

# PRODUCT OVERVIEW — BGP Security Intelligence Platform

---

## 1. Title Page

**BGP Security Intelligence Platform**

**Predictive Routing Risk, ASN Vulnerability Analytics & Global BGP Threat Intelligence**

---

## Guide to This Document (How to Use This Overview)

This document provides a full strategic, architectural, and technical overview of the **BGP Security Intelligence Platform**, its capabilities, and its enterprise value.

**Section overview:**

### **Section 2 — Executive Summary**

What the platform is, what problem it solves, and what intelligence it produces.

### **Section 3 — The Problem: Routing Security in Today's Internet**

Why BGP remains structurally fragile and why current tools fail to provide predictive risk insight.

### **Section 4 — High-Level Solution Overview**

How the platform addresses these problems using multi-layer analytics and ML-driven risk modeling.

### **Section 5 — Platform Architecture (High-Level)**

End-to-end data flow: collectors, datastore, ML, and combined risk engine.

### **Section 6 — Core Components**

Detailed breakdown of analytic engines, collectors, ML models, and database structures.

### **Section 7 — Key Features & Capabilities**

Operational capabilities at a glance.

### **Section 8 — Unique & Proprietary Intelligence**

What the platform produces that does not exist elsewhere.

### **Section 8.1 — Origin-Side Vulnerability & Attack Propagation Risk**

Technical definition of ASN vulnerability and propagation tolerance.

### **Section 9 — Competitive Advantages**

Why this platform is unique in the market.

### **Section 10 — Real-World Use Cases**

### **Section 11 — Benefits for Operators & Security Companies**

Including a dedicated Noction-specific value section.

### **Section 12 — Integration & Deployment Options**

### **Section 13 — Summary & Next Steps**

---

## **2. Executive Summary**

The **BGP Security Intelligence Platform** is a next-generation system providing **predictive routing-risk analysis, origin-side ASN vulnerability assessment, and prefix-level structural risk modeling** across the global Internet.

The platform continuously collects and processes data from:

- BGP control-plane (RIS Live)
- RPKI validation systems
- IRR databases
- CAIDA AS-relationship datasets
- Multi-source prefix visibility measurements

This enables operators, network-security teams, and service providers to:

- identify systemic weaknesses in Internet routing,
- anticipate environments capable of enabling large-scale traffic redirection or BGP hijacking,

- evaluate the security posture and propagation tolerance of upstreams, peers, and customers.

The platform delivers predictive intelligence that does not exist in any commercial or academic system today.

---

## **3. The Problem — Routing Security in Today's Internet**

Border Gateway Protocol (BGP), the foundational routing protocol of the Internet, was not designed with modern threat models in mind.

### **3.1 No native authentication**

BGP relies on mutual trust between peers and lacks native cryptographic authentication for routing intent.

### **3.2 BGP hijacks remain a top-tier threat**

Misoriginations and leaks continue to cause:

- traffic interception
- traffic blackholing
- large-scale prefix misdirection

### **3.3 RPKI adoption remains partial**

Despite progress, a significant portion of global routing still depends on unvalidated or partially validated announcements.

### **3.4 Filtering practices vary widely across operators**

In practice, many networks still:

- do not enforce strict prefix filtering across all BGP sessions
- accept and propagate RPKI-invalid or unvalidated routes

- operate with incomplete, outdated, or inconsistent IRR data
- have not fully deployed RPKI-based Route Origin Validation (ROV)
- inadvertently create conditions under which hijacked or malformed origin traffic can propagate globally

### 3.5 Current monitoring tools fail to provide predictive intelligence

Most tools detect **incidents**, not **structural risk**.

Organizations cannot answer:

- Which ASNs operate in permissive routing environments?
- Which prefixes are structurally weak?
- Which ASN–prefix combinations create the highest real-world risk?
- Which routing behaviors implicitly enable propagation of invalid routes?

This platform addresses these unanswered questions.

---

## 4. High-Level Solution Overview (the core idea)

At its core, the platform answers one operational question:

“Which specific ASN–prefix pairs represent the most realistic, high-impact routing risk on today’s Internet?”

Let’s assume I am a network operator who owns a set of IP prefixes.

Some of these prefixes may be vulnerable to routing attacks.

An attacker does not necessarily need to operate from the same ASN as the vulnerable prefixes. In fact, the tool does not focus on cases where the attacker ASN and the victim prefixes legitimately match, because such scenarios are not representative of real-world hijack attacks. Instead, they can leverage a different ASN that exists in a very permissive routing environment, where false or malicious BGP announcements are likely to propagate.

The combination of:

- vulnerable prefixes, and
- a highly permissive (or poorly filtered) attacker ASN

can give an experienced attacker a high probability of successfully hijacking those prefixes.

This tool is designed to identify exactly these high-risk ASN–prefix combinations — cases where a hijack would not just be theoretically possible, but operationally likely to succeed.

Importantly, the tool does not stop at checking whether RPKI exists or not.

Even when RPKI is present, it does not automatically imply full protection.

Instead, it models and analyzes what would actually happen in practice if a BGP hijack were attempted, analyze how those environments actually behave in practice, and evaluates the real-world impact and likelihood of success.

And in the absence of RPKI, the success of a hijack can vary significantly depending on the surrounding routing environment.

This tool aims to capture and quantify that difference.

To do this, it models risk as the combination of two independent factors:

## **(1) Origin-Side ASN Vulnerability (Propagation Tolerance)**

An ASN is “vulnerable” when it may operate inside a **permissive routing environment**—meaning upstreams, peers, and surrounding networks are more likely to **accept and propagate weakly validated or unsafe origin behavior**.

In other words, this measures **how easily harmful announcements originated from that ASN can spread** under current real-world filtering and validation conditions.

## **(2) Prefix Structural Vulnerability**

A prefix is “vulnerable” when it is structurally weakly protected—e.g., missing or permissive ROAs, weak IRR anchoring, low validation strength, or abnormal visibility patterns—making it an attractive target for hijack, misdirection, and substitution.

## **Why the Platform Combines Them**

Real-world routing risk emerges when **a weak prefix is originated or handled within a permissive origin environment**.

Therefore, the platform produces a ranked list of the highest-risk ASN–prefix combinations on the global Internet by combining:

- **origin-side ASN vulnerability** (environment permissiveness & propagation tolerance)
- **prefix structural vulnerability**
- **RPKI / IRR correctness and coverage**
- **real-world propagation and visibility patterns**

By merging these independent layers, the system identifies which (*ASN*, *prefix*) pairs create the highest real-world routing risk, enabling operators and security teams to prioritize:

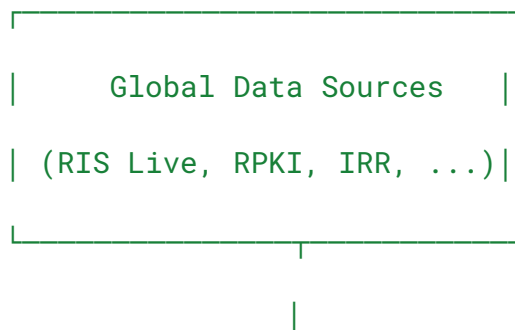
- filtering and mitigation
- customer and partner risk evaluation
- routing-policy hardening
- upstream/downstream trust decisions

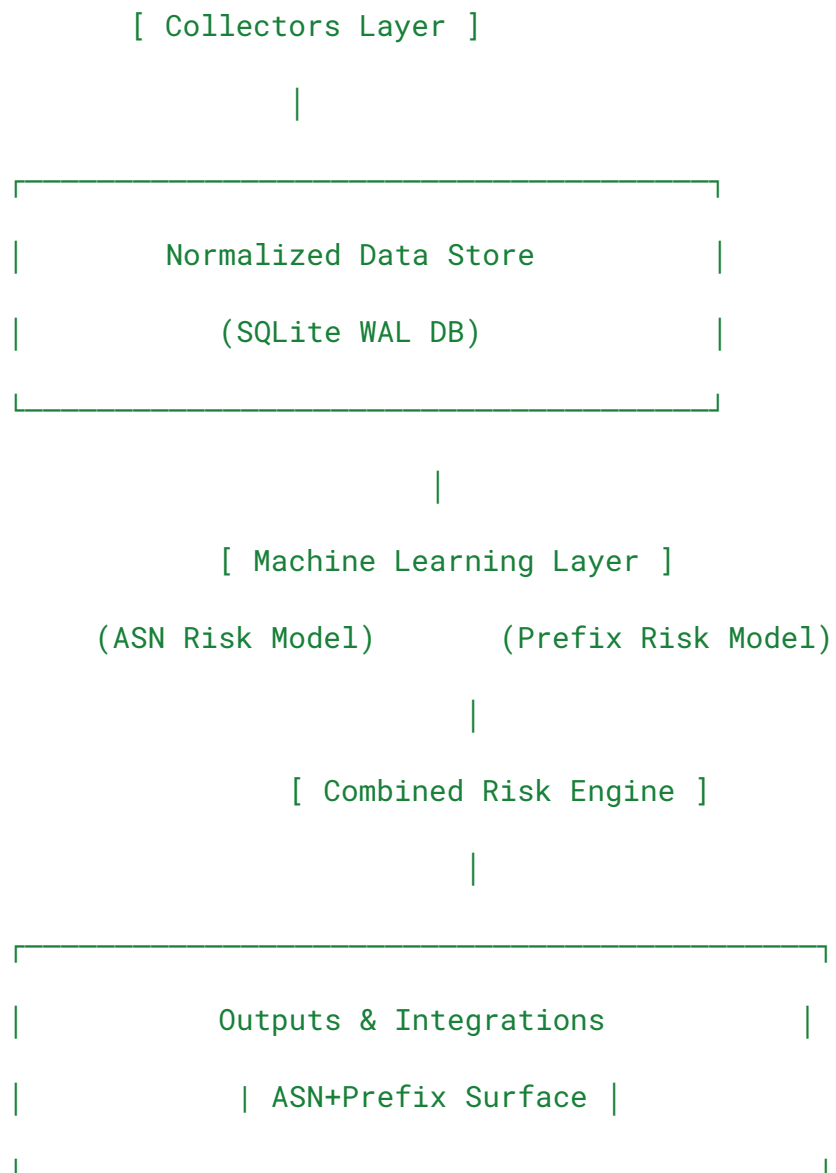
Each (*ASN*, *prefix*) combination represents a concrete model of how severe and how widely a malicious, hijacked, or malformed announcement would be likely to propagate across the Internet if originated under current routing conditions.

This combined risk-surface ranking is the platform’s most valuable output because it focuses on actionable, realistic propagation impact, not abstract or isolated scores.

---

## 5. Platform Architecture (High-Level)





---

## 6. Core Components

### 6.1 Data Collection Pipeline

ASN collectors:

- ASN discovery

- AS-path length metrics
- IRR object coverage
- Filtering strictness
- Reachability propagation
- CAIDA AS-relationships

**Prefix collectors:**

- Prefix discovery
- ROA presence & scope
- VRP counts
- IRR exact matches
- Prefix length classification
- Vantage-point visibility

Collectors run continuously with rate-limiting, retries, and persistence.

---

## **6.2 Machine Learning Layer**

### **ASN ML Model — Origin-Side Vulnerability**

Predicts:

- environment permissiveness
- filtering weakness
- tolerance to invalid routing behavior
- propagation-enabling characteristics

## **Prefix ML Model — Structural Vulnerability**

Predicts:

- hijack / misdirection susceptibility
- ROA / IRR weakness
- low-visibility anomalies

Both models use:

- LightGBM classification
  - auto-labeling heuristics
  - confidence estimation
- 

## **6.3 Combined ASN–Prefix Risk Engine**

This highlights:

- weak prefixes originated by permissive ASNs
  - high-impact routing attack surfaces
  - realistic vectors for large-scale routing disruption
- 

## **6.4 Database & Data Model**

Key tables:

- asn\_data
- rpki\_results
- irr\_results

- asn\_filter\_features
  - asn\_reachability\_propagation
  - asn\_rov\_score
  - asn\_rov\_dp
  - prefix\_data
  - prefix\_ml\_vuln
  - asn\_ml\_risk
  - asn\_prefix\_risk
- 

## 7. Key Features & Capabilities

- Global ASN origin-side vulnerability scoring
  - Prefix structural risk analytics
  - Combined ASN–prefix risk ranking
  - ML-based classification
  - Continuous intelligence generation
  - Autonomous operation
- 

## 8. Unique Intelligence

The platform uniquely unifies:

- ASN environment vulnerability

- prefix structural weakness
- real-world propagation behavior
- ML-driven combined risk modeling

No existing platform provides this depth of **predictive routing-risk intelligence**.

---

## 8.1 Origin-Side Vulnerability & Attack Propagation Risk

One critical and underestimated weakness in Internet routing is **origin-side propagation tolerance**.

In realistic threat models risk arises when:

- an attacker legitimately operates or controls an ASN (,has a BGP gateway), and
- the surrounding routing ecosystem is permissive enough to allow malformed or misleading announcements to propagate.

The platform therefore evaluates **how tolerant the environment around an ASN is** to unsafe origin behavior.

### Origin-Side Vulnerability Score

The platform quantifies:

- how permissive an ASN's surrounding routing environment appears,
- how widely announcements originated from that ASN are likely to propagate,
- how tolerant upstreams, peers, and downstreams are to weakly validated routing data.

Indicators include:

- filtering strictness
- RPKI / ROV enforcement

- IRR correctness
  - AS-relationship structure
  - misconfiguration patterns
  - invalid / unknown propagation behavior
- 

## Propagation Tolerance Assessment

The platform does **not** simulate attacks.

Instead, it infers propagation tolerance by observing how legitimate announcements from each ASN propagate and how strictly they are validated in practice.

---

## Most Vulnerable Prefix Identification

The prefix-level engine identifies structurally weak prefixes based on:

- absence or weakness of ROAs
  - permissive ROA maxLength
  - low VRP counts
  - weak IRR validation
  - low visibility
- 

## Combined Origin + Prefix Risk Surface

The platform merges:

- **ASN origin-side vulnerability**, and
- **prefix structural vulnerability**,

into a single ranked list of the most dangerous ASN–prefix combinations on the Internet.

---

## **9. Competitive Advantages**

- No comparable platform exists
  - Predictive, not incident-driven
  - ML at Internet scale
  - Combined ASN–prefix risk modeling
- 

## **10. Real-World Use Cases**

- Identifying risky customers or upstreams
  - Detecting permissive transit environments
  - Preventing traffic misdirection
  - Risk-aware peering decisions
  - Supply-chain routing security
- 

## **11. Benefits for Operators & Security Companies**

### **Operators:**

- Reduce routing exposure
- Detect weak peers
- Improve filtering hygiene

### Security Providers:

- Gain predictive routing-risk intelligence
- Enhance threat-intelligence products

### Cloud / CDN Providers:

- Reduce platform-wide routing risk
  - Evaluate tenants and partners
- 

## 12. Integration & Deployment Options

- APIs
  - Data exports (CSV / Parquet)
  - Dashboards
  - Periodic intelligence feeds
- 

## 13. Product Maturity & Validation Status

The BGP Security Intelligence Platform is currently delivered as an **advanced prototype / pre-production system**.

All analytics are computed on **live, real-world Internet routing data** (BGP control-plane, RPKI, IRR, and global visibility signals).

While the underlying methodologies and scoring logic are fully implemented and continuously exercised on global routing data, the platform **has not yet undergone long-term production deployment within a customer network environment**.

The next phase focuses on **operational validation, integration testing, and calibration within real customer workflows**, in partnership with an early adopter.

## 14. Summary

The **BGP Security Intelligence Platform** introduces a new category of **predictive routing-security intelligence**, enabling organizations to:

- understand global routing risk
- identify permissive environments
- predict exposure
- prioritize security investments
- protect infrastructure at Internet scale

This capability is **unavailable from any competitor today**.