The missing layer: solving the BGP security blind spot

White paper

Contents

Introduction

The Border Gateway Protocol (BGP) underpins the routing of every packet across the global internet. But it was designed for reachability, not security, and was built on the assumption that network operators would behave honestly and that their public routing information could be trusted. For most of the internet's history, that assumption held. It no longer does.

That's because BGP hijacking and route leak incidents have become recurring problems. A network operator may, deliberately or accidentally, advertise IP prefixes they do not own—redirecting traffic through unintended paths, enabling interception or causing widespread outages. In documented incidents traffic destined for financial institutions, cloud providers and government networks has been silently redirected—sometimes for seconds, sometimes for hours.

The community's response has been substantial. RPKI provides a cryptographic framework for binding IP prefixes to their legitimate originating Autonomous Systems (AS). Route Origin Validation (ROV), built on RPKI, allows routers to reject routes whose origin does not match a valid Route Origin Authorization (ROA). Autonomous System Provider Authorization (ASPA) extends this to path validation, detecting route leaks that ROV alone cannot catch. Both ARIN and RIPE NCC enabled ASPA object creation in late 2025 and early 2026, marking the protocol's transition from draft to production reality.

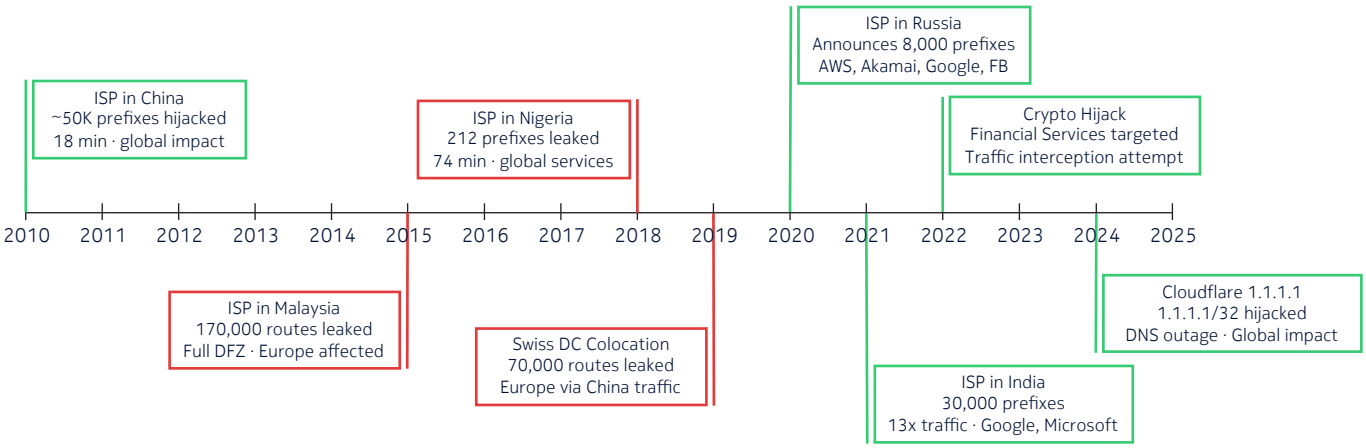
The protocols are ready, but the implementation gap is not the standards—it is the tooling. No existing tool correlates a network operator's live routing state with their RPKI and ASPA data to produce a unified, real-time security posture. What is needed is the correlation layer that brings these together using the infrastructure operators already have. Fortunately, that layer can be built today, and its value is immediate.

The challenge: mature protocols, immature visibility

The incident record

The widespread nature of the problem is evident in the public record. In 2010, a major Asian carrier originated approximately 50,000 prefixes belonging to hundreds of other networks, routing a significant fraction of global internet traffic—including that of US government agencies—through its network for 18 minutes [1]. In 2018, a BGP route leak redirected traffic to a major internet platform through networks in West Africa and Asia, affecting global services for 74 minutes [2]. In 2024, Cloudflare's 1.1.1.1 DNS resolver was hijacked when a Brazilian ISP announced the prefix as its own, causing global DNS outages [3]. All three were detectable in principle using real-time data, but the tooling to detect them in real time did not exist in a usable form.

Figure 1. Timeline of significant BGP security incidents 2010–2025, annotated with attack class (origin hijack vs. route leak) and whether ROV or ASPA enforcement would have prevented each. Source: BGPStream, CAIDA [4] and public incident records.



RPKI ROV: necessary, but not sufficient

RPKI addresses the origin authentication problem. A ROA cryptographically binds a prefix to the AS authorized to originate it. Routers implementing ROV classify any received route as valid, invalid or notfound, and reject those classified as invalid. As of early 2026, approximately 45–50% of the global routing table is covered by ROAs, and a growing number of operators have deployed ROV enforcement [5].

But ROV does not catch route leaks. A route leak is not origin fraud—the originating AS is legitimate, and the prefix matches a valid ROA. What is wrong is the path: the route has propagated in a direction inconsistent with the customer-provider relationships declared by the involved networks. ROV is blind to this, and ROV enforcement at 100% deployment would not have prevented the multi-hour global service disruptions that dominated BGP incident reporting in 2018 and 2019 [6].

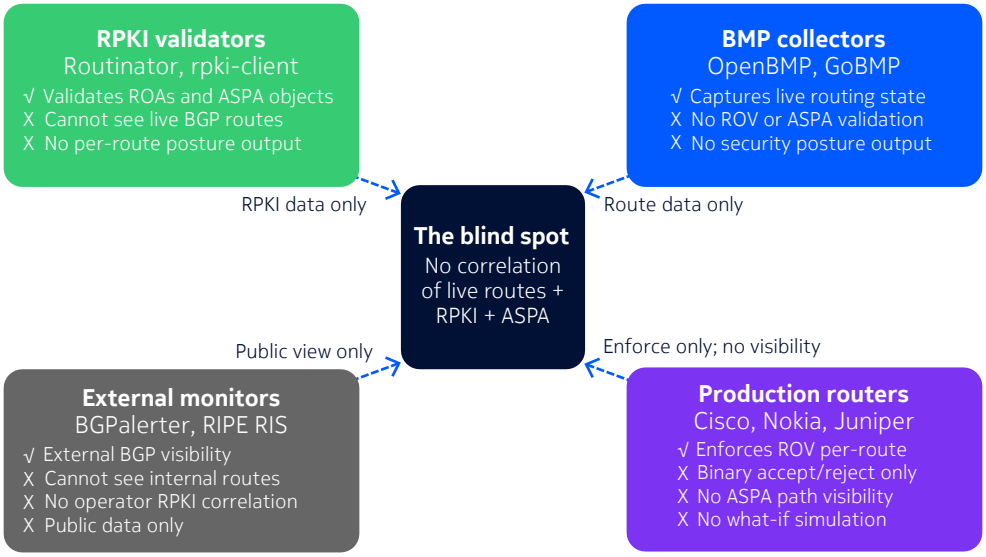
ASPA: the missing piece

ASPA extends BGP path security to detect route leaks. An ASPA object, registered with a RIR, declares the set of Autonomous Systems authorized to provide transit to that operator. A router implementing ASPA verification walks an AS_PATH hop by hop, and if a route leak produces a path that violates declared provider authorizations, ASPA detects it. ASPA objects are now registerable at ARIN and RIPE NCC, with APNIC and LACNIC planned for 2026. Routinator supports ASPA validation and delivers ASPA data via RTRv2. The foundational infrastructure exists, but adoption sits at less than 1% of the global ASN space [7], primarily because operators cannot answer the basic question of what ASPA enforcement would actually do on their network before committing to it.

The tooling gap

The routing security ecosystem has mature but siloed components. RPKI validators know whether a ROA is valid, but cannot see whether any router is currently receiving a route that violates it. BMP collectors know exactly what routes every router is receiving, but cannot tell whether any of those routes fail RPKI or ASPA validation. External monitors provide a useful view of publicly visible events, but cannot see inside an operator's routing table. Production routers enforce ROV, but their decisions are binary and opaque—there is no mechanism to ask, "What would happen if I deployed reject-invalid today?"

Figure 2. The siloed landscape of routing security tools. Each component holds a piece of the picture, but none correlates to the full view. The gap between them is the blind spot.



No existing tool answers the fundamental operator question: *What is my routing security posture right now, and what would change if I deployed enforcement?* This is the blind spot.

The solution: routing security as an observability problem

BMP as security telemetry

The BGP Monitoring Protocol (RFC 7854) gives network management systems a real-time view of a router's BGP state. A BMP-capable router streams every BGP UPDATE it receives—pre-policy, post-policy or both—in near real-time. Most modern routers from major vendors natively support BMP, but most operators who have BMP configured use it for traffic engineering or topology visibility, not security analysis. For security analysis, the pre-policy Adj-RIB-In is the most valuable feed—it shows what peers are actually sending, unmodified by local import policy, where security anomalies first appear.

BMP is the routing security telemetry interface that operators already have, and largely do not use for security.

Closing the loop: the correlation architecture

Closing the observability gap requires three components, all of which exist today. A BMP receiver parses routers' streaming route updates into structured route objects. An RTR client synchronizes validated ROA payloads and—via RTRv2—ASPA payloads from an RPKI validator in real time. A validation engine annotates each route with ROV state per RFC 6811 and ASPA state by walking the AS_PATH hop-by-hop, producing the combined security posture shown in Table 1.

Table 1. Combined ROV × ASPA security posture

ROV State	ASPA State	Security Posture	Interpretation
Valid	Valid	Secured	Origin and path fully verified. Highest confidence.
Valid	Unknown	Origin-Only	Origin verified; path not verifiable due to ASPA coverage gap. Common during early adoption.
Valid	Invalid	Path-Suspect	Legitimate origin, path inconsistent with declared provider relationships. Possible route leak.
Not Found	Valid	Path-Only	Path is clean; origin AS has not registered ROAs.
Not Found	Unknown	Unverified	No RPKI coverage. The status quo for much of the internet today.
Not Found	Invalid	Path-Suspect	No origin coverage and path violates ASPA. High suspicion.
Invalid	Any	Origin-Invalid	Origin fails ROV. Should be rejected under the enforce-invalid policy.

When the RTR client receives updated RPKI data—such as a VRP withdrawn, or an ASPA object changed—the engine immediately identifies every route in the table affected by that change and re-validates them, emitting state-change events for any route whose posture transitions. Dashboards update and alerts fire. The routing security posture reflects reality in real time.

Observability before enforcement

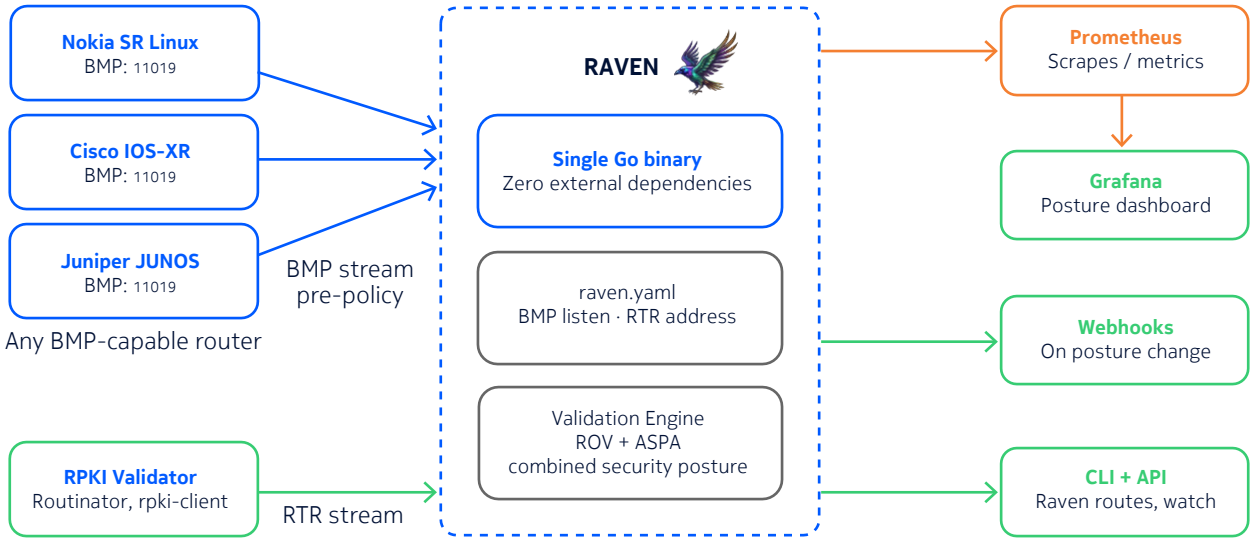
An operator does not need to wait for their router vendor to ship ASPA support, or for their network to complete an RPKI ROV deployment, to gain routing security visibility.

That's because BMP is already supported, RTR is already running, and the data is already there. Deploying the correlation layer provides immediate value even in networks that have not yet deployed any enforcement policy. A network can measure its routing security posture today, identify routes most affected by enforcement, simulate the impact of deploying reject-invalid or ASPA enforcement against live data without touching a single router configuration, and build the operational confidence necessary to move toward enforcement on a measured timeline.

RAVEN: a reference implementation

The architecture described in this paper is implemented in Routing Analysis, Validation, and Event Network (RAVEN), an open-source tool developed by Nokia and published on GitHub under the BSD-3-Clause license. RAVEN is a single Go binary that accepts BMP sessions from any BMP-capable router, connects to any RPKI validator via RTR, performs real-time ROV and ASPA validation, and exposes results through a CLI, Prometheus metrics and Grafana dashboards. It requires no infrastructure beyond the binary and a configuration file. A Containerlab-based demo environment is included for operators who want to evaluate the full stack on a laptop before connecting to production routers. RAVEN is a reference implementation, not a commercial product, and serves as a practical reference for the active IETF work documented in draft-wang-grow-bmp-rpki-mon-reqs [8].

Figure 3. RAVEN system overview. A single binary connects BMP feeds from routers and RTR from an RPKI validator, runs a real-time ROV and ASPA validation engine, and exposes results via CLI, Prometheus metrics and event-driven outputs, including webhooks and Grafana dashboards.



Business benefits: visibility before commitment

Reduced mean time to detection

The most direct operational benefit is reduced detection time for BGP hijacking and route leak events. Today, most operators learn of routing incidents from external sources—a customer complaint, a public monitoring alert or a peer notification—by which point traffic has already been affected for minutes or hours. With real-time BMP-based ROV and ASPA correlation, an operator receives an alert the moment an invalid-posture route appears in its routing table, before traffic is affected. Mean time to detection drops from minutes or hours to seconds. Because industry estimates place the average cost of a significant network security incident at hundreds of thousands to several million dollars [9], reducing detection time from hours to seconds can materially change the exposure profile.

A measured path to enforcement and peer engagement

ROV deployment has historically stalled at the “we know we should, but we are not sure what would break” stage. What-if simulation directly addresses this: an operator runs an impact analysis on their live routing table and receives a precise report of which routes would be dropped, which prefixes would be affected and which peers would be most impacted—converting a leap of faith into an evidence-based operational change. The same applies to ASPA: an operator can identify exactly which peers have not registered ASPA objects, quantify the coverage gap and engage those peers with data rather than assumptions. This turns ASPA deployment from a unilateral decision into a collaborative process.

Compliance and audit posture

Routing security is increasingly appearing in regulatory and audit frameworks for critical infrastructure operators. Several national cybersecurity frameworks now recommend or require RPKI ROV as a control for ISPs [10]. The ability to produce a real-time routing security posture report—covering every BGP-speaking router, peer and received route annotated with ROV and ASPA validation state—provides direct audit evidence that security controls are operational and effective. This capability does not exist in any other tool in the routing security ecosystem today.

Table 2. Operational benefits summary

Benefit	Without Observability	With BMP + RPKI + ASPA Correlation
Incident detection time	Minutes to hours (external notification)	Seconds (real-time posture change alert)
ROV enforcement decision	Qualitative judgment	Quantitative impact simulation
ASPA deployment planning	No data available	Coverage analysis, peer gap identification
Audit and compliance evidence	Manual sampling, no continuous monitoring	Real-time posture export, per-router reports
Peer engagement	Reactive	Proactive, data-driven

Conclusion

The routing security protocols needed to address BGP hijacking and route leaks are no longer theoretical. RPKI and ROV are deployed and effective against origin hijacking. ASPA, newly available at major RIRs, extends that protection to route leaks as well. The standards are mature, the validators are production-ready and router support is growing.

The blind spot is not a protocol gap—it is an observability gap. Closing it requires no new infrastructure, only the correlation layer that connects BMP telemetry and RPKI data operators already have. Nokia has built a reference implementation—RAVEN—to demonstrate that this architecture is practical, can be built with standard open-source components and is immediately useful.

Operators who instrument routing security observability today will be better positioned to respond to incidents, make evidence-based enforcement decisions and engage constructively with the ASPA ecosystem as it matures. Those who do not will continue to rely on external notifications of incidents that are, in principle, detectable from within their own network.

The infrastructure is present. The protocols are ready.
The missing piece—the observability layer—can be built today.

Abbreviations

ARIN: American Registry for Internet Numbers
ASN: Autonomous System Number
ASPA: Autonomous System Provider Authorization
BGP: Border Gateway Protocol
BMP: BGP Monitoring Protocol
IETF: Internet Engineering Task Force
LACNIC: Latin America and Caribbean Network Information Center

NOC:	Network Operations Center
RIPE NCC:	Réseaux IP Européens Network Coordination Centre
RIR:	Regional Internet Registry
ROA:	Route Origin Authorization
ROV:	Route Origin Validation
RPKI:	Resource Public Key Infrastructure
RTR:	Router-to-Cache (RPKI-Router Protocol)
SLA:	Service Level Agreement
VRP:	Validated ROA Payload

References

[1] BGPMon (2010). “Chinese BGP Hijack — Putting Things into Perspective.” https://www.bgpmon.net/chinese-bgp-hijack-putting-things-in-perspective/

[2] Cloudflare (2018). “How a Nigerian ISP Accidentally Knocked Google Offline.” Cloudflare Blog. https://blog.cloudflare.com/how-a-nigerian-isp-knocked-google-offline/

[3] Cloudflare (2024). “Cloudflare’s 1.1.1.1 DNS Resolver Incident.” Cloudflare Blog. https://blog.cloudflare.com/cloudflare-1111-incident/

[4] CAIDA BGPStream — open-source framework for live and historical BGP data analysis. https://bgpstream.caida.org/

[5] NIST RPKI Monitor, Q1 2026. https://rpki-monitor.antd.nist.gov/ and RIPEstat, RIPE NCC. https://stat.ripe.net/

[6] Sriram, K. et al. (2016). RFC 7908 — Problem Definition and Classification of BGP Route Leaks. IETF. https://datatracker.ietf.org/doc/rfc7908/

[7] ARIN and RIPE NCC ASPA registration statistics, Q1 2026. Available via RIR RPKI repositories and Routinator statistics endpoint.

[8] Wang, H. et al. “Requirements for BMP Extensions to Support RPKI-Based BGP Route Origin Validation.” IETF GROW WG, draft-wang-grow-bmp-rpki-mon-reqs. https://datatracker.ietf.org/doc/draft-wang-grow-bmp-rpki-mon-reqs/

[9] IBM / Ponemon Institute. “Cost of a Data Breach Report 2025.” IBM Security. https://www.ibm.com/reports/data-breach

[10] Sriram, K. and Montgomery, D. (2025). “Border Gateway Protocol Security and Resilience.” NIST Special Publication 800-189r1. https://csrc.nist.gov/pubs/sp/800/189/r1/ipd

About Nokia

Nokia is a global leader in connectivity for the AI era. With expertise across fixed, mobile, and transport networks, we’re advancing connectivity to secure a brighter world.

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: (June) CID215442