" tickets into actionable data. By tracing the user's route to the application, NetRoute often reveals if the problem is network-related and where. For example, a user's complaint about slow SaaS access might be traced to an overloaded router on their path. NetRoute correlates route performance with the user's issue, drastically reducing the time to root cause.

- **"We lack visibility across internet paths."**
  NetRoute solution: Extends your observability beyond your private network. It monitors **internet routing** hops by leveraging both agent-based traces and public data (like AS lookups). You gain visibility into external networks – seeing if, say, a particular ISP's backbone is dropping packets. Essentially, NetRoute gives you **ISP and cloud path visibility** that typical NPM solutions cannot, bridging the gap between your enterprise network and the outside world.

- **"We can't proactively catch routing issues."**
  NetRoute solution: Enables **proactive alerting on path metrics**. Instead of waiting for users to complain, you can set policies (e.g., if any path's latency jumps or if a

backup path is taken). The moment a route deviates or degrades beyond set thresholds, NetRoute fires an alert (with severity color-coding on the map)[4]. This means you can address a routing issue – such as a failing WAN provider link – before it causes a major incident or outage for users.

- **"Our teams lack context for triage."**
  NetRoute solution: Every alert or route view in NetRoute comes with rich context – the device names, roles, ownership (via dynamic entity resolution), timestamped history, and correlation with other events. When a NOC engineer looks at a NetRoute alert, they don't just see "path latency high"; they see **which hop**, the likely owner (e.g., "ISP – Comcast" or "Firewall – HQ"), and recent changes on that path. This context empowers Level 1 support to do smarter triage and hand off issues with clear evidence (e.g., providing the exact hop/IP that's problematic and who to escalate to).

By directly solving these pain points, NetRoute reduces frustration and back-and-forth in troubleshooting. Teams can **focus on fixing the problem rather than finding it**.

Target Personas

Different IT personas benefit from NetRoute in distinct ways. Here's a quick view of who gains what value:

Persona	Key Pain Point	Value NetRoute Delivers
NOC Engineer (Network Ops Center)	Slow RCA (Root Cause Analysis) during outages – war-room bridges taking hours to isolate whether it's the network and where.	**Hop-level fault isolation** in seconds. NetRoute points the NOC to the exact segment or node causing the issue (e.g., "it's the link between hop 4 and 5"). Reduces mean time to identify and repair drastically.
Network Architect	Uncertainty in how traffic actually flows, especially with dynamic routing – *"Route drift"* over time or across hybrid cloud.	**Route consistency over time.** NetRoute's historical playback lets architects verify if actual traffic paths align with design, and detect unintended changes or suboptimal routing. They can validate routing policies and see if any path is taking a detour.
Application Owner (IT App Manager)	User experience issues (slow or down apps) often turn into finger-pointing between app and network teams. Lack of end-to-end validation to prove the network is or isn't at fault.	**End-to-end path validation** for their application. With NetRoute, an app owner can trace from user to app server, confirming network health. If an issue is network-related, it's pinpointed; if not, they have evidence the network is clear. This builds trust between app and network teams and speeds up problem resolution for the application.

Demo Walkthrough

A well-structured demo can make NetRoute's value **tangible**. Here's a guide:

Pre-Demo Checklist

- **Set Up Sample Paths:** Before the demo, configure a couple of NetRoute paths that will be interesting to show. For example, one path from a branch office agent to a cloud application (to illustrate internet hops), and another within the datacenter (to show internal hops and maybe an induced issue). Ensure these are polling and have data in NetRoute.
- **Test Data Ready:** If possible, introduce a *controlled issue* to demonstrate (e.g., use a traffic control tool to add latency or drop packets on a certain router for the demo – or use historical data from a past incident). This will make the demo realistic and highlight problem detection.
- **Dashboards & Access:** Have the Motadata AIOps UI logged in and navigate to the NetRoute module or dashboard. Ensure the audience can also see any correlated views (alerts console, etc.) if you plan to show them.
- **Narrative Planned:** Know the storyline – for instance, *"User in London can't reach our CRM – let's use NetRoute to find out why"* – and have that scenario ready to walk through.

Suggested Demo Data/Scenario

- **Synthetic Route for Demo:** Create a synthetic monitoring route (if available) to, say, google.com or a SaaS site from multiple agents. This often shows a mix of internal and external hops and can intentionally have one path healthier than another (for example, one agent might route through a slower ISP). Alternatively, use a known **historical event**: e.g., "Last Friday we had an issue – let me show you how we diagnosed it with NetRoute's playback."
- **In-App Context:** Make sure to demonstrate how NetRoute is accessible in the platform – for instance, perhaps show that from a central NOC dashboard, an alert can drill-down into a NetRoute view (if such integration exists). This ties the feature into daily use.

Key Demo Highlights to Emphasize

1. **Hop Severity Coloring:** Show a route where one of the hops is colored yellow or red due to a threshold breach. Explain, *"See how Hop 5 is red – that indicates it's in a critical state (perhaps high latency or packet loss). NetRoute immediately draws your attention there."* This visual pop is compelling. **Explain the threshold/policy** that caused the coloring (e.g., >5% packet loss turns it red) and how that could trigger an alert. This answers "how do we know if something's wrong?" – it's instantly visible.
2. **Timeline Route Switching:** Utilize the historical slider or time picker. For example, *"Now, let's rewind to an hour ago… notice the route was different (or healthy). You*

can literally see how the path changed." If a route changed (e.g., took a different ISP), point that out: *"At 1 PM, traffic shifted through a backup path – see these extra hops appear."* This shows off the **Historical Route Playback**. If nothing changed in topology, use performance: *"At 12:00, latency at hop 5 was 20ms (green); by 12:30 it spiked to 200ms (red). NetRoute captured that change."* This highlight proves that NetRoute is not just a static tool, but a time machine for network paths.

3. **Alert Policy Violation Simulation:** If possible, trigger an alert in real-time. For instance, manually increase latency on a test link or use a network emulator. If live simulation is risky, have a **pre-recorded alert** (maybe show one in the alert list that occurred). Walk through how a NetRoute alert appears: *"Here's an alert we got – 'High packet loss on Path X (Critical)'. Clicking it takes us to the NetRoute view and it's pinpointing the problem on the path."* Show the audience how you'd then drill in, maybe by clicking the problematic hop to get details (like IP, device name, metrics). This drives home that **proactive, policy-based alerts** are part of the solution – not just passive maps.
4. **Integration Points (if time permits):** Mention or show that NetRoute is part of the unified platform. For example, demonstrate cross-launch: *"From this hop, I can pivot to see device metrics or logs"* (if applicable) to show the power of having NetRoute within Motadata vs. a standalone tool.
5. **Use Case Tie-back:** End the demo segment by tying what you showed to a real use case. For example, *"In a real scenario, what we just saw could mean the difference between a 2-hour outage and a 10-minute glitch – because with NetRoute, we identified the ISP in Paris was at fault and rerouted traffic."*

Demo Pro Tips: Keep the demo **interactive and story-driven**. Instead of just feature dumping, pose a problem ("user can't reach service") and then use NetRoute to solve it. Encourage questions like *"What if the issue is outside our network?"* – then show how NetRoute reveals external hops. And always highlight the outcome: faster resolution, evidence for ISP escalation, etc., as you demonstrate each feature.

Objection Handling

Handling common objections confidently can turn skeptics into champions. Here are likely objections and **suggested responses**:

Objection	Suggested Response
"We already use traceroute tools."	*"I understand – almost everyone uses traceroute. The problem is, traceroute is a manual, one-off tool and gives you just a snapshot with no intelligence. It lacks correlation with other data, has no historical memory, and can't alert you proactively. NetRoute automates what traceroute does, running continuously in the background and logging every hop's performance over time. It's like having an expert constantly mapping and watching your routes, so you don't have to. Plus, traceroute outputs text that you have to interpret – NetRoute shows it in a live diagram with context (device names, severities). And you can set policies – traceroute won't page you at 2 AM if a path is down, but NetRoute will. In short, we take traceroute's concept to an enterprise-grade level: always on, historically aware, and integrated with your monitoring."*
"How does this work in hybrid cloud environments? Our network isn't just on-prem."	*"Great question. NetRoute was built with cloud and hybrid in mind. We deploy lightweight agents wherever you need them – on-premises, in cloud VMs, even in container environments – to initiate routes from those points. And from the central server side, it can trace to cloud endpoints as well. So whether the path goes through AWS, Azure, or your on-site data center, NetRoute can cover it. Motadata's platform is designed for cloud, on-premises, and hybrid infrastructure – you get a unified view. For example, you can trace from a branch office to an Office365 endpoint, traversing the internet, and see each hop. Many of our customers specifically use NetRoute to gain visibility into cloud provider networks and the links between their offices and cloud services. Bottom line: if your network spans multiple environments, NetRoute will connect the dots."*
"Why not just use our existing Network Performance Monitoring (NPM) tools?"	*"Traditional NPM tools are excellent for device health (CPU, memory), interface stats, SNMP traps, etc. But they don't visualize the end-to-end path that user traffic takes. They tell you if a router is up or if a link is congested, but not which path a user's packet chose across a complex network. NetRoute is complementary – it fills the gap by*

Objection	Suggested Response
	focusing on the path perspective. *It answers questions standard NPM can't:* Is the problem on the user's local network, on one of the hops in between, or at the destination? *It's especially useful for troubleshooting issues that involve third-party networks (ISP, cloud). Many NPM solutions also don't retain hop-by-hop historical data or allow per-hop alerting. So by adding NetRoute, you're supercharging your NPM: it's like adding a GPS on top of your car's engine monitor. The engine monitor (NPM) tells you the car's performance, but the GPS (NetRoute) tells you the road you're on and where there's a traffic jam. For a complete observability story, you want both. And Motadata provides both in one platform."*

Tip: When handling objections, always acknowledge the point (*"I hear you – traceroute is familiar"*) and then pivot to how we **enhance or address** that concern. Use real examples if possible (e.g., a story of a customer who thought their basic tools were enough until a problem hit and NetRoute saved the day). Back up technical claims with brief facts (as above, we mention traceroute's lack of history as a known limitation). Keep the tone confident, not defensive, and end by checking if the answer addresses their concern.

Pricing & Licensing Snapshot

(Note: Pricing can vary, so use this as a general guide – be sure to consult the latest pricing sheets.)

- **Core Module Licensing:** The NetRoute module is part of the Motadata AIOps **Unified Observability** suite. It is typically licensed based on the number of *NetRoute paths* you want to monitor. **No separate product to buy** – it's a feature module within the platform, so if you have the appropriate edition of Motadata AIOps, you have NetRoute available.

- **Add-On Requirements:** NetRoute's functionality leverages Motadata agents for distributed path monitoring. The **Motadata Monitoring Agents** (lightweight software) can be deployed to remote locations or cloud instances to initiate routes. These agents are the same ones used for infrastructure monitoring, so there's no special "NetRoute-only" agent. You'll just need to account for any additional agent installations in your licensing. Other than agents, no additional add-ons are required – features like AS lookup, historical storage, etc., are included. In contrast to some competitors that charge separately for "network path monitoring" or cloud-based path tests, Motadata includes NetRoute under the unified license, making it **cost-effective** for comprehensive use.

- **Typical Deployment Size & ROI:** A typical deployment might start with monitoring, say, 5-10 critical routes (e.g., HQ to Data Center, Data Center to Cloud, key branch to HQ, etc.). Many customers then expand to dozens of routes as they realize the value. **ROI** is usually seen in terms of reduced downtime and faster MTTR: for instance, a customer running NetRoute across their WAN links identified issues 40% faster than before, on average, translating to significant savings (both in IT effort and business impact of outages).

  When pitching ROI, mention: *"If NetRoute prevents even one major outage or saves a few hours of troubleshooting each week, it pays for itself. Imagine proving an SLA breach and getting credits from your ISP – that alone can justify the cost."* Additionally, because NetRoute is integrated in the platform, there's an **operational efficiency ROI**: teams don't juggle multiple tools (saving training and integration costs).

Summary

Finally, condense everything into a one-page high-level **summary** that sales reps can use at a glance or leave with the customer. Here's what that summary should include:

Top 5 Benefits of NetRoute:

Faster MTTR (Mean Time to Repair): Cuts troubleshooting time by up to 50% by instantly isolating problem hops (no more trial-and-error).
End-to-End Visibility: See the entire journey of your data – across on-prem, cloud, and ISP networks – nothing lies in the shadows.
Proactive Issue Detection: Get ahead of outages with policy-based alerts on path performance (find out about issues before users do).
Accountability & Proof: Hard evidence of where issues occur – use it to hold ISPs accountable to SLAs or to show other teams "it's not the network" (or prove that it is!).
Unified Observability & AIOps: Seamlessly integrated into Motadata's platform – correlate route issues with device metrics, logs, and events using AI for a holistic approach.

Key Differentiators (Why Motadata NetRoute):

Built-in Agents: Deploy anywhere – monitor from branch offices to cloud VPCs without costly add-ons (competitors often require separate appliances or licenses for this).
Full Historical Replay: NetRoute is like a DVR for your network routes – competitors show only current data or limited history. We store and visualize the past, which is golden for post-incident analysis.
Rich Context Per Hop: Every hop isn't just an IP – it's enriched with info (hostname, ASN/ISP, etc.) automatically, saving you time and making the data immediately actionable.
Hop-Level Alerting: Our alerts don't just say "path down"; they say "hop 7 packet loss 80% – Critical" and flash it on the map[4]. Precision and clarity that others lack.
Part of Unified Platform: One tool to learn, one support to call. NetRoute works hand-in-hand with your infrastructure monitoring and service desk (Motadata ServiceOps) – an integrated solution vs. a patchwork.