Technical Proposal

*Online Operation and QoS Monitoring System for Fixed Broadband Service Providers*

# Table of Contents

*(Right-click and select 'Update Field' to refresh TOC in Word)*

Project Understanding Summary-2 (Technical Proposal)

**Project:** Online Operation and QoS Monitoring System for Fixed Broadband Service Providers

**Client:** Bangladesh Telecommunication Regulatory Commission (BTRC)

**EOI Reference:** 14.32.0000.000.400.07.0021.25.1685

**Bidder:** Telcobright + Comptech + OzoTech Joint Venture

# Executive Summary

## Why Telcobright + Comptech + OzoTech JV?

The Joint Venture of Telcobright, Comptech, and OzoTech presents the most compelling value proposition for BTRC's QoS Monitoring Platform. Each partner brings unique strengths that collectively address all EOI requirements.

### 1. Telcobright — Technical Lead

Telcobright assumes the technical lead for this project based on critical domain expertise. Our leadership team brings 20+ years of experience across MNOs, telecom vendors, large ISPs, and IIGs in Bangladesh and internationally.

**Core Competencies:**

* Telecom-grade monitoring systems (SS7/SIGTRAN, BGP, real-time traffic analysis)
* Big Data architecture (Kafka, Flink, Spark) handling millions of events per second
* QoS measurement methodologies aligned with ITU and APT standards
* Carrier-class platform development for regulatory and operator environments

**Proven Track Record — Specific Experience Summary:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Part** | **Project** | **Client** | **Key Highlights** |
| Part 1 | Common Interconnection SMS Platform (CISP) | AIOB (for all MNOs) | NMS/OSS platform with 42+ external integrations, SIGTRAN/SS7 signaling, multi-site HA (Borak/Khaza towers), BGP routing, real-time alerting |
| Part 2 | CDR Analyzer System (CAS) | BTRC Data Center | Analytics/QoS platform processing 400M+ CDRs/day, ASR/ACD metrics, integration with 42 softswitches (Huawei, ZTE, Nokia, Dialogic, etc.) |
| Part 3 | SMSC, Hosted Contact Center, Softswitch | BTCL, CCL (ISP) | SAS/BSS platforms with REST API, SIGTRAN, ERP/CRM (Dolibarr), Facebook/WhatsApp integration |

*Detailed documentation with screenshots, POs, and completion certificates provided in Specific Experience Response (Parts 1-3).*

### 2. Comptech — Infrastructure & Financial Strength

Comptech brings 10+ years of experience with a proven track record of large-scale ICT project delivery and significant PO value in Bangladesh.

**Key Strengths:**

* Hardware Deployment Expertise: Successful deployment of enterprise-grade hardware projects
* Hyper Converged Infrastructure (HCI): Proven experience in HCI deployment — a specific requirement mentioned in this EOI
* Cloud-based Software: Track record in cloud platform implementations
* Financial Guarantee: Strong financial capacity to support project execution and provide necessary guarantees
* ISO Certification: Holds required ISO certifications (ISO 9001, etc.)
* Company Experience: Exceeds the mandatory 5+ years company experience requirement

**Role in JV:**

* Infrastructure procurement and deployment
* Government sector liaison and compliance
* Training and capacity building
* Financial backing and project guarantees

### 3. OzoTech — Consultancy & Certified Network Engineers

OzoTech specializes in ICT consultancy and fills a critical gap in the EOI requirements: mandatory involvement of experienced and certified network engineers, names of the consultants are not included, but the following certifications will be matched.

**Certified Professional Team:**

|  |  |  |
| --- | --- | --- |
| **Certification** | **Description** | **Relevance to Project** |
| CCIE | Cisco Certified Internetwork Expert | Network architecture, ISP infrastructure, routing protocols |
| CISSP | Certified Information Systems Security Professional | Security architecture, compliance, data protection |
| CISA | Certified Information Systems Auditor | Audit, compliance, quality assurance |
| Additional | Cloud certifications (AWS, Azure), ITIL, PMP | Platform deployment, project management |

**Role in JV:**

* Network architecture design and validation
* Security assessment and compliance review
* Quality assurance and audit support
* Specialized consultancy for ISP integration

### JV Synergy Summary

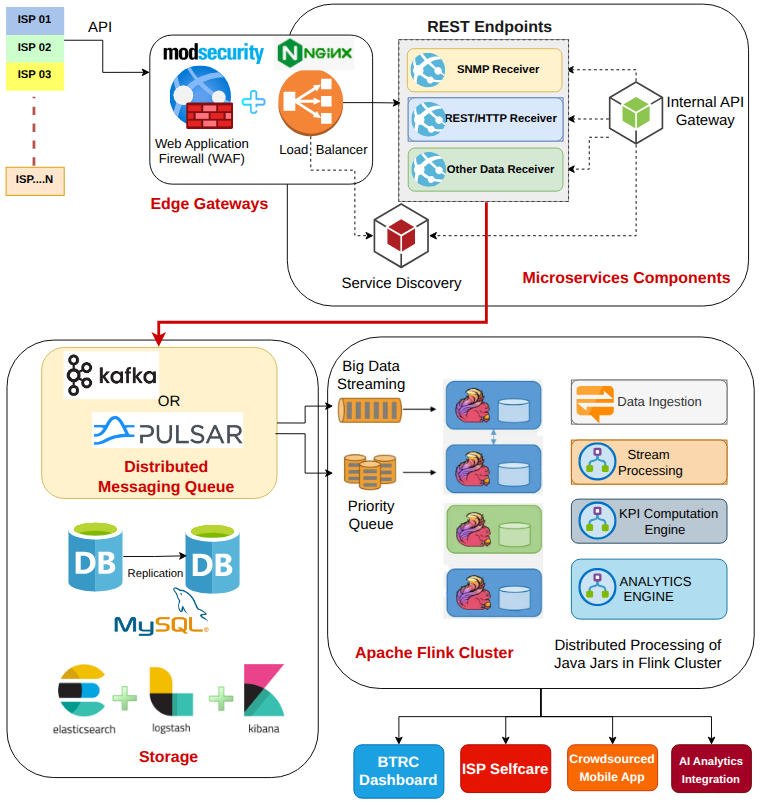
|  |  |  |  |
| --- | --- | --- | --- |
| **Capability** | **Telcobright** | **Comptech** | **OzoTech** |
| Technical Lead | ✓ |  |  |
| Platform Development | ✓ |  |  |
| Big Data / Analytics | ✓ |  |  |
| Telecom Integration | ✓ |  |  |
| Hardware Deployment | ✓ |  |  |
| HCI Experience | ✓ |  |  |
| Financial Strength | ✓ |  |  |
| ISO Certification | ✓ |  |  |
| Certified Engineers (CCIE/CISSP/CISA) | ✓ |  |  |
| Security Consultancy | ✓ |  |  |
| Government Experience | ✓ | ✓ | ✓ |

### Cost-Effective Innovation

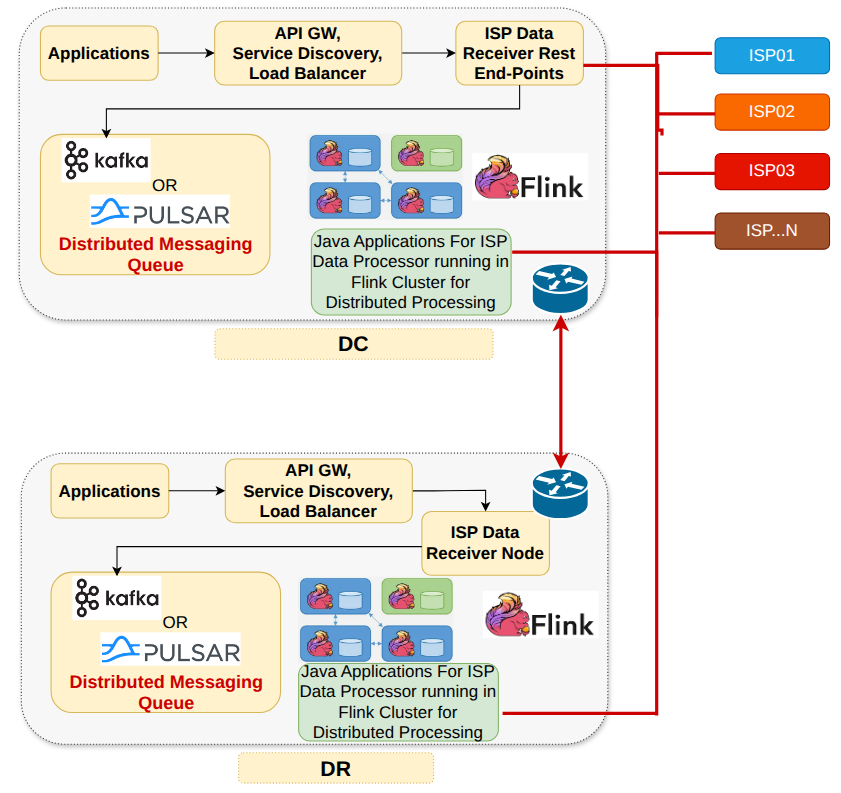
We propose open-source technologies (Kafka, Flink, Grafana, Keycloak) that eliminate vendor lock-in while reducing licensing costs. Our modular architecture allows BTRC to extend the platform independently.

# 2. Solution Architecture

## 2.1 Architecture Overview



*Figure: High-Level Architecture*



*Figure: DC/DR Architecture*

The proposed platform follows a distributed, event-driven microservices architecture designed for scalability, resilience, and real-time processing.

*[Diagram: architecture-high-level.drawio]*

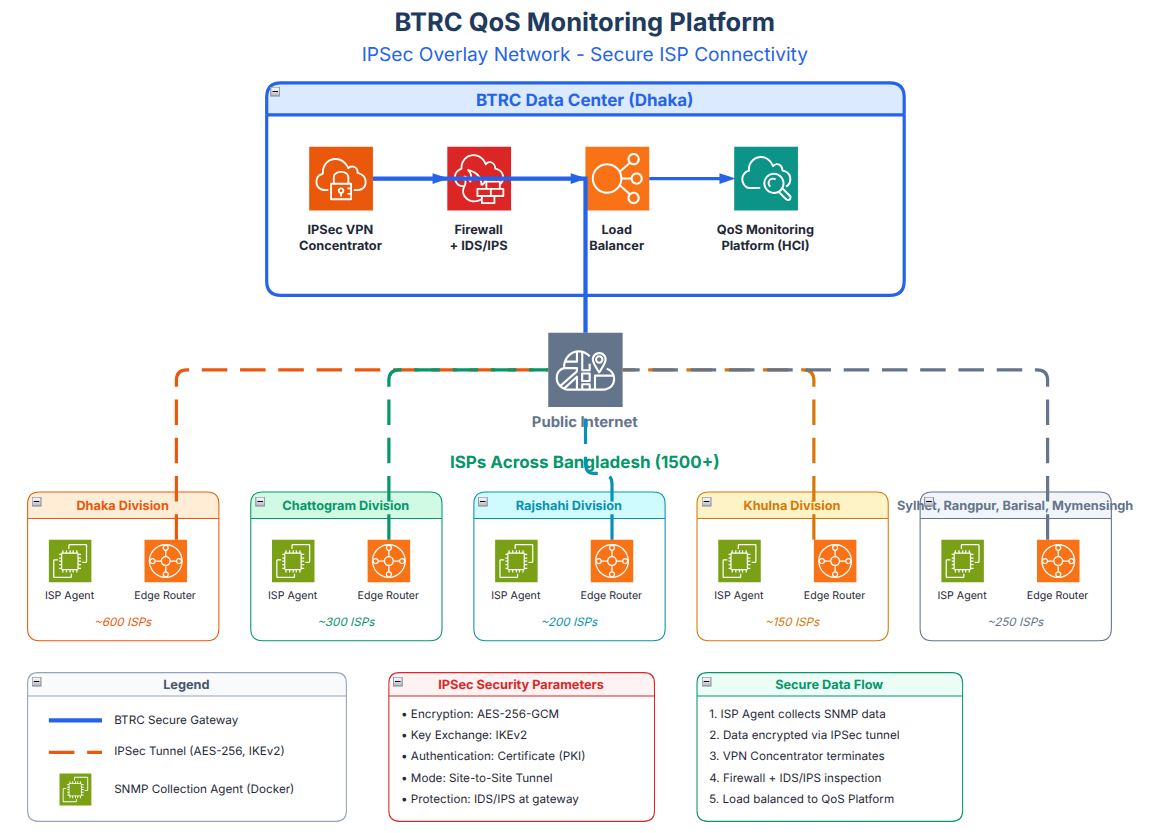
### Key Architectural Differentiators

|  |  |  |
| --- | --- | --- |
| **Differentiator** | **Description** | **Benefit** |
| Distributed Stream Processing | Apache Kafka + Flink for real-time event processing | Handle 1500+ ISPs, millions of metrics/sec, sub-second alerting |
| Multi-Protocol Data Collection | SNMP, REST API, gNMI support | Accommodate diverse ISP infrastructure |
| Time-Series Optimized Storage | TimescaleDB + ClickHouse | Efficient 1-year retention, fast analytical queries |
| Geographic-Aware Analytics | PostGIS integration | Division → District → Upazila → Thana drill-down |
| Zero-Trust Security Model | IPSec overlay + mTLS + RBAC | End-to-end encryption, defense in depth |

### Component Summary

|  |  |  |
| --- | --- | --- |
| **Layer** | **Components** | **Technology** |
| Data Ingestion | SNMP Collectors, API Gateway, Message Queue | Telegraf, Kong, Kafka |
| Processing | Stream Processing, KPI Computation, Anomaly Detection | Apache Flink |
| Storage | Time-Series, Analytics, Relational/Geo | TimescaleDB, ClickHouse, PostgreSQL+PostGIS |
| Application | Dashboards, Reports, Alerting | Grafana, Custom React |
| Security | Authentication, Authorization, Audit | Keycloak, RBAC, Audit Logs |
| Infrastructure | Container Orchestration, HCI | Kubernetes, HCI Cluster (5 nodes) |

## 2.2 Secure Network Connectivity: IPSec Overlay



*Figure: Secure IPSec Overlay Network*

A critical security requirement is secure data transport between ISP infrastructure and BTRC's central platform. We propose an IPSec overlay network for all ISP-to-BTRC communications.

### Network Security Architecture

┌─────────────────────────────────────────────────────────────────────┐  
│ BTRC Data Center │  
│ ┌─────────────┐ ┌─────────────┐ ┌─────────────────────────┐ │  
│ │ IPSec VPN │ │ Firewall │ │ QoS Monitoring │ │  
│ │ Concentrator│◄──►│ + IDS/IPS │◄──►│ Platform │ │  
│ └─────────────┘ └─────────────┘ └─────────────────────────┘ │  
└────────────▲────────────────────────────────────────────────────────┘  
 │ IPSec Tunnel (AES-256, IKEv2)  
 │  
 ┌────────┴────────┬─────────────────┬─────────────────┐  
 │ │ │ │  
┌───▼───┐ ┌───▼───┐ ┌───▼───┐ ┌───▼───┐  
│ ISP-1 │ │ ISP-2 │ │ ISP-3 │ │ISP-N │  
│ Router│ │ Router│ │ Router│ │Router │  
│+Agent │ │+Agent │ │+Agent │ │+Agent │  
└───────┘ └───────┘ └───────┘ └───────┘

*[Diagram placeholder: ipsec-overlay-network.drawio]*

### IPSec Configuration

|  |  |
| --- | --- |
| **Parameter** | **Specification** |
| Encryption | AES-256-GCM |
| Key Exchange | IKEv2 |
| Authentication | Certificate-based (PKI) or PSK |
| Tunnel Mode | Site-to-Site (ISP PoP to BTRC) |
| Intrusion Prevention | IDS/IPS at BTRC gateway |
| Logging | Full connection audit trail |

### Security Benefits

* Data Confidentiality: All SNMP/API traffic encrypted in transit
* Source Authentication: Only authorized ISPs can connect
* Intrusion Detection: Centralized IDS/IPS monitors all incoming traffic
* Tamper Protection: Integrity verification on all packets
* Audit Compliance: Complete connection and data logs

# 3. Core Modules & Features

## 3.1 Data Acquisition Layer

|  |  |  |
| --- | --- | --- |
| **Feature** | **Sub-Features** | **Process** |
| SNMP Collection | Interface stats, BRAS metrics, device health | Agent polls devices → Kafka → Flink → Storage |
| REST API Gateway | ISP data submission, package/subscriber data | ISP POST → Kong → Validation → Kafka → Storage |
| Automated Probes | Speed test, latency, DNS, traceroute | Scheduled probes → Results → Kafka → KPI Engine |

### Data Categories Collected

|  |  |  |
| --- | --- | --- |
| **Category** | **Data Points** | **Source** |
| Operational | Package definitions, subscriber counts, bandwidth capacity, POP locations | ISP API submission |
| QoS Metrics | Latency, packet loss, jitter, throughput, availability | SNMP + Probes |
| Revenue | Revenue by package/region, ARPU indicators | ISP API submission |
| Incidents | Outages, degradations, restoration times | ISP reports + Anomaly detection |

## 3.2 QoS Monitoring Module

|  |  |  |
| --- | --- | --- |
| **KPI** | **Measurement Method** | **Threshold Example** |
| Service Availability | SNMP polling + incident correlation | ≥99.5% uptime |
| Download Speed Ratio | Probe measurement vs advertised | ≥80% of advertised |
| Upload Speed Ratio | Probe measurement vs advertised | ≥80% of advertised |
| Network Latency (95th) | ICMP/TCP probes | <50ms domestic |
| Packet Loss | Network probes | <1% |
| Jitter | Continuous measurement | <30ms |
| DNS Resolution | DNS query timing | <100ms |
| Web Response Time | HTTP timing | <3s for standard pages |

## 3.3 Alerting & Notification

|  |  |  |
| --- | --- | --- |
| **Alert Type** | **Trigger** | **Notification** |
| Threshold Breach | KPI exceeds configured limit | Email, SMS, Dashboard |
| Anomaly Detection | Statistical deviation from baseline | Dashboard + Investigation queue |
| Outage Detection | Multiple metrics indicate service down | Priority alert + Escalation |
| Compliance Violation | Missed data submission deadline | ISP notification + BTRC alert |

## 3.4 Reporting & Analytics

|  |  |  |
| --- | --- | --- |
| **Report Type** | **Content** | **Frequency** |
| Executive Summary | National QoS overview, top/bottom ISPs | Daily, Weekly, Monthly |
| ISP Performance | Individual ISP KPIs, trends, compliance | On-demand, Monthly |
| Regional Analysis | Division/District breakdown | Monthly |
| Comparative Analysis | ISP benchmarking, ranking | Quarterly |
| Incident Reports | Outage analysis, root cause | Per incident |
| Custom Reports | User-defined parameters | On-demand |

# 4. ISP Selfcare Portal

A dedicated portal for ISP operators to manage their regulatory compliance, monitor their own performance, and interact with BTRC's QoS Monitoring Platform.

*Detailed feature specification: `isp-mon/ISP-PORTAL-FEATURES.md` (540 lines)*

*Screenshots: `isp-mon/ISP-Portal-Screenshots.docx`*

## 4.1 Portal Feature Areas (10 Modules)

|  |  |  |
| --- | --- | --- |
| **#** | **Module** | **Key Features** |
| 1 | Dashboard & Overview | Quick stats cards, compliance status widget, pending tasks, activity feed |
| 2 | Integration & Provisioning | Device registry, SNMP/Netflow config, API credentials, webhook setup |
| 3 | BGP Routing Management | Route table submission, prefix monitoring, RPKI validation, peering info |
| 4 | Security & Threat Center | DDoS attack reporting, BGP threat alerts, IP reputation, blocklist management |
| 5 | Alerts & Notifications | Alert dashboard, severity levels, notification preferences, escalation rules |
| 6 | Support & Ticketing | Ticket creation, tracking, categories, SLA monitoring |
| 7 | Data Submissions & Compliance | Submission calendar, monthly/quarterly forms, document repository |
| 8 | Incident Management | Network incident reporting, maintenance scheduling, timeline tracking |
| 9 | Reports & Analytics | QoS metrics reports, custom report builder, scheduled delivery |
| 10 | Settings & Configuration | Company profile, user management, security settings, notifications |

## 4.2 Device Management & SNMP Integration

|  |  |
| --- | --- |
| **Component** | **Details** |
| Device Registry | Add/Edit/Remove devices (Router, Switch, Firewall, Server, Probe) |
| Device Status | Active, Pending Approval, Suspended, Decommissioned |
| SNMP Config | v2c/v3 support, SNMPv3 SHA-256/AES-256, configurable polling intervals |
| Netflow/IPFIX | Flow export to BTRC collector, template configuration, sampling rates |
| API Integration | REST API key generation, rate limits, usage statistics, webhooks |

## 4.3 BGP & Security Features

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Route Table Upload | MRT format, CSV/JSON, scheduled auto-upload via API |
| RPKI Validation | ROA status tracking, Valid/Invalid/Unknown classification |
| Prefix Alerts | Unauthorized announcements, sub-prefix hijacking, route leaks |
| DDoS Reporting | Attack type, vectors, target IP, peak bandwidth, evidence upload |
| Threat Intelligence | BTRC-distributed indicators, industry threat sharing |
| Blocklist Management | Request/view IP/ASN blocks, BTRC approval workflow |

## 4.4 Alert Categories

|  |  |  |
| --- | --- | --- |
| **Category** | **Alert Types** | **Severity** |
| Security | DDoS attack, BGP hijack, route leak, suspicious IP activity | Critical/High |
| Network | Device offline, QoS threshold breach, high latency, packet loss | Critical/Medium |
| Compliance | Submission overdue, document expiring, submission reminder | High/Medium/Info |
| System | Data staleness, API rate limit approaching | High/Medium |

## 4.5 ISP Portal Process Flows

### 4.5.1 Data Submission Flow

ISP Login → Select Data Type → Upload/Enter Data → Validation  
 → Confirmation → BTRC Processing → Dashboard Update

### 4.5.2 Incident Reporting Flow

ISP Login → Report Incident → Location/Impact Details → Submit  
 → BTRC Acknowledgement → Status Tracking → Resolution Closure

### 4.5.3 BGP Route Update Flow

ISP Login → Upload BGP RIB → Validation → RPKI Check  
 → Anomaly Detection → Alert if Issues → Dashboard Update

### 4.5.4 DDoS Attack Reporting Flow

ISP Login → Report Attack → Type/Vector/Target → Evidence Upload  
 → BTRC Analysis → Threat Intelligence Feed → Industry Sharing (Optional)

# 5. User-Facing Applications

## 5.1 Mobile Speed Test App (Android/iOS/Web)

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Speed Test | Download/upload measurement to multiple servers |
| Latency Test | Ping to domestic and international endpoints |
| Jitter & Packet Loss | Advanced network quality metrics |
| Traceroute | Visual path display |
| History | Past test results with graphs |
| Location Tagging | GPS-based result mapping (with consent) |
| ISP Detection | Automatic identification of service provider |
| Feedback/Complaint | Optional submission to BTRC |

**Languages:** Bengali and English

## 5.2 BTRC Regulatory Tool

Internal measurement tool for BTRC officials with:

* Official measurement capability (evidentiary standard)
* Detailed logging for regulatory proceedings
* Scheduled automated testing
* Comparison with ISP-reported data

# 6. Dashboards & Visualization

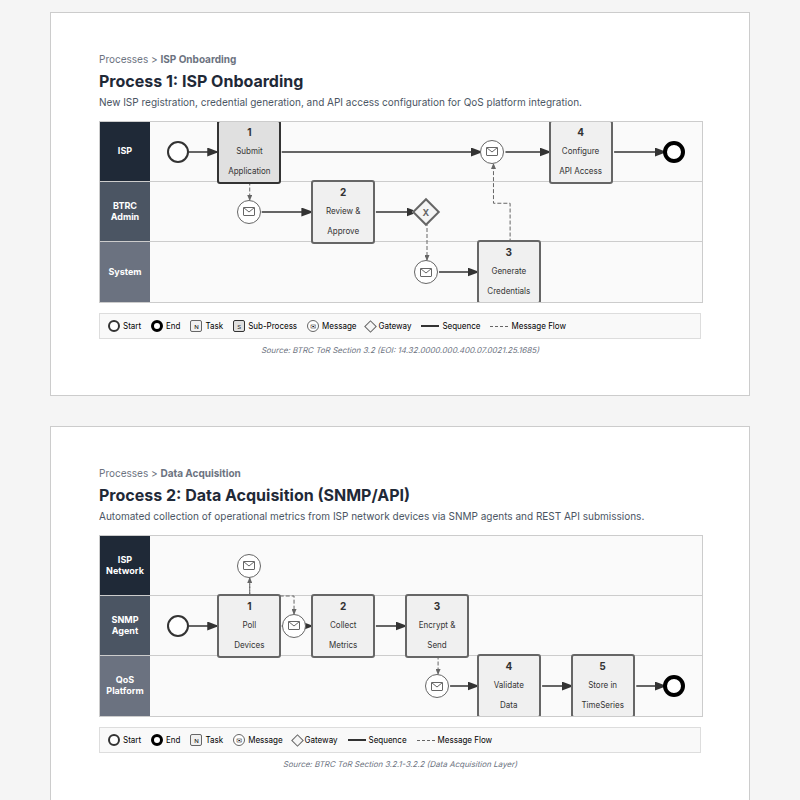
## 6.1 BTRC Executive Dashboard

|  |  |
| --- | --- |
| **Panel** | **Content** |
| National Overview | Map with ISP coverage, color-coded QoS |
| Top/Bottom ISPs | Ranked by key KPIs |
| Alert Summary | Active incidents, resolution status |
| Trend Charts | Historical KPI trends |
| Revenue Analytics | National revenue indicators |

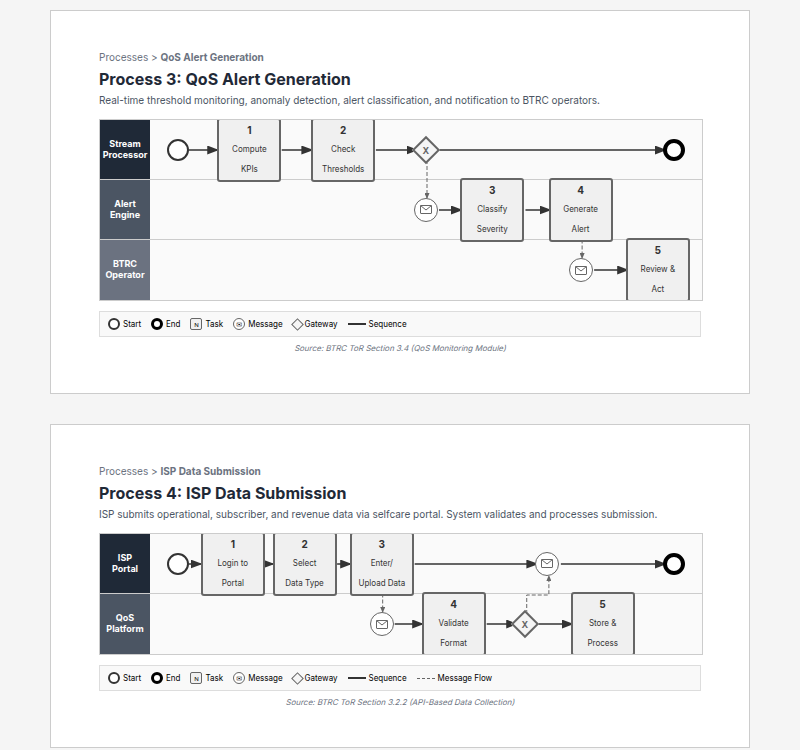
## 6.2 Operational Dashboard

|  |  |
| --- | --- |
| **Panel** | **Content** |
| Real-Time Metrics | Live KPI gauges |
| Data Collection Status | Agent health, submission status |
| System Health | Platform component monitoring |
| Recent Alerts | Chronological alert feed |

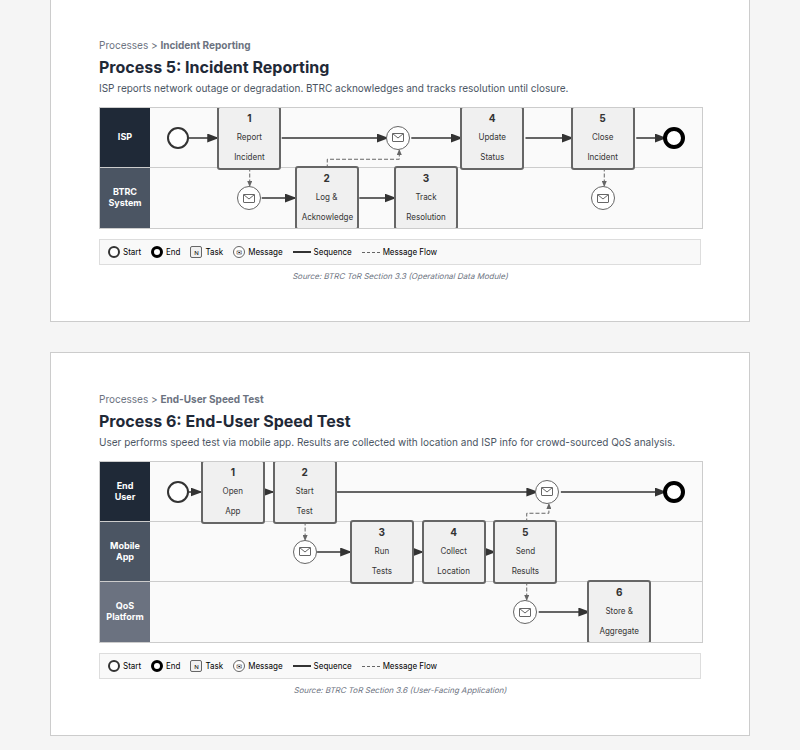
# 7. Process Flows (Summary)



*BPMN 1: ISP Onboarding Process*



*BPMN 2: Data Acquisition Process*



*BPMN 3: QoS Alert Generation Process*

|  |  |  |  |
| --- | --- | --- | --- |
| **Process** | **Trigger** | **Steps** | **Output** |
| Data Acquisition | Scheduled/Event | Collect → Validate → Transform → Store | Metrics in DB |
| KPI Computation | New data arrival | Aggregate → Calculate → Threshold check | KPI values, Alerts |
| Alert Generation | Threshold breach | Detect → Classify → Route → Notify | Notifications |
| Report Generation | Schedule/Request | Query → Aggregate → Format → Deliver | PDF/Dashboard |
| ISP Onboarding | New ISP registration | Register → Configure → Test → Activate | Active ISP account |

# 8. Limitations & Dependencies

## 8.1 Technical Limitations

|  |  |
| --- | --- |
| **Limitation** | **Mitigation** |
| SNMP polling interval (max 15 min) | Acceptable per ToR; can be reduced if needed |
| Encrypted traffic analysis | Flow telemetry provides metadata only (no DPI) |
| CPE monitoring excluded | Core/aggregation devices per ToR scope |

## 8.2 Dependencies on ISPs

|  |  |  |
| --- | --- | --- |
| **Dependency** | **Risk** | **Mitigation** |
| ISP cooperation for SNMP access | Medium | Regulatory mandate, phased rollout |
| Data submission accuracy | Medium | Validation rules, audit capability |
| Network connectivity | Low | IPSec with failover |

# 9. Requirements Traceability Summary

*Full requirements matrix: `submission/doc/requirement-matrices/TABLE-OF-CONTENTS.md`*

## 9.1 ToR Requirements Coverage

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Category** | **Req IDs** | **ToR Section** | **Count** | **Status** |
| Business Objectives | BO-001 to BO-007 | Section 2, p.1-2 | 7 | ✅ Covered |
| Data Acquisition - SNMP | DA-001 to DA-013 | Section 3.2.1, p.3-4 | 13 | ✅ Covered |
| Data Acquisition - QoS | DA-020 to DA-027 | Section 3.2.1, p.4 | 8 | ✅ Covered |
| Data Acquisition - API | DA-030 to DA-038 | Section 3.2.2, p.5-6 | 9 | ✅ Covered |
| Data Categories | DC-001 to DC-022 | Section 3.2.2, p.5-6, 9 | 22 | ✅ Covered |
| Legacy Migration | DM-001 to DM-004 | Section 3.2.5, p.7 | 4 | ✅ Covered |
| Operational Module | OP-001 to OP-004 | Section 3.3, p.7-8 | 4 | ✅ Covered |
| QoS Monitoring | QM-001 to QM-012 | Section 3.4, p.8-9 | 12 | ✅ Covered |
| QoS Features | QF-001 to QF-005 | Section 3.4, p.9 | 5 | ✅ Covered |
| Revenue Analytics | RA-001 to RA-007 | Section 3.5, p.9-10 | 7 | ✅ Covered |
| User Application | UA-001 to UA-009 | Section 3.6, p.10-11 | 9 | ✅ Covered |
| User App Data | UD-001 to UD-008 | Section 3.6, p.10-11 | 8 | ✅ Covered |
| Regulatory Tool | RT-001 to RT-007 | Section 3.7, p.11 | 7 | ✅ Covered |
| Data Storage/Dashboard | DS-001 to DS-008 | Section 3.8, p.12-13 | 8 | ✅ Covered |
| Platform Capabilities | PC-001 to PC-009 | Section 3.8, p.12-13 | 9 | ✅ Covered |
| Security & Compliance | SC-001 to SC-007 | Section 3.9, p.13 | 7 | ✅ Covered |
| Infrastructure (HCI) | IF-001 to IF-008 | Section 3.10.1, p.14 | 8 | ✅ Covered |
| Network Fabric | NF-001 to NF-004 | Section 3.10.1, p.15 | 4 | ✅ Covered |
| Load Balancer | LB-001 to LB-003 | Section 3.10.1, p.15 | 3 | ✅ Covered |
| Testing | TS-001 to TS-008 | Section 3.11, p.15-16 | 8 | ✅ Covered |
| Training | TR-001 to TR-005 | Section 3.12, p.16 | 5 | ✅ Covered |
| Support & Maintenance | SM-001 to SM-008 | Section 3.13/8, p.16,23 | 8 | ✅ Covered |
| Personnel | HR-001 to HR-014 | Section 5, p.19-21 | 14 | ✅ Covered |
| Deliverables | DL-001 to DL-005 | Section 6, p.21-22 | 5 | ✅ Covered |

## 9.2 SRS Document Mapping

|  |  |  |  |
| --- | --- | --- | --- |
| **SRS Section** | **Requirement IDs** | **ToR Section** | **Description** |
| SRS 3.1 | FR-DAQ-001 to FR-DAQ-033 | 3.2 | Data Acquisition Requirements |
| SRS 3.2 | FR-OPS-001 to FR-OPS-009 | 3.3 | Operational Module Requirements |
| SRS 3.3 | FR-QOS-001 to FR-QOS-016 | 3.4 | QoS Monitoring Requirements |
| SRS 3.4 | FR-REV-001 to FR-REV-012 | 3.5 | Revenue Analytics Requirements |
| SRS 3.5 | FR-APP-001 to FR-APP-015 | 3.6 | User Application Requirements |
| SRS 3.6 | FR-REG-001 to FR-REG-007 | 3.7 | Regulatory Tool Requirements |
| SRS 3.7 | FR-DSH-001 to FR-DSH-012 | 3.8 | Dashboard & Storage Requirements |
| SRS 3.8 | FR-SEC-001 to FR-SEC-008 | 3.9 | Security Requirements |

**Total Identified Requirements:** 190+ from ToR analysis

# 10. Value Additions (Optional Enhancements)

*The following enhancements are proposed as options for BTRC's consideration only. Implementation is subject to BTRC's explicit request, scope definition, and budget allocation during the RFP phase. These are not commitments but illustrations of potential platform extensibility.*

## 10.1 Flow Telemetry (NetFlow/IPFIX/sFlow) — Optional

*If BTRC determines that flow-level visibility would enhance regulatory oversight, the platform architecture can support integration with flow telemetry protocols.*

### The Fundamental Difference

|  |  |  |
| --- | --- | --- |
| **Aspect** | **SNMP (Core Requirement)** | **Flow Telemetry (Optional)** |
| What it sees | Interface totals (aggregate counters) | Individual conversations (per-flow) |
| Granularity | "Port 1 passed 500GB today" | "IP A sent 50MB to IP B on port 443" |
| Analogy | Water meter on building entrance | Individual apartment meters |

### Potential Regulatory Insights

|  |  |  |  |
| --- | --- | --- | --- |
| **Insight** | **SNMP** | **Flow** | **Potential BTRC Use** |
| Total bandwidth used | ✅ | ✅ | Capacity verification |
| Which interface is congested | ✅ | ✅ | Bottleneck identification |
| Which services dominate traffic | ❌ | ✅ | Subscriber usage patterns |
| Traffic to specific destinations | ❌ | ✅ | Top content providers |
| International vs domestic ratio | ❌ | ✅ | BDIX utilization, IIG capacity |
| Traffic anomalies by destination | ❌ | ✅ | Potential DDoS detection |
| Comparative fairness across destinations | ❌ | ✅ | Net neutrality indicators |

### Limitations (Acknowledged)

|  |  |
| --- | --- |
| **Cannot See** | **Reason** |
| Actual application within HTTPS | Encrypted traffic, same port |
| Content of traffic | No payload inspection (no DPI) |
| True latency/RTT | Not in standard flow export |

*Note: Flow telemetry implementation would require ISP cooperation and may involve additional infrastructure. Scope to be determined by BTRC.*

## 10.2 BGP Route Monitoring & Validation — Optional

*If BTRC wishes to extend regulatory visibility into routing security, the platform can potentially incorporate BGP monitoring capabilities. This addresses routing integrity—a layer not covered by traditional QoS metrics.*

### Potential Regulatory Value

|  |  |  |
| --- | --- | --- |
| **Capability** | **Description** | **Benefit** |
| Protect IP Space | Detect unauthorized announcements of Bangladesh prefixes | National security |
| Verify Routing Hygiene | Monitor ISP RPKI adoption | Compliance measurement |
| Identify Security Risks | Flag routes through high-risk jurisdictions | Risk awareness |
| Support Incident Response | Forensic data for routing disruptions | Investigation support |

### Data Collection Options (For BTRC Consideration)

|  |  |  |
| --- | --- | --- |
| **Option** | **Protocol** | **Suitability** |
| BMP (RFC 7854) | Real-time streaming | Modern routers (Cisco, Juniper, Huawei) |
| Passive BGP Peering | BGP session | Universal compatibility |
| Router API | REST/NETCONF | Legacy equipment, MikroTik |
| Hybrid | Combination | Diverse ISP landscape |

*The optimal approach would be finalized in consultation with BTRC during detailed design, if this module is requested.*

### Potential Detection Capabilities

|  |  |
| --- | --- |
| **Detection Type** | **Description** |
| RPKI Validation | Verify routes against cryptographic ROAs |
| Origin AS Anomaly | Detect unauthorized prefix origination |
| Sub-prefix Hijack | Identify more-specific announcements by foreign ASes |
| Route Leak Detection | Detect valley-free violations |
| Bogon Filtering | Verify ISPs reject reserved/private space |

### Open-Source Tools (If Implemented)

|  |  |  |
| --- | --- | --- |
| **Tool** | **Purpose** | **License** |
| BGPalerter | Hijack detection, RPKI validation | BSD (Free) |
| Routinator | Self-hosted RPKI validator | BSD (Free) |
| OpenBMP | BMP collector | Apache 2.0 (Free) |

*Note: Specific tools, data sources, and commercial integrations would be determined based on BTRC requirements and budget if this module is requested.*

## 10.3 AI-Assisted Analysis — Proposed

*The platform will integrate AI/ML capabilities to enhance data analysis and operator decision support.*

|  |  |  |
| --- | --- | --- |
| **Area** | **Capability** | **Data Sources** |
| Anomaly Detection | Identify unusual patterns in network metrics | SNMP, Flow telemetry |
| Threat Correlation | Correlate events from multiple sources | BGP feeds, threat intelligence APIs |
| Alert Prioritization | Score and rank alerts to reduce fatigue | Historical alert data |
| Operator Suggestions | Recommend investigation steps for detected issues | Pattern matching, knowledge base |

**Implementation Approach:**

* Leverages external analytics APIs or on-premise models based on BTRC preference
* Operator decisions remain human-driven; AI provides suggestions only
* Integrated into alerting and dashboard modules

*Flow Telemetry (10.1) and BGP Monitoring (10.2) are optional enhancements for BTRC's consideration. AI-Assisted Analysis (10.3) is included as a proposed platform capability.*

# 11. Mock UI Reference

Interactive mockups demonstrating proposed user interfaces have been developed using the isp-mon React application.

## 11.1 Available Mockup Screens

|  |  |  |
| --- | --- | --- |
| **Module** | **Components** | **Description** |
| BTRC Dashboard | BtrcDashboard/ | Executive overview, national KPIs |
| QoS Monitoring | QosMonitoring/ | Real-time metrics, threshold alerts |
| ISP Management | IspManagement/ | ISP registry, compliance tracking |
| ISP Portal | IspPortal/ | ISP selfcare interface |
| Reports | Reports/ | Report builder, templates |
| Speed Test | SpeedTest/ | End-user measurement interface |
| Alerts | Alerts/ | Alert management, notifications |
| Regional Filter | RegionFilter/ | Geographic drill-down |

## 11.2 Running the Mockups

cd isp-mon  
npm install  
npm start # Runs on configured port

*Screenshots and detailed UI documentation to be included in final submission.*

# 12. Submission Deliverables Checklist

|  |  |  |
| --- | --- | --- |
| **Document** | **Status** | **Notes** |
| Technical Proposal (This Document) | ✅ Draft | Architecture, features, process flows |
| Specific Experience Response Part 1 (CISP) | ✅ Complete | NMS/OSS, 42+ integrations |
| Specific Experience Response Part 2 (CAS) | ✅ Complete | Analytics, 400M+ CDRs/day |
| Specific Experience Response Part 3 (SAS/BSS) | ✅ Complete | CRM/ERP integration |
| High-Level Architecture Diagram | ✅ Complete | architecture-high-level.drawio |
| IPSec Network Diagram | ✅ Complete | ipsec-overlay-network.drawio |
| ISP Portal Features Spec | ✅ Complete | isp-mon/ISP-PORTAL-FEATURES.md (540 lines) |
| ISP Portal Screenshots | ✅ Complete | isp-mon/ISP-Portal-Screenshots.docx |
| Requirements Traceability | ✅ Complete | submission/doc/requirement-matrices/TABLE-OF-CONTENTS.md |
| Mock UI Screenshots | 🔲 Pending | isp-mon application ready |
| Value Addition Documents | ✅ Complete | BGP, Flow Telemetry |

*Document Version: Draft 2.0*

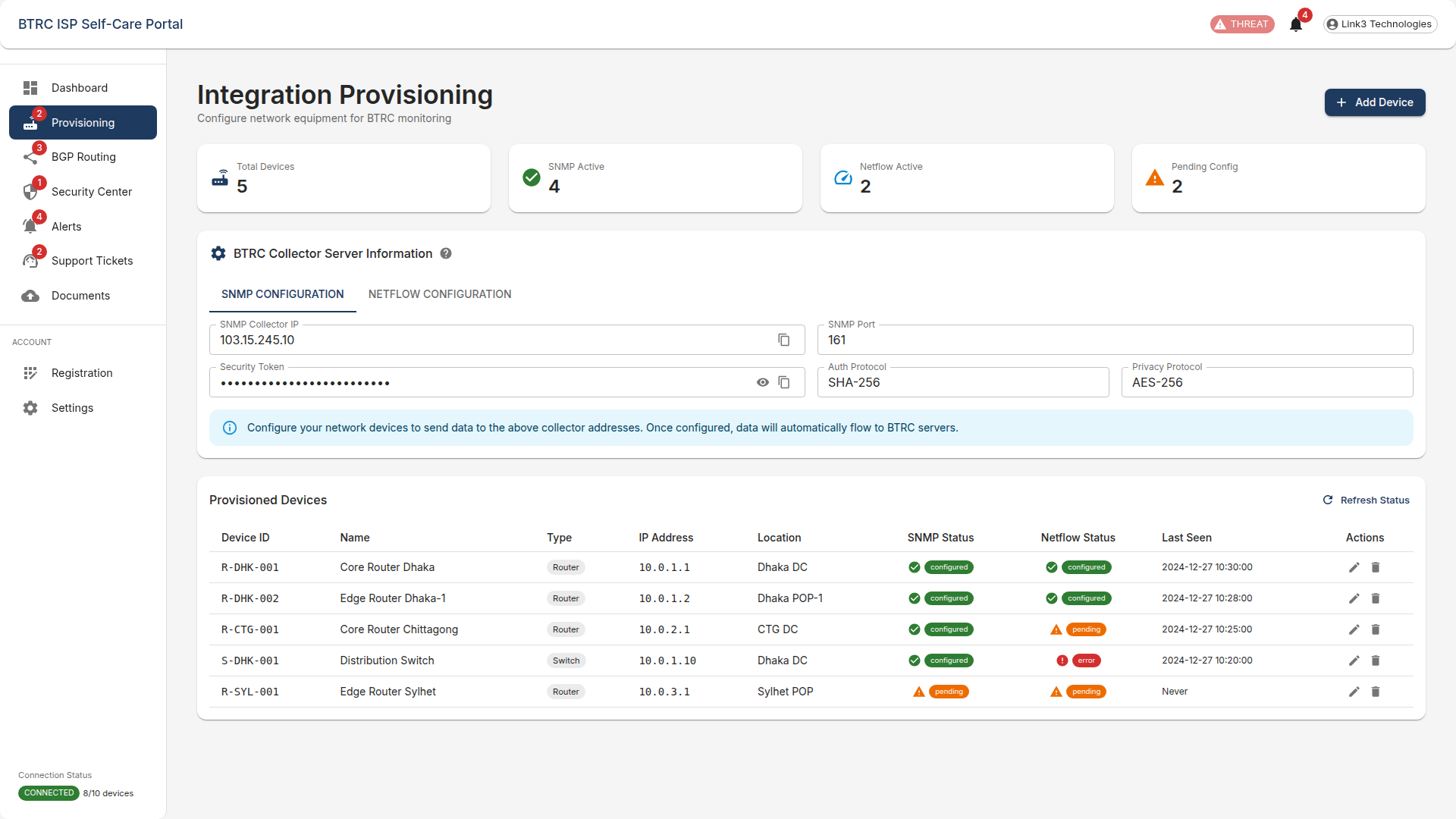
*Last Updated: December 2024*

# Appendix A: ISP Portal Mock UI Screenshots

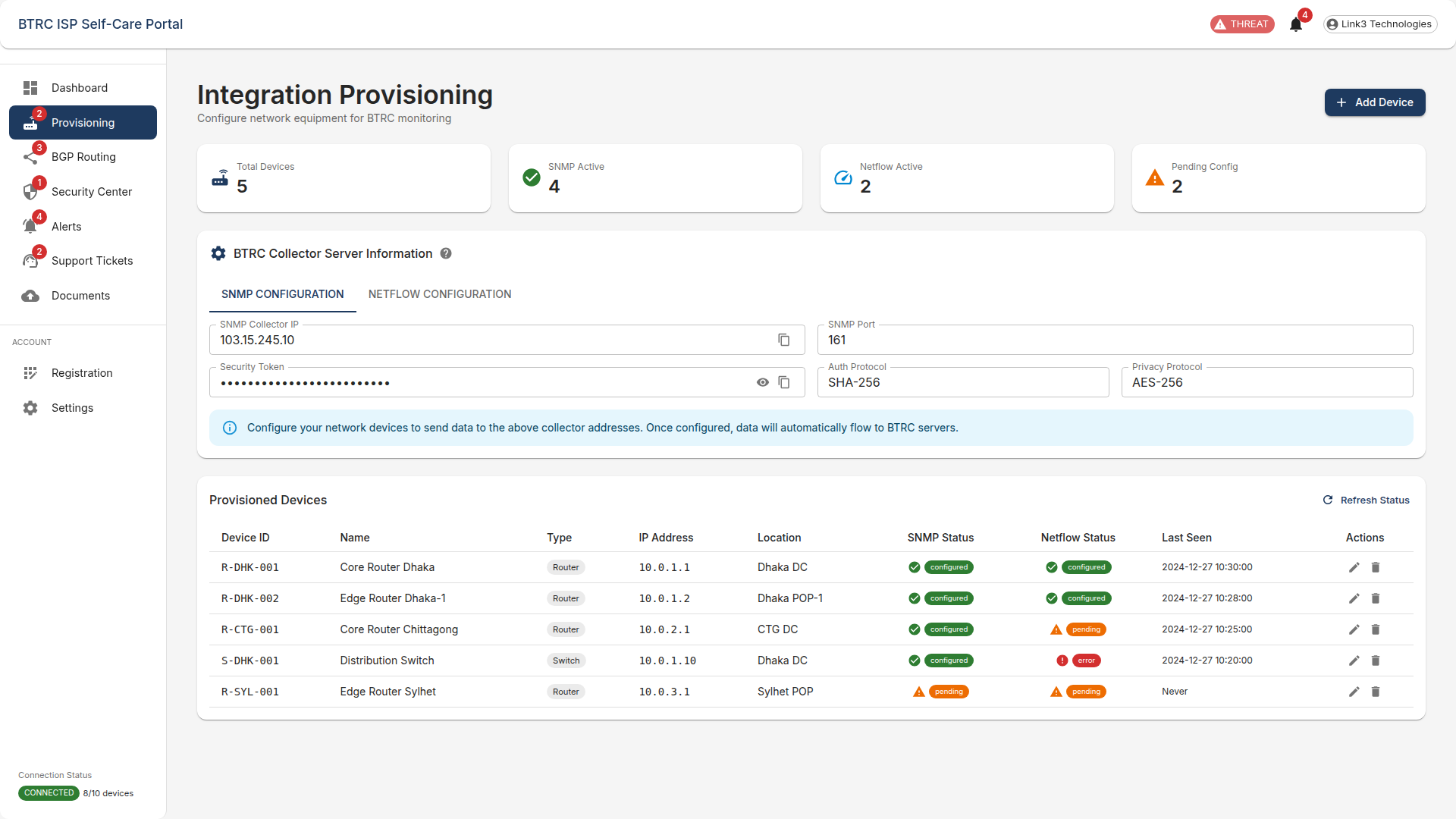
The following screenshots demonstrate the proposed ISP Selfcare Portal interface. *These mockups illustrate key features including dashboard, device management, BGP routing, security center, alerts, support ticketing, compliance submissions, incident management, and reporting modules.*



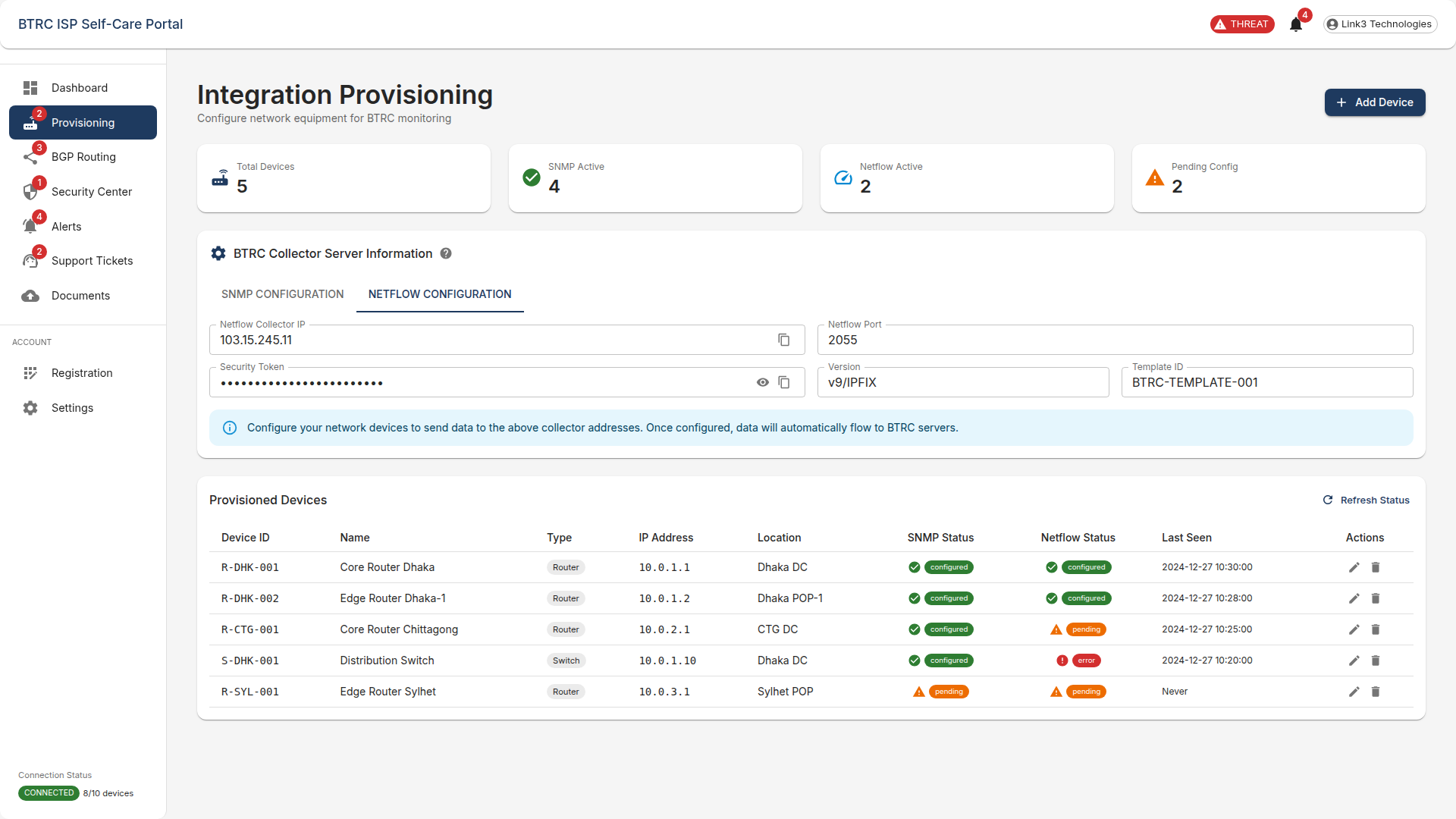
*Screenshot 1: ISP Portal Interface*



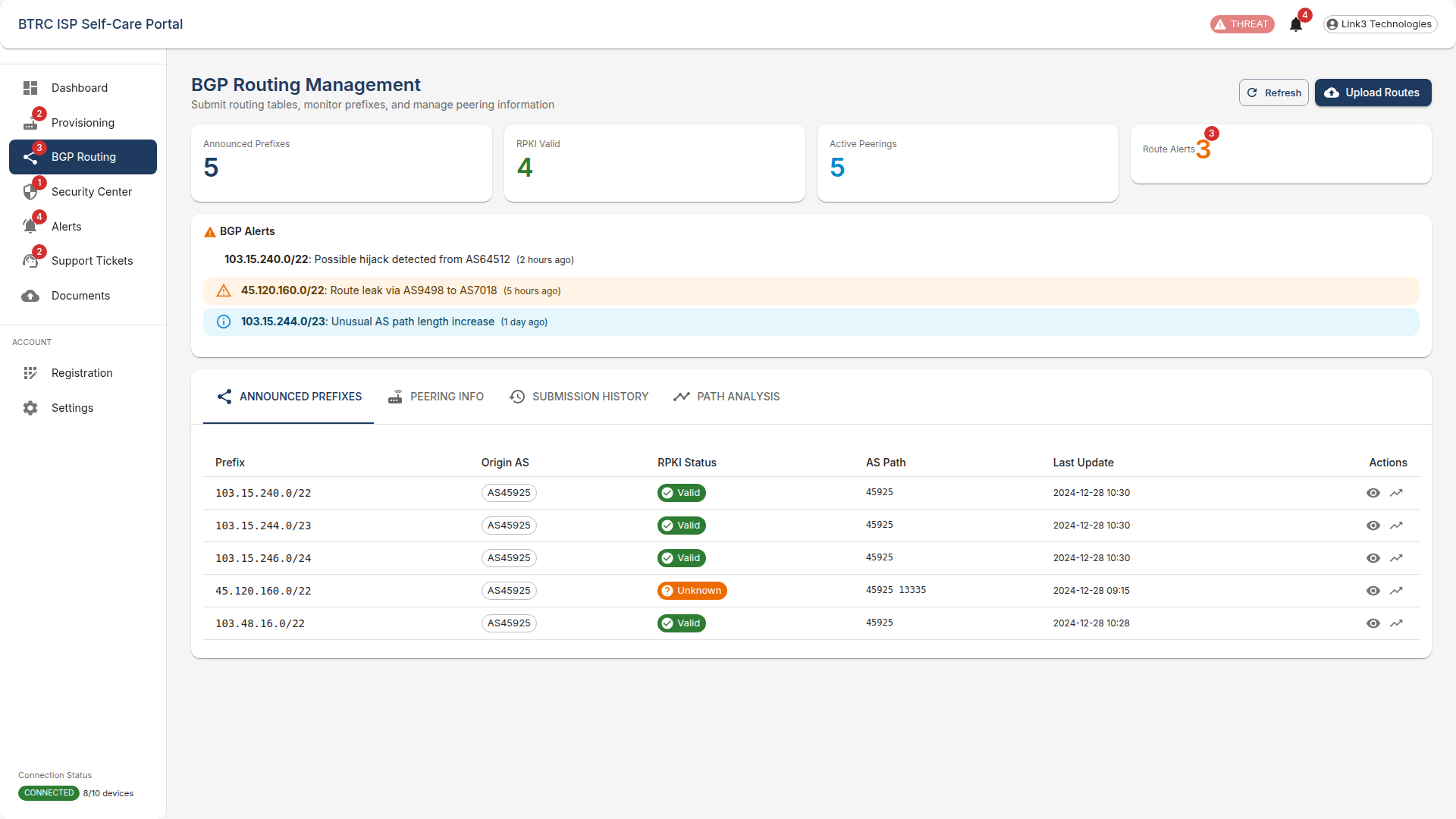
*Screenshot 2: ISP Portal Interface*



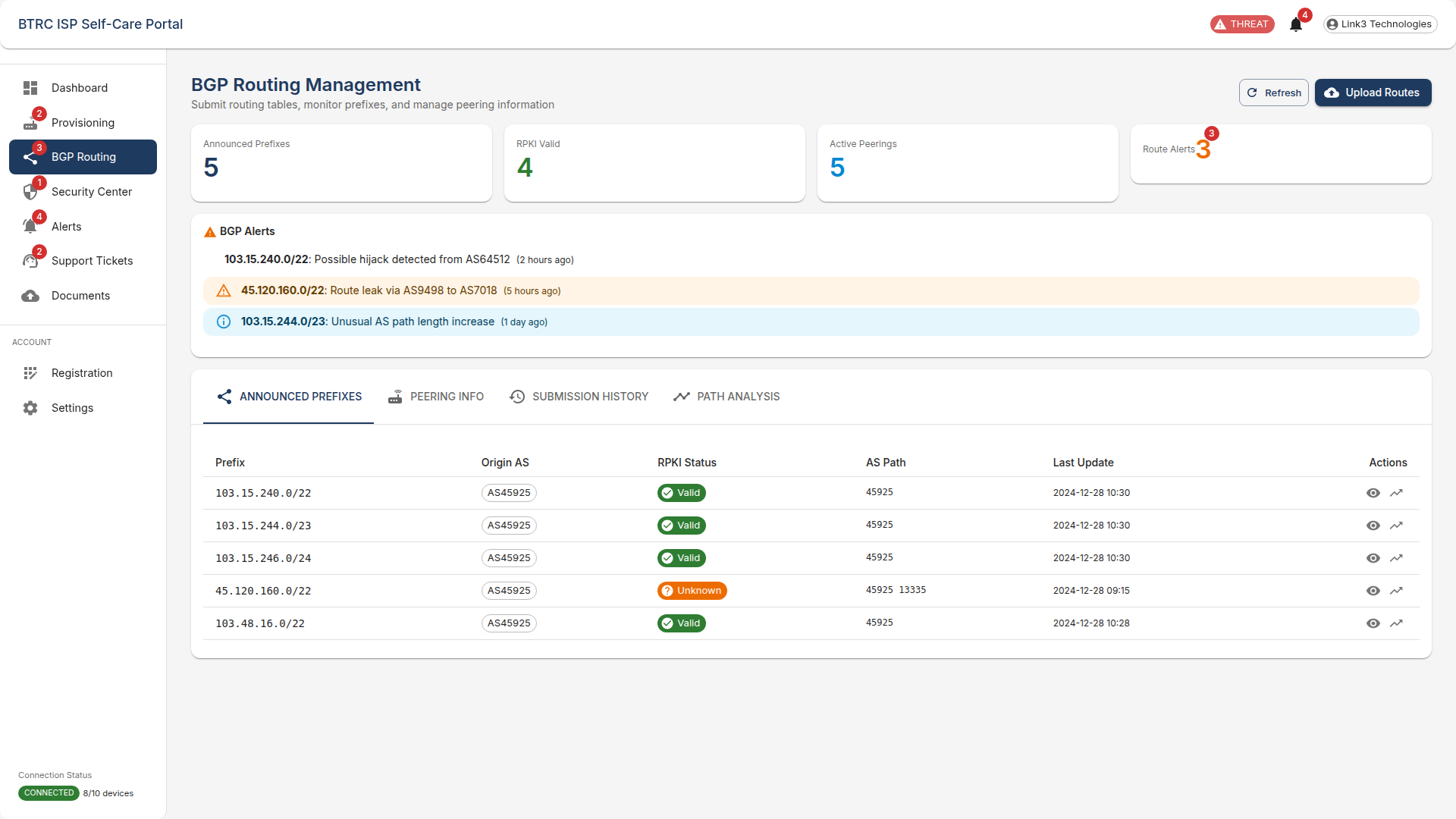
*Screenshot 3: ISP Portal Interface*



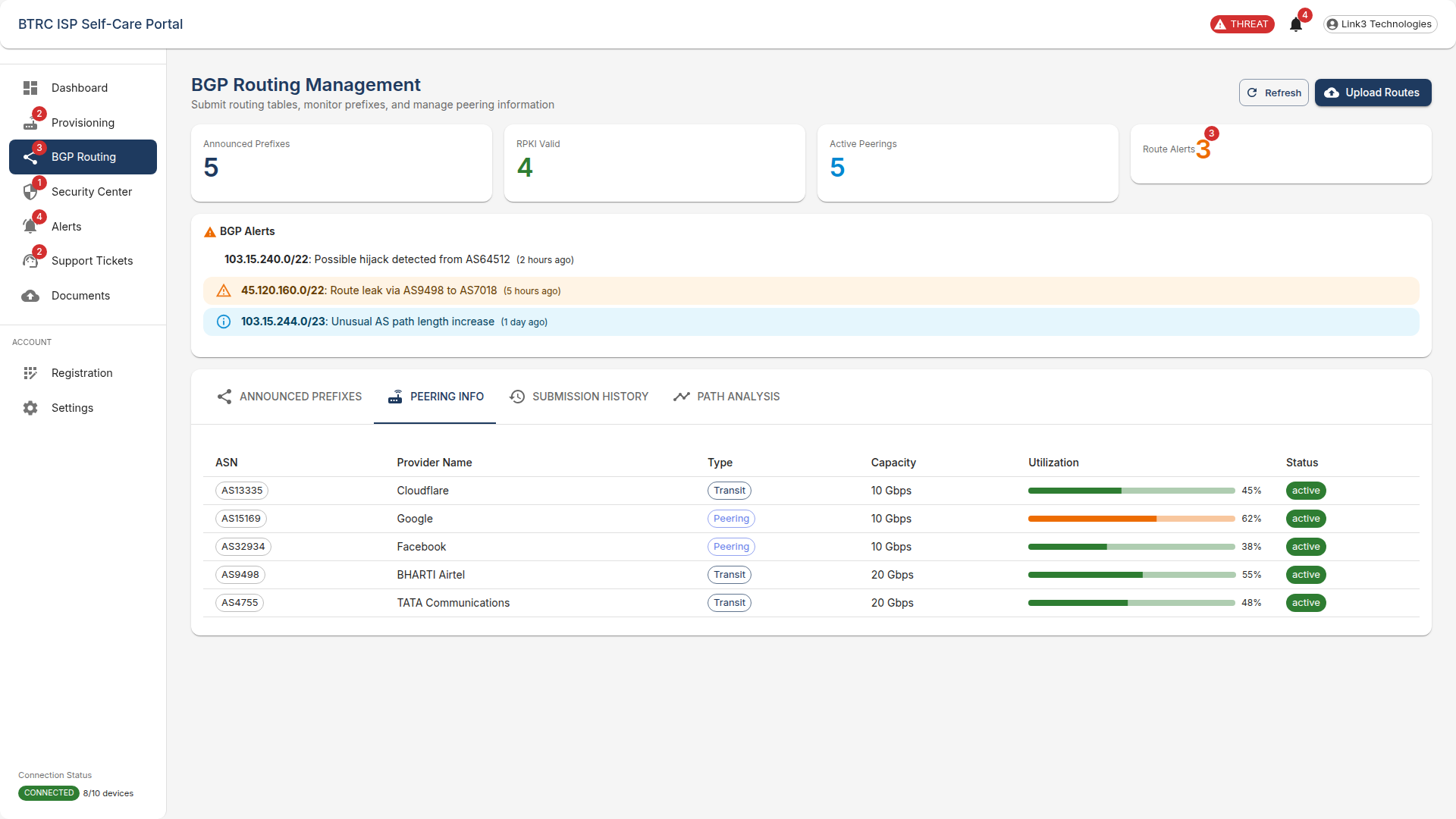
*Screenshot 4: ISP Portal Interface*



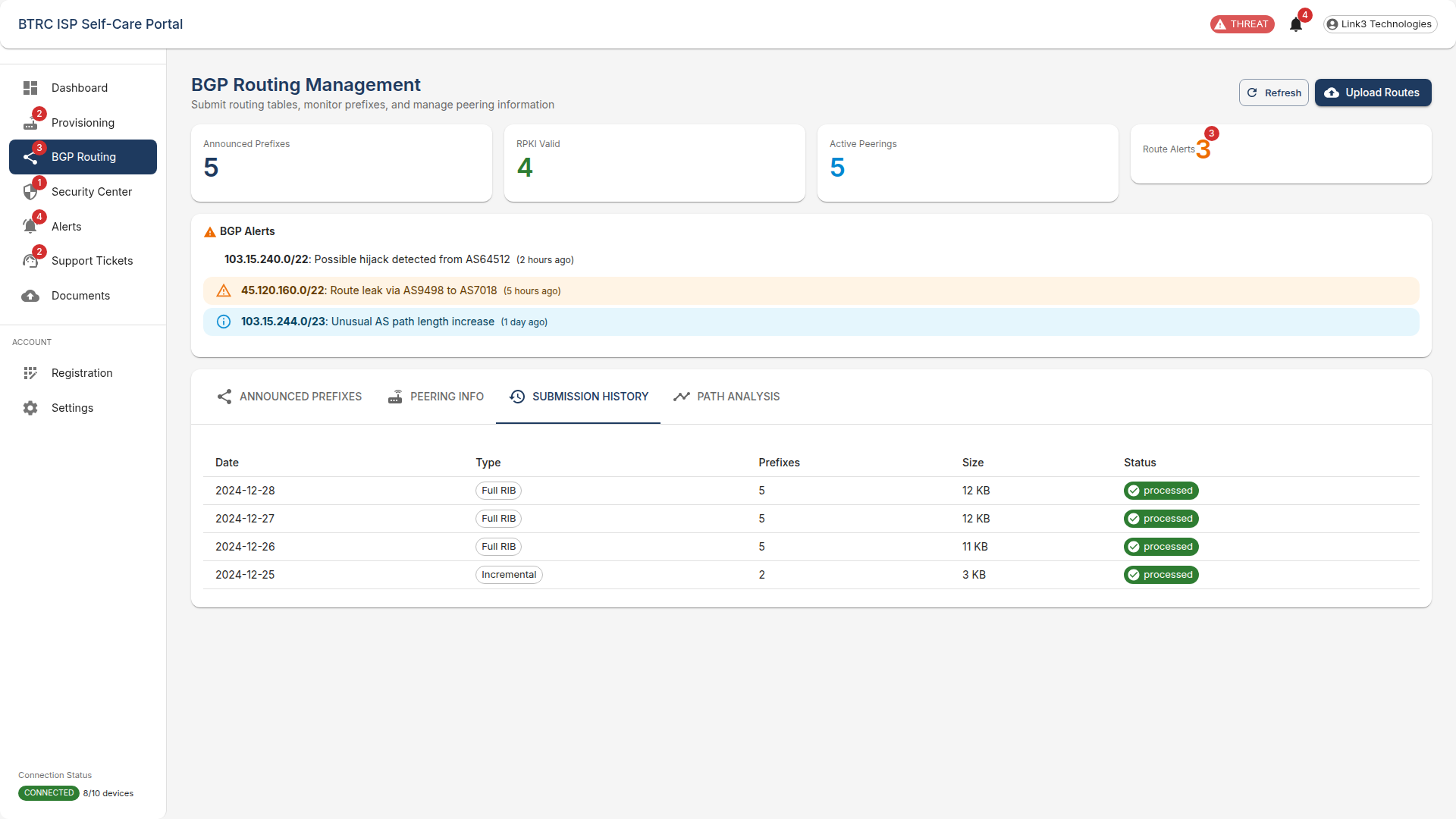
*Screenshot 5: ISP Portal Interface*



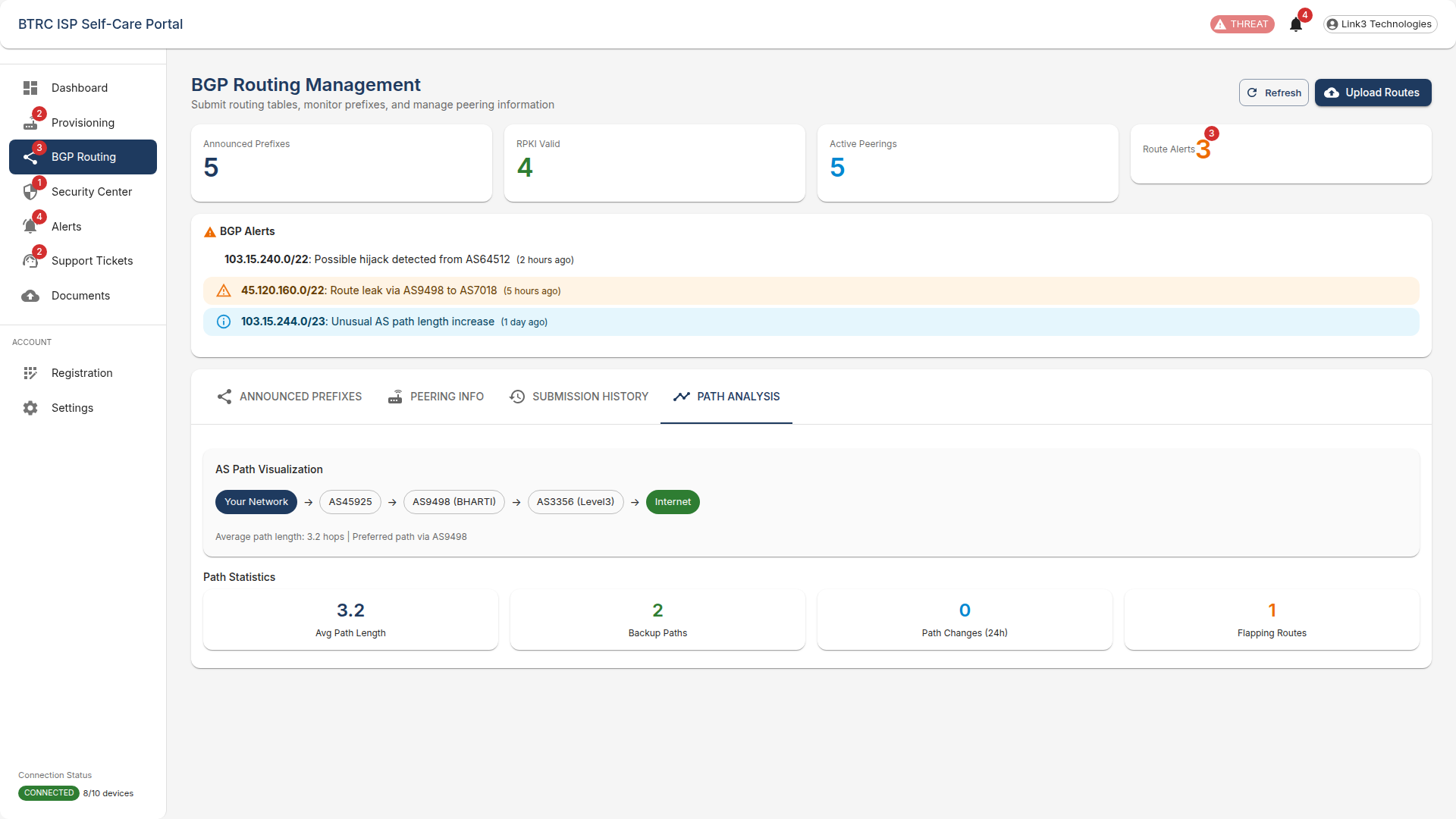
*Screenshot 6: ISP Portal Interface*



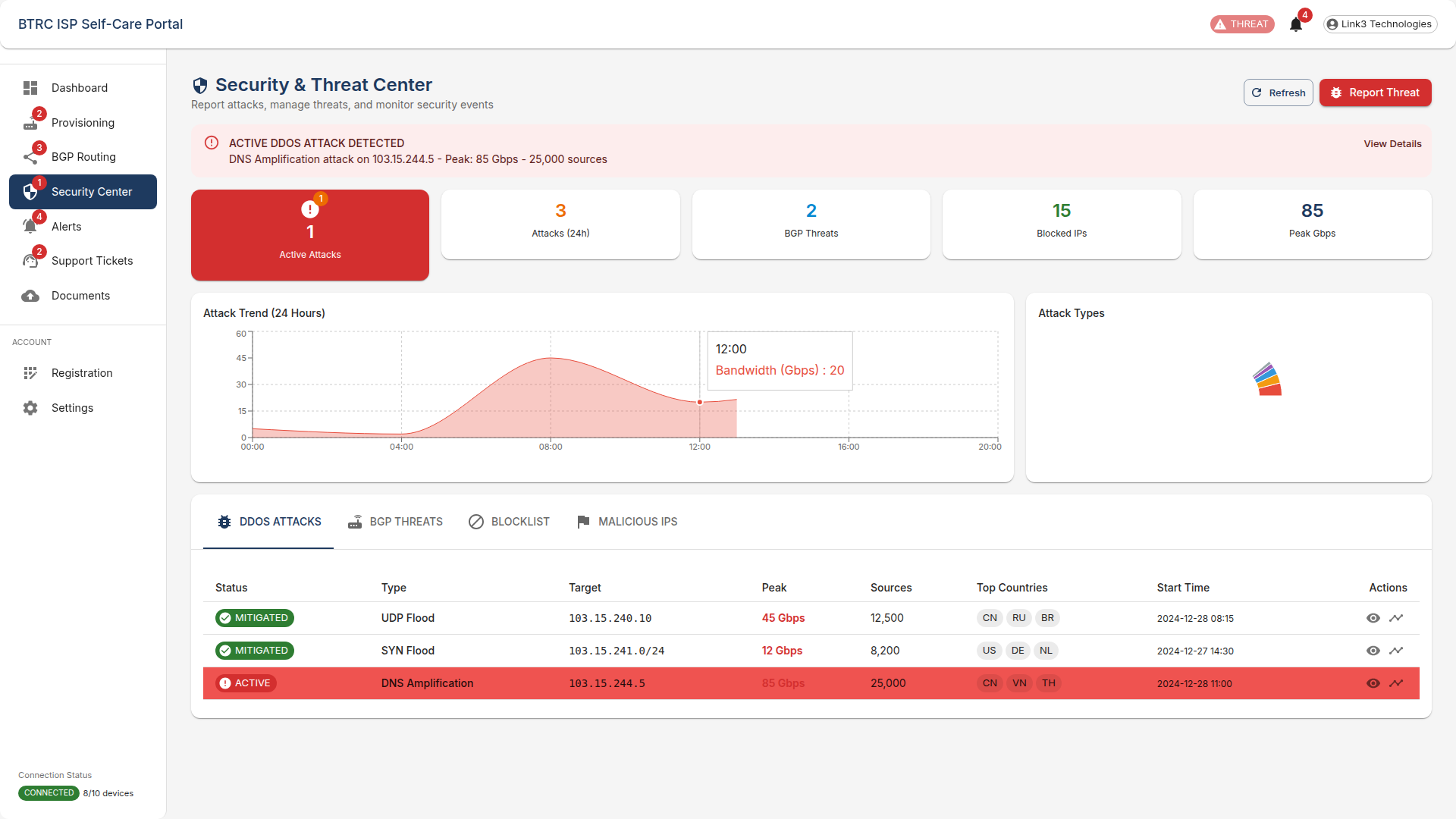
*Screenshot 7: ISP Portal Interface*



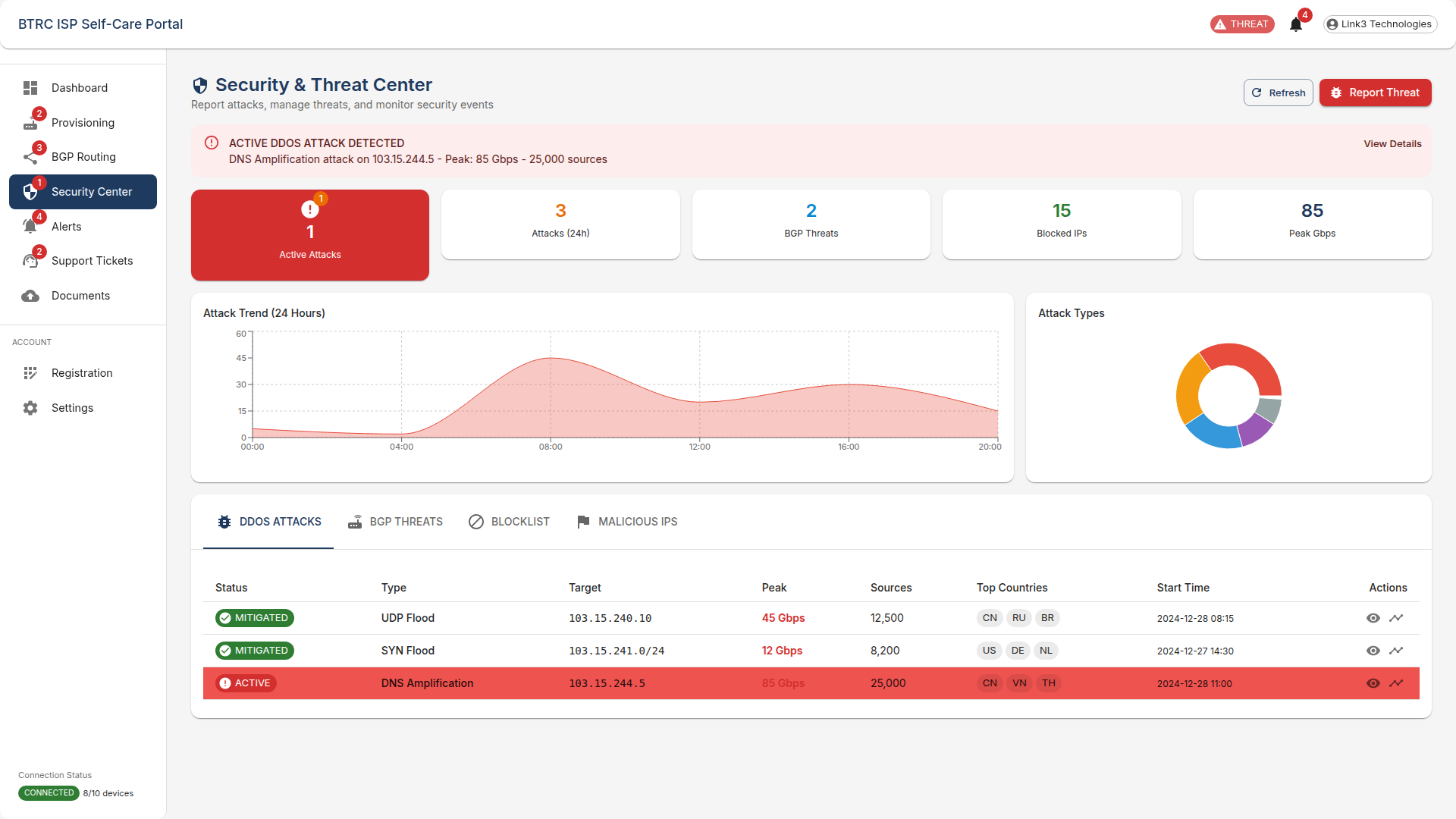
*Screenshot 8: ISP Portal Interface*



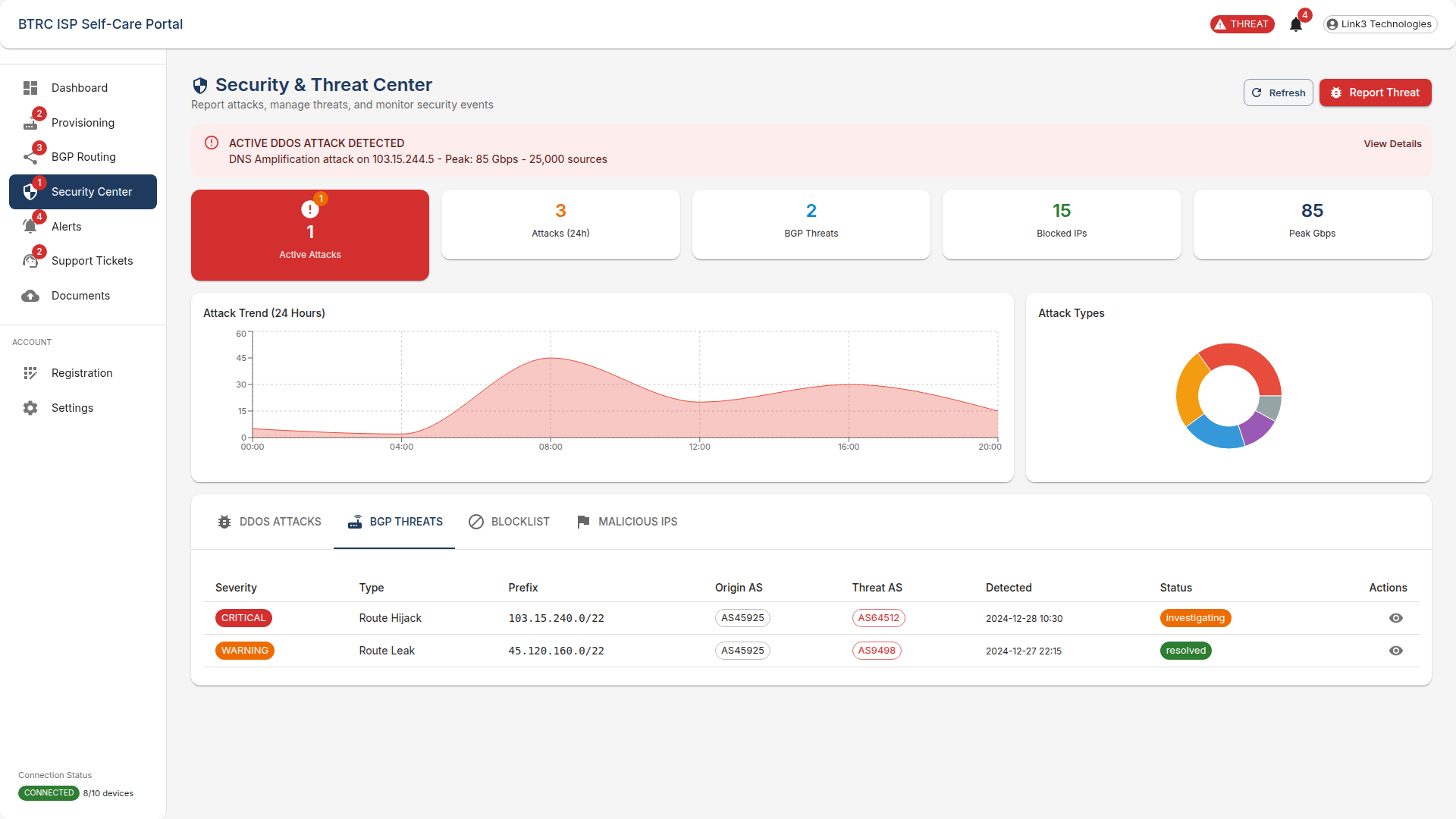
*Screenshot 9: ISP Portal Interface*



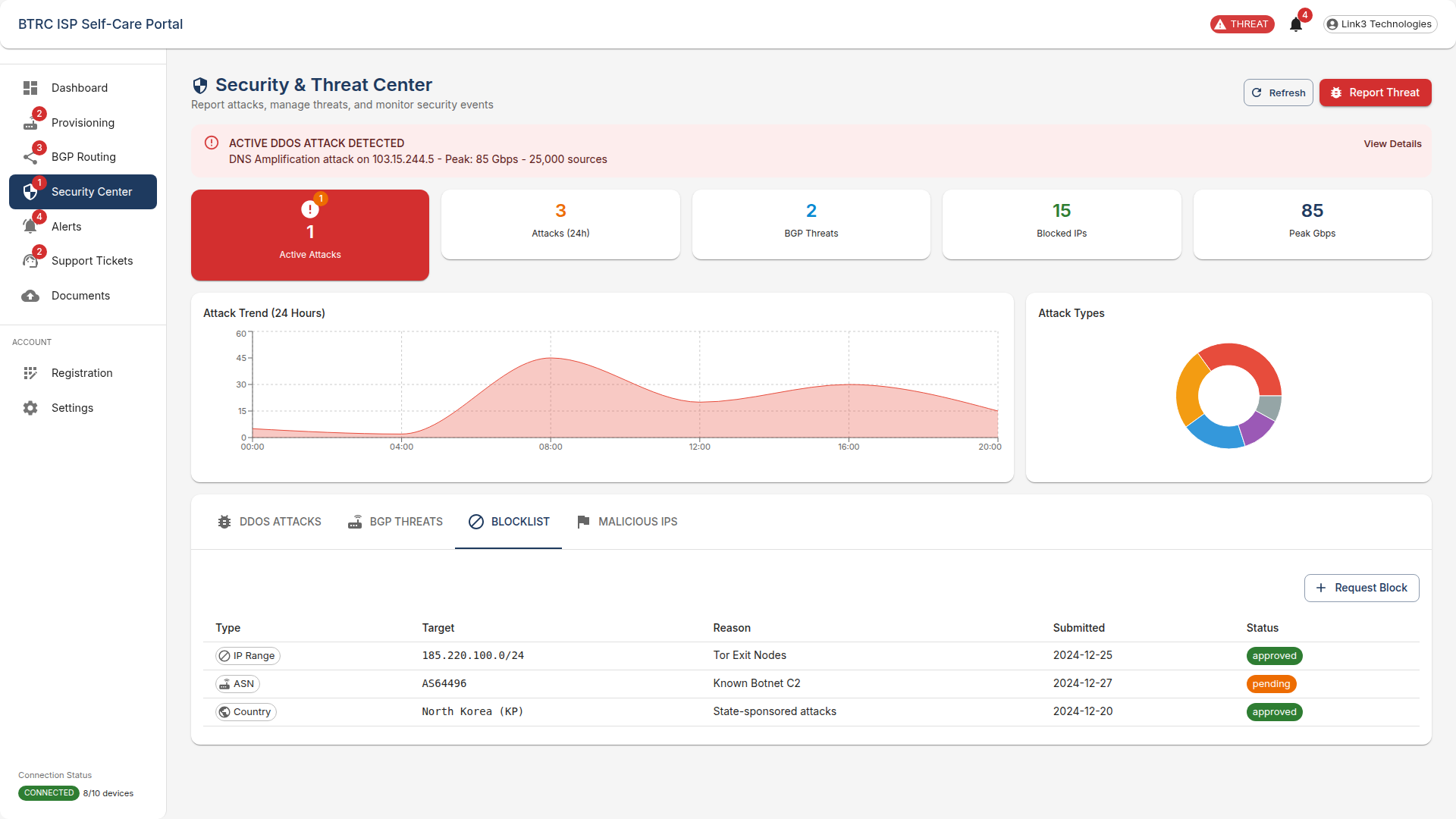
*Screenshot 10: ISP Portal Interface*



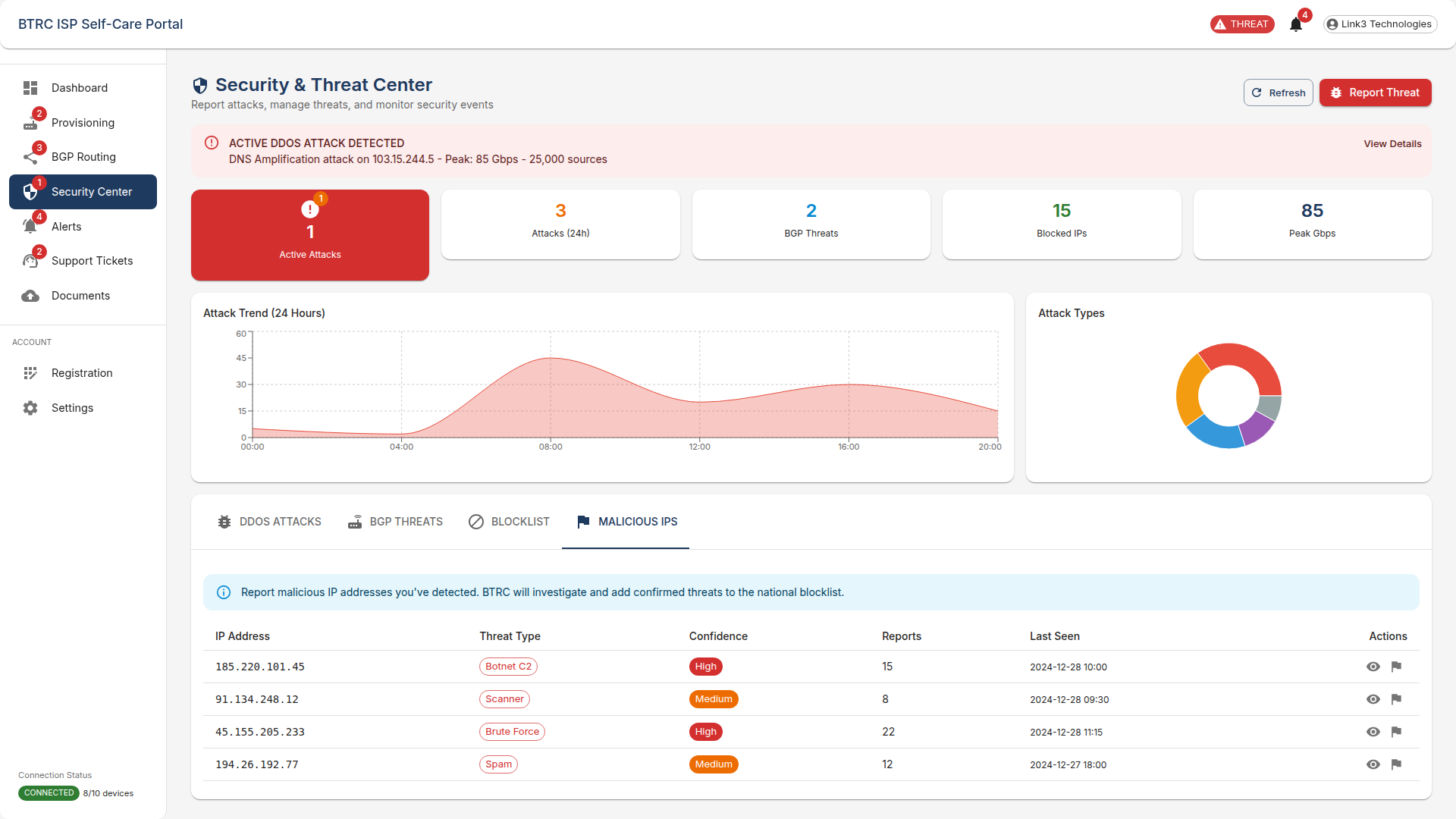
*Screenshot 11: ISP Portal Interface*



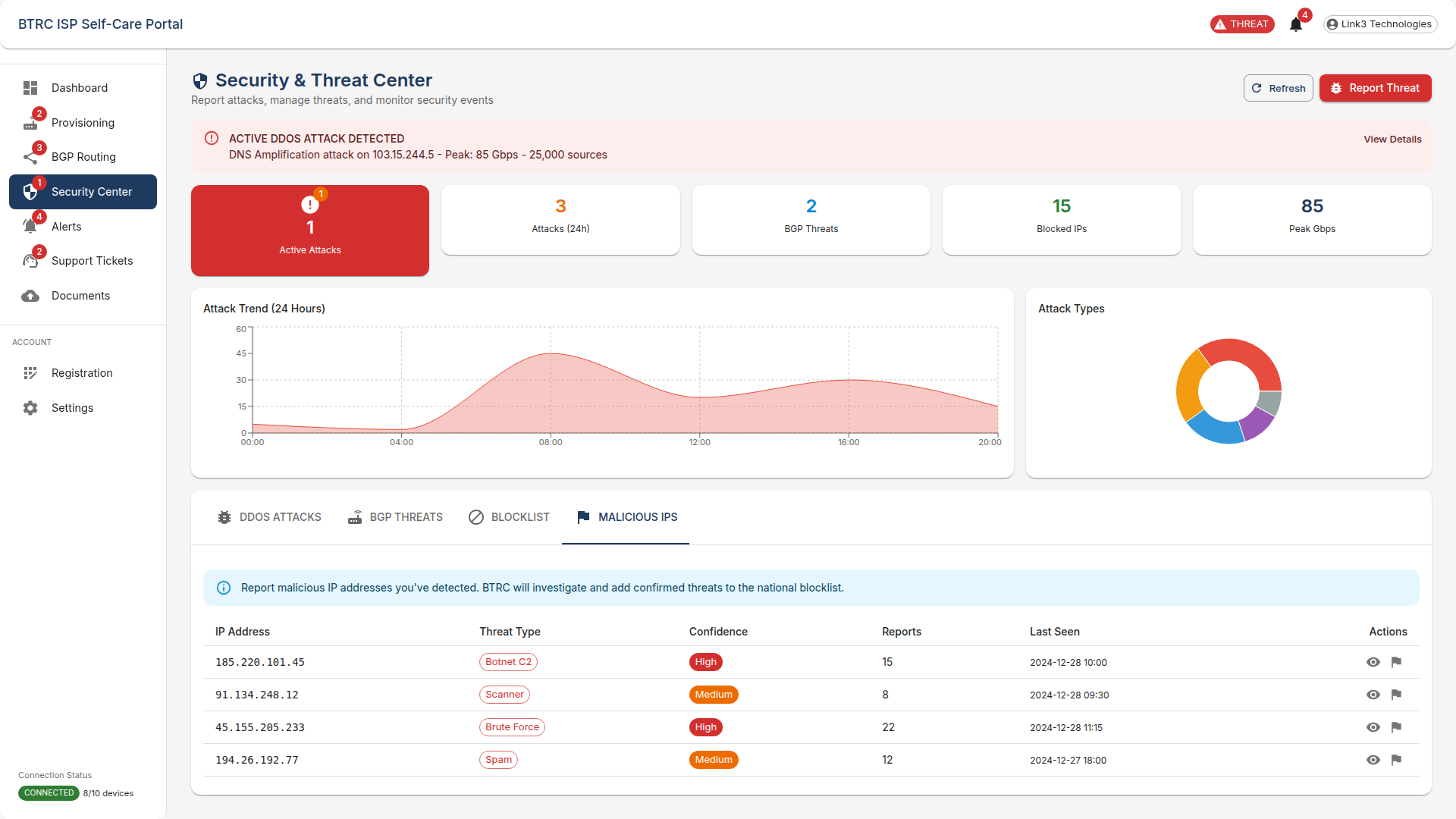
*Screenshot 12: ISP Portal Interface*



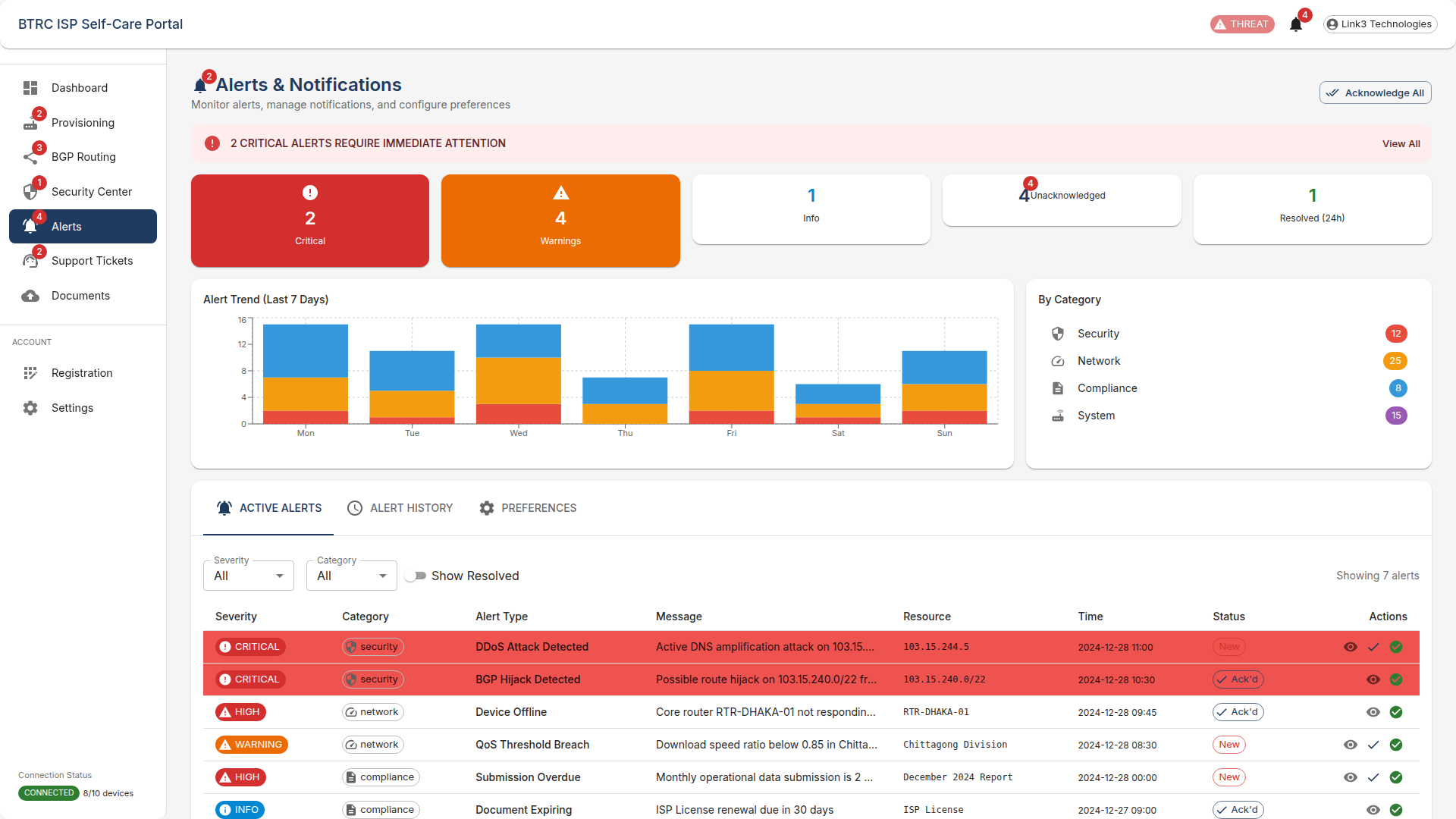
*Screenshot 13: ISP Portal Interface*



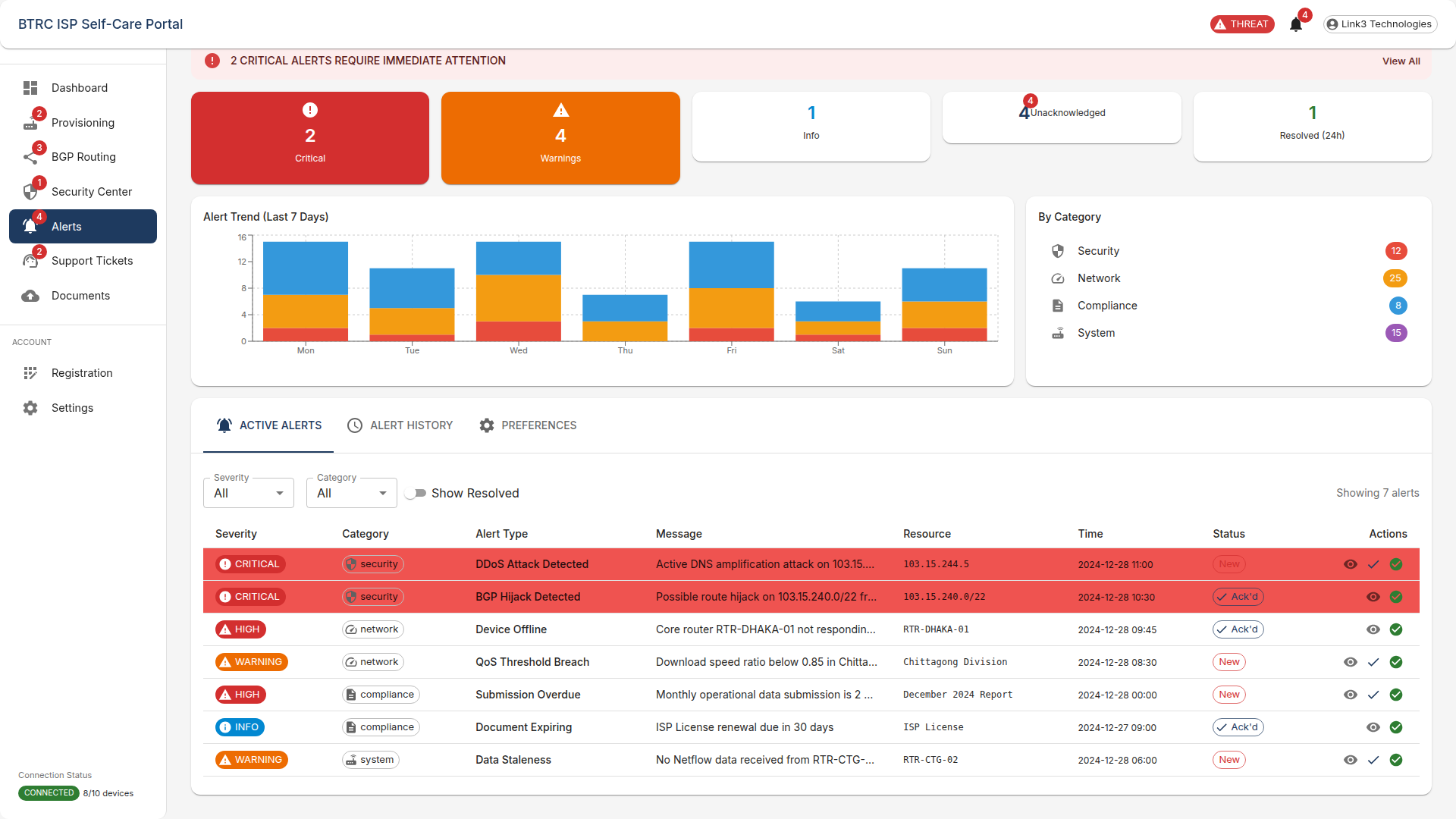
*Screenshot 14: ISP Portal Interface*



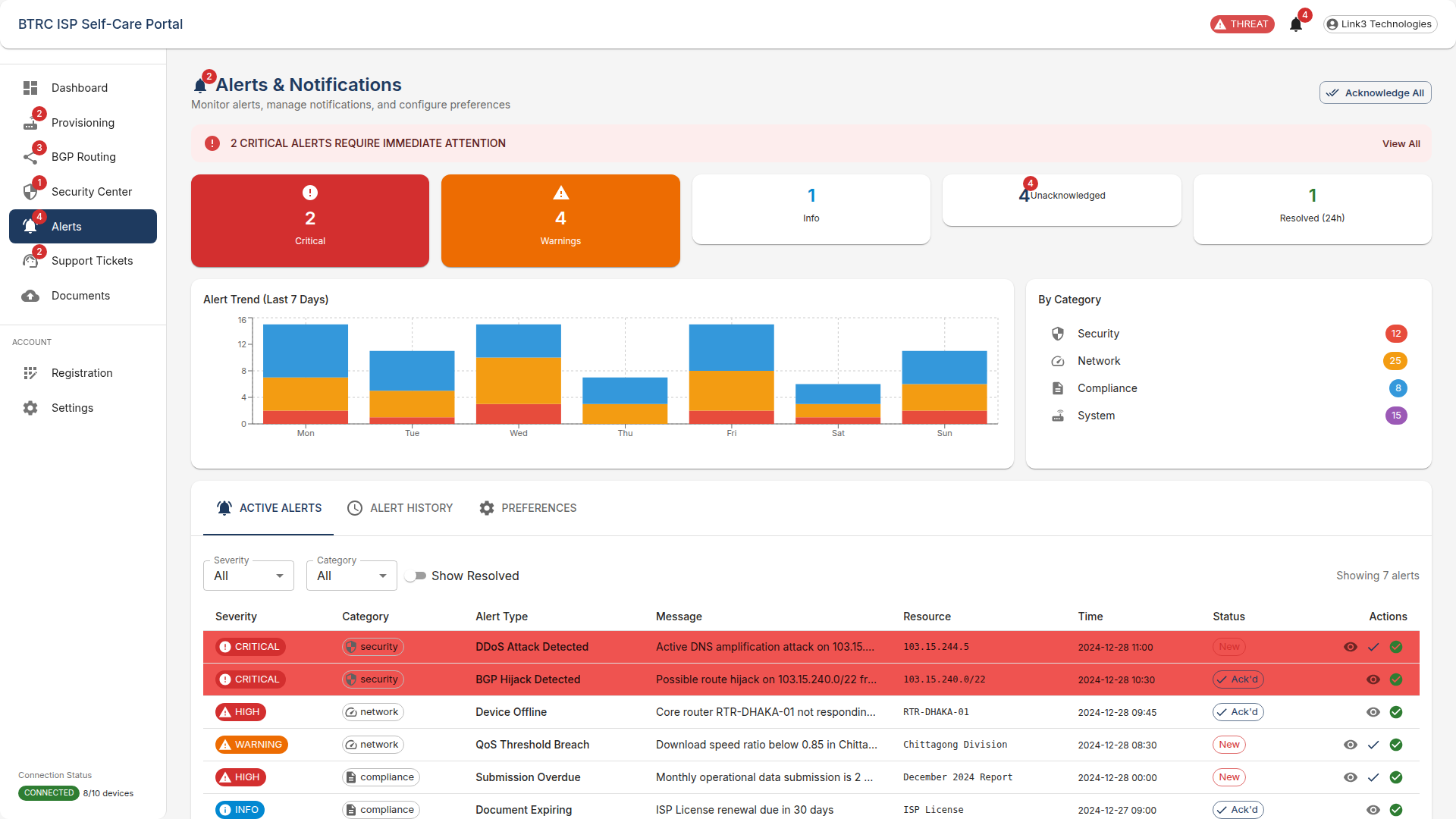
*Screenshot 15: ISP Portal Interface*



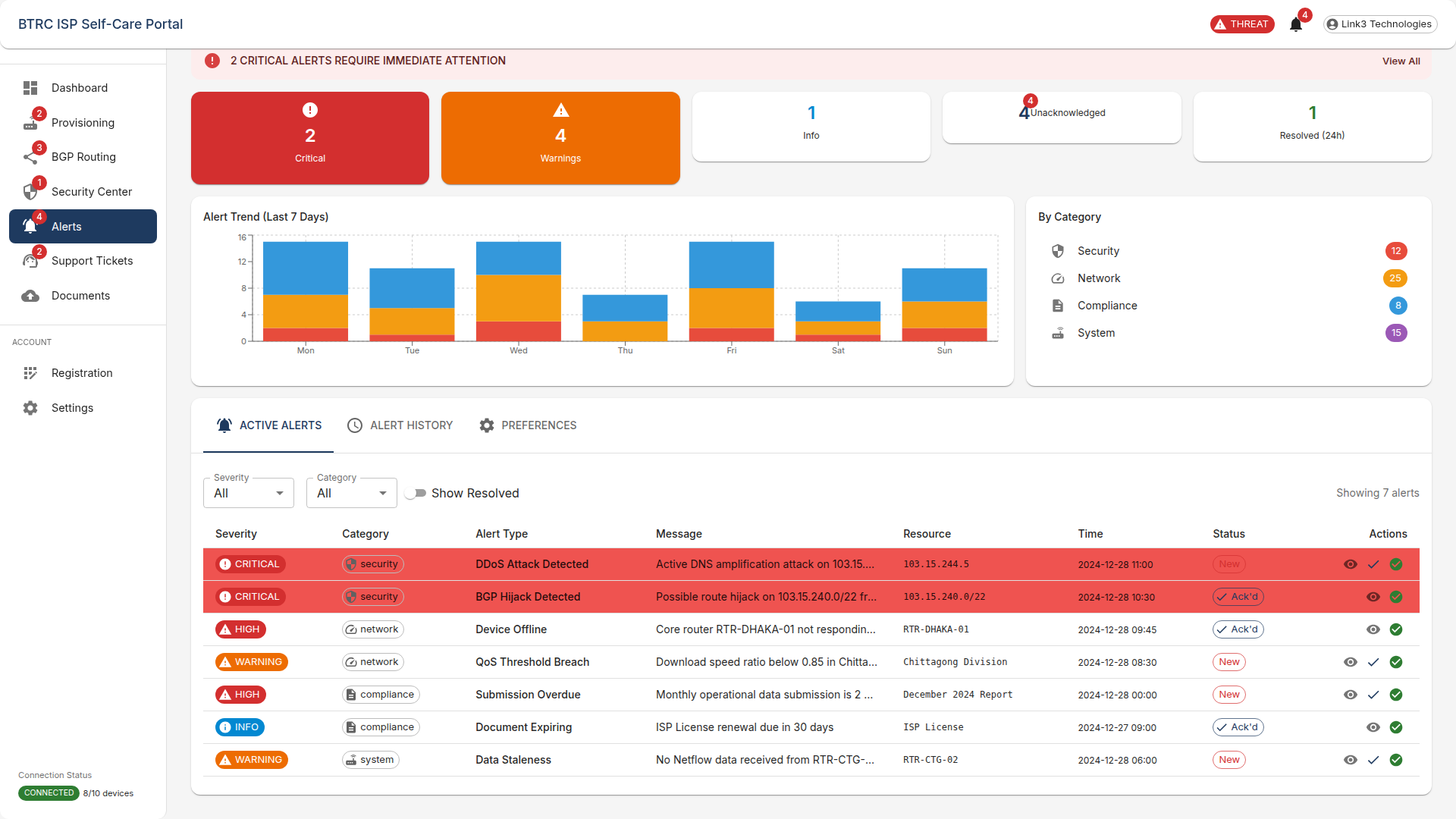
*Screenshot 16: ISP Portal Interface*



*Screenshot 17: ISP Portal Interface*



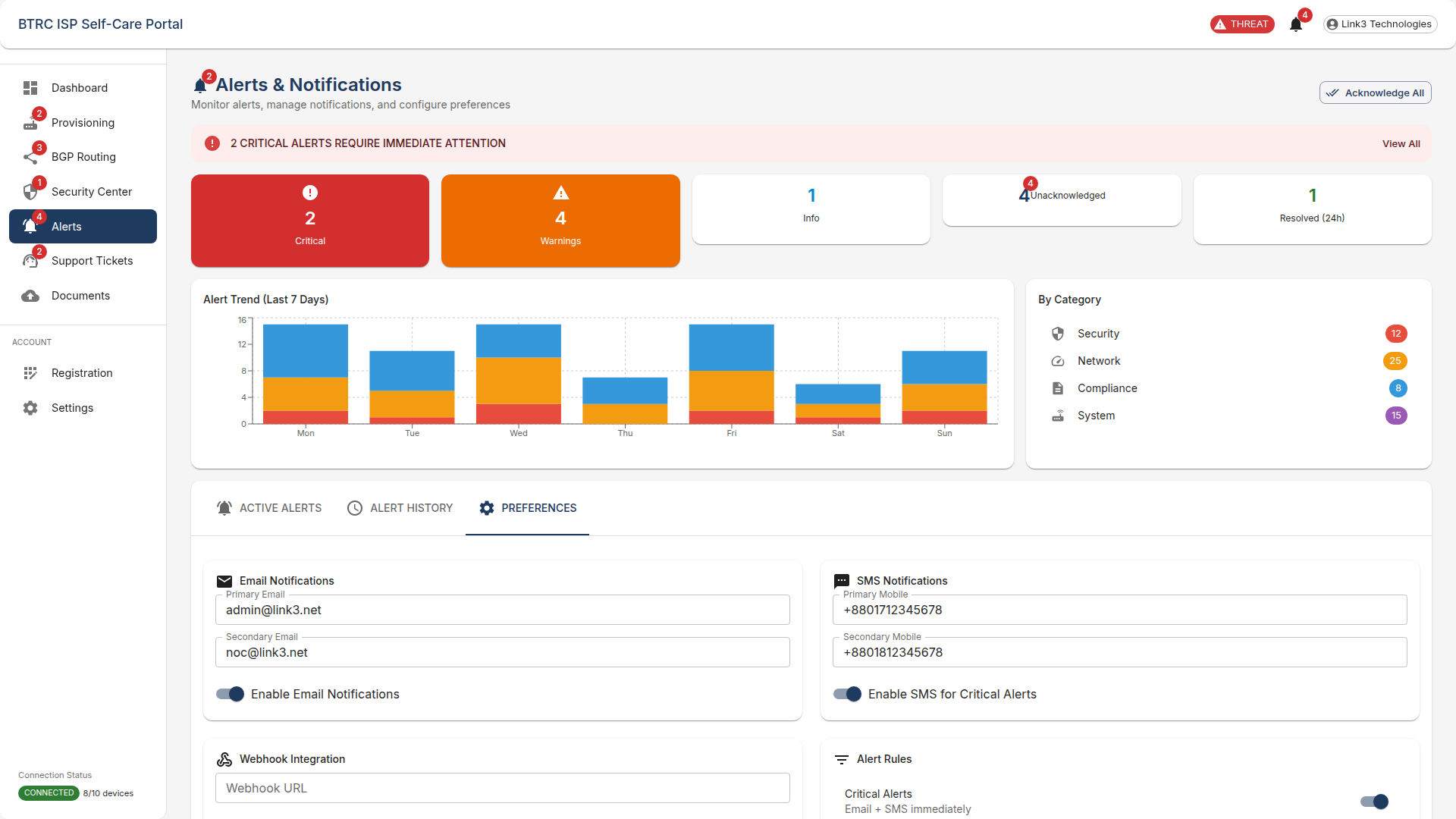
*Screenshot 18: ISP Portal Interface*



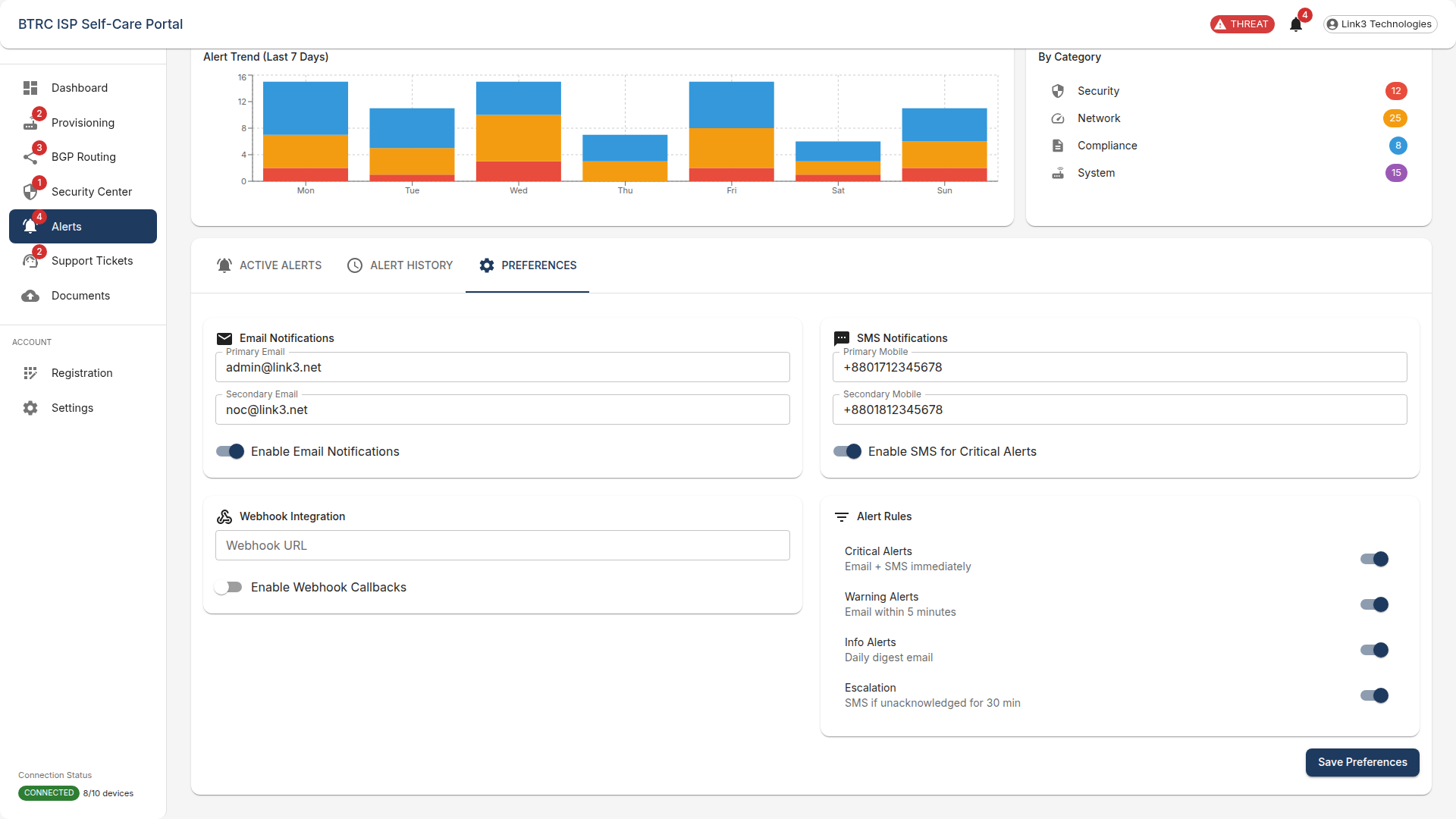
*Screenshot 19: ISP Portal Interface*



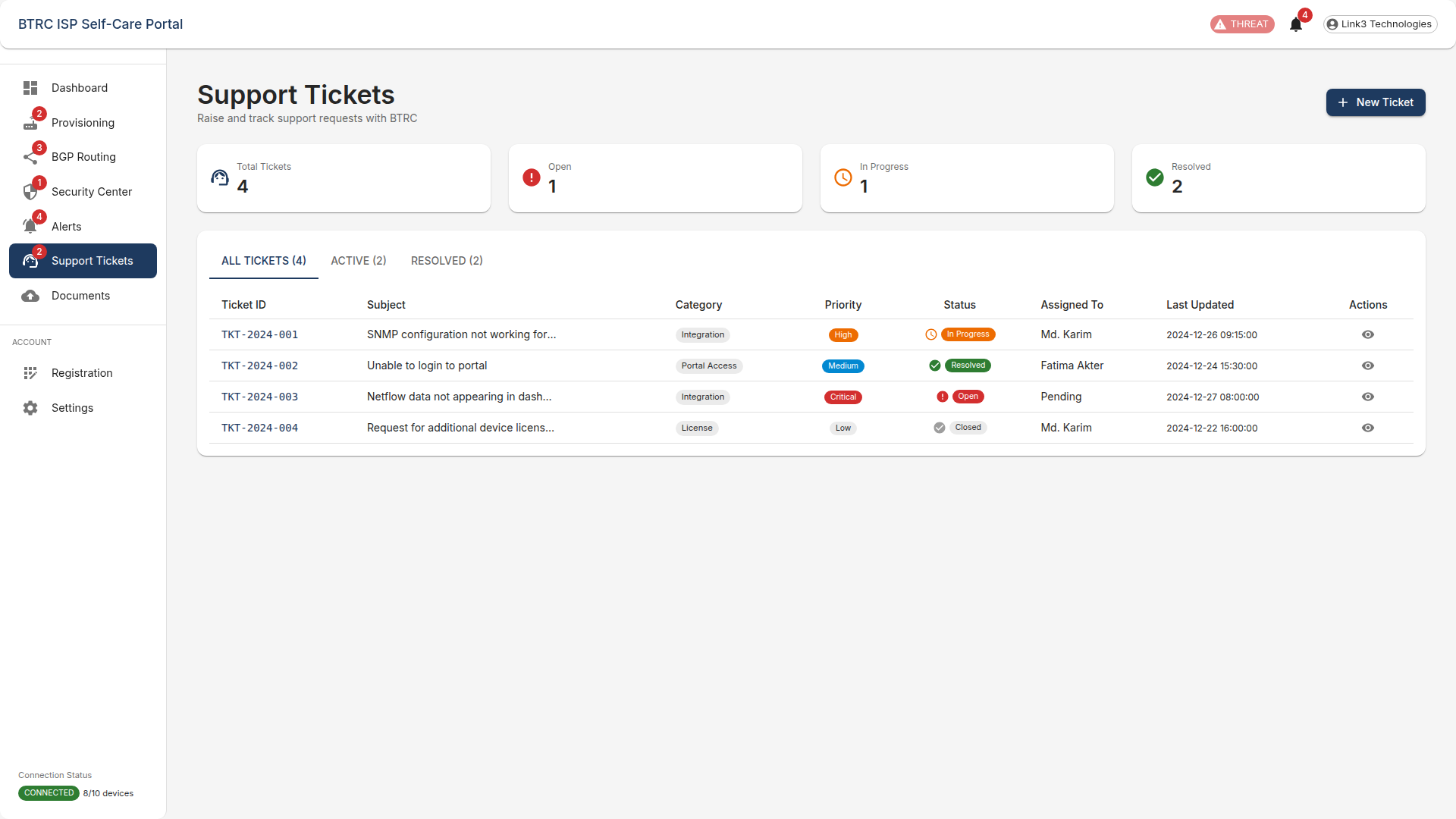
*Screenshot 20: ISP Portal Interface*



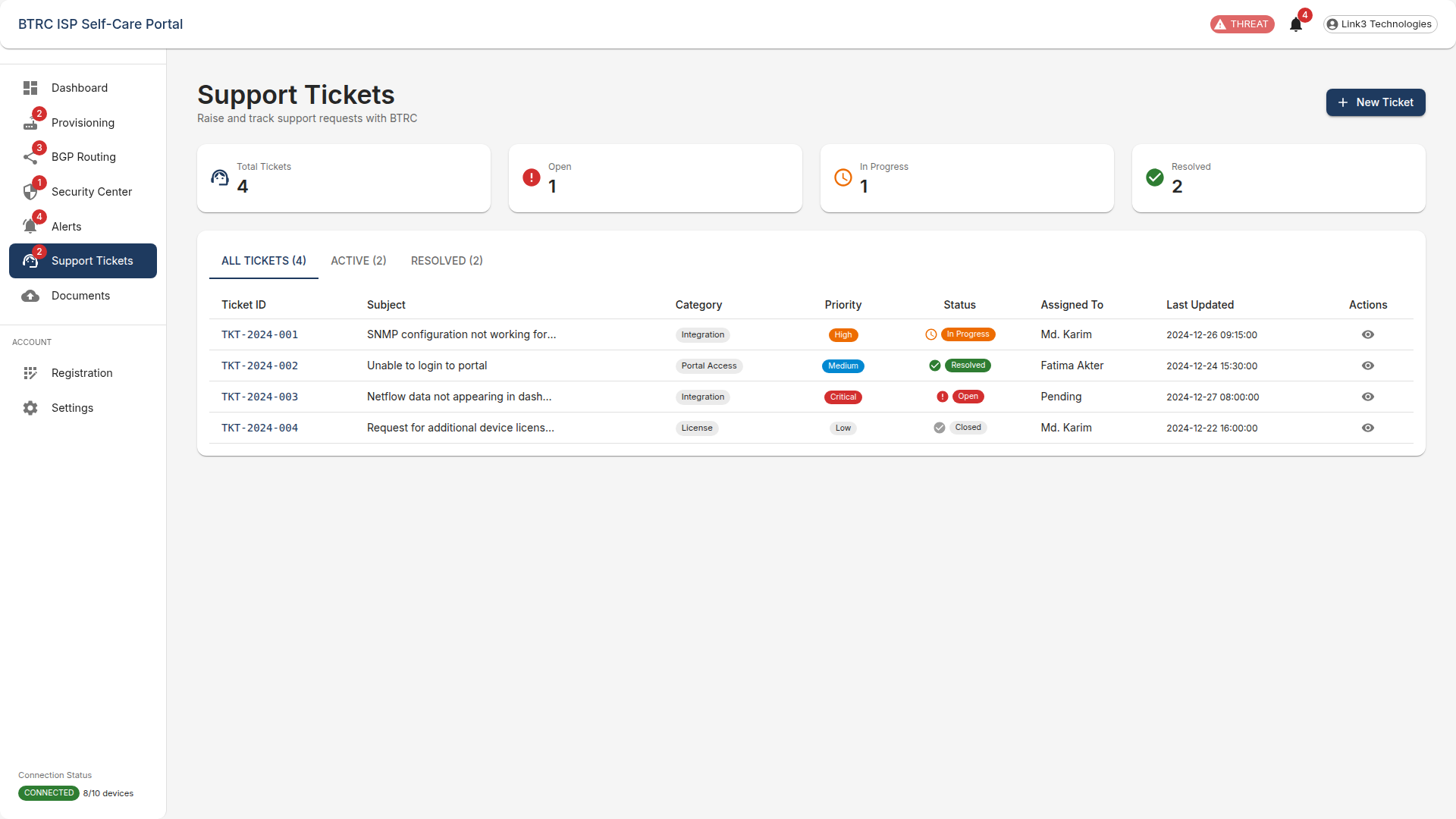
*Screenshot 21: ISP Portal Interface*



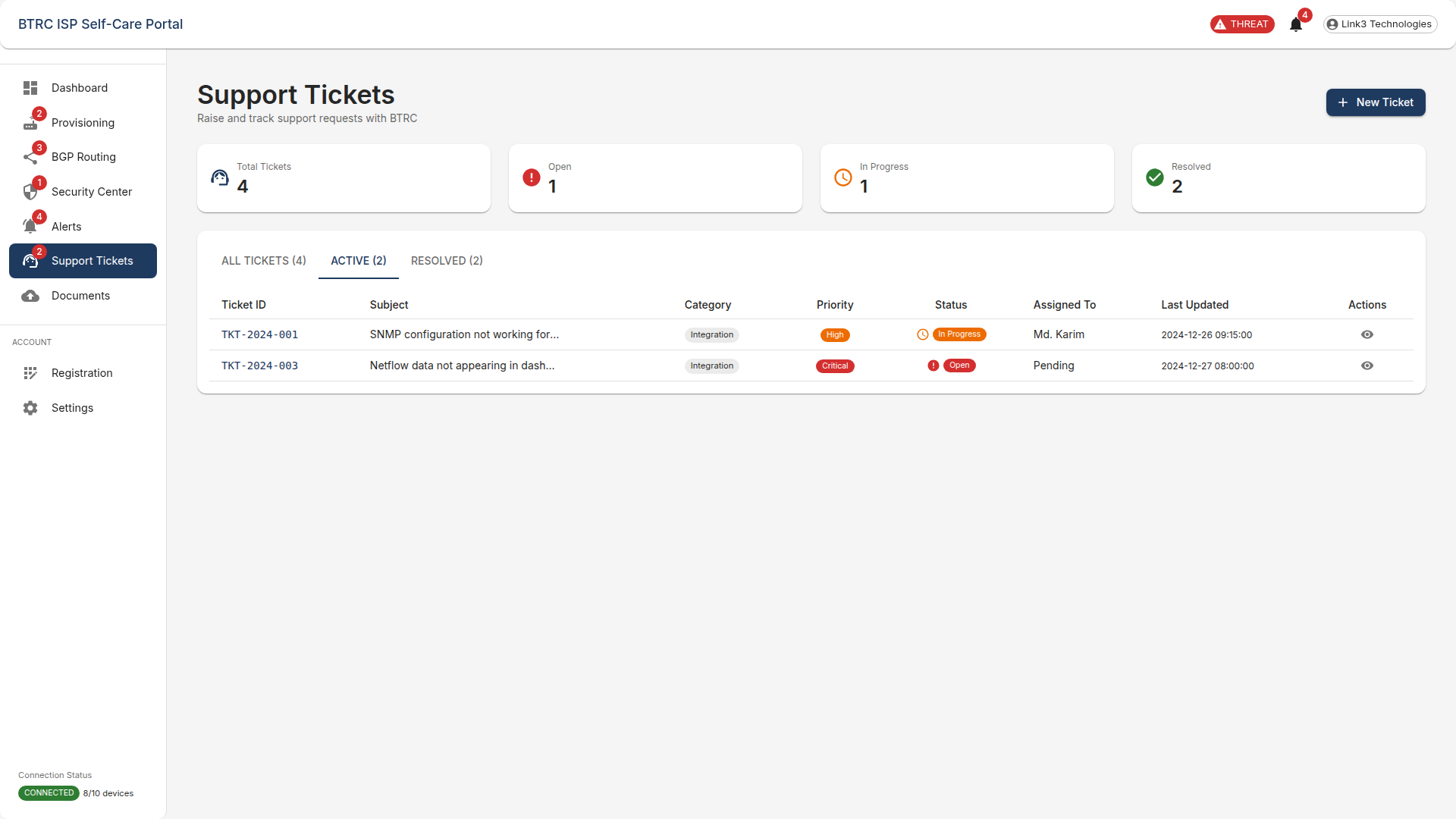
*Screenshot 22: ISP Portal Interface*



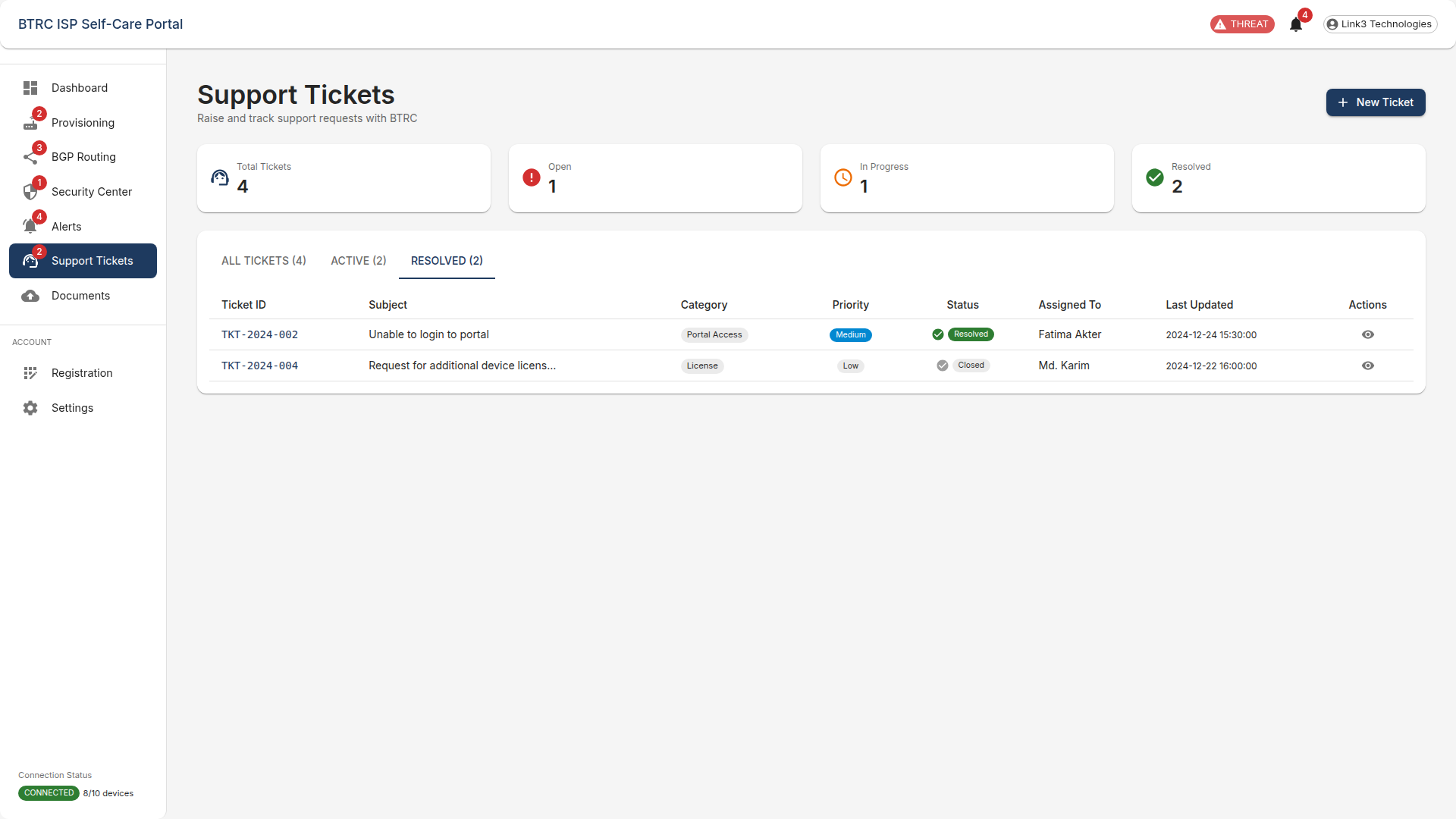
*Screenshot 23: ISP Portal Interface*



*Screenshot 24: ISP Portal Interface*



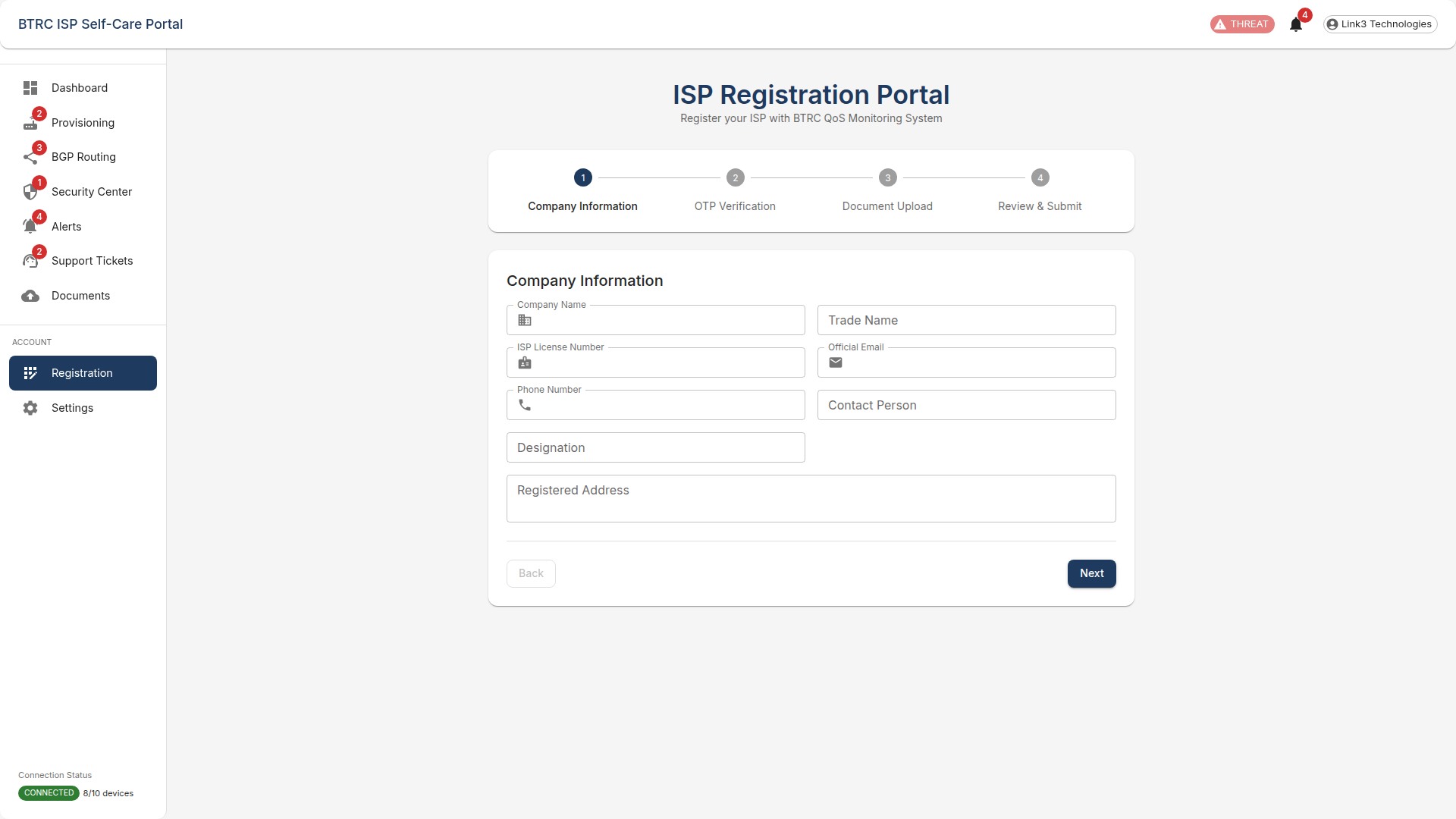
*Screenshot 25: ISP Portal Interface*



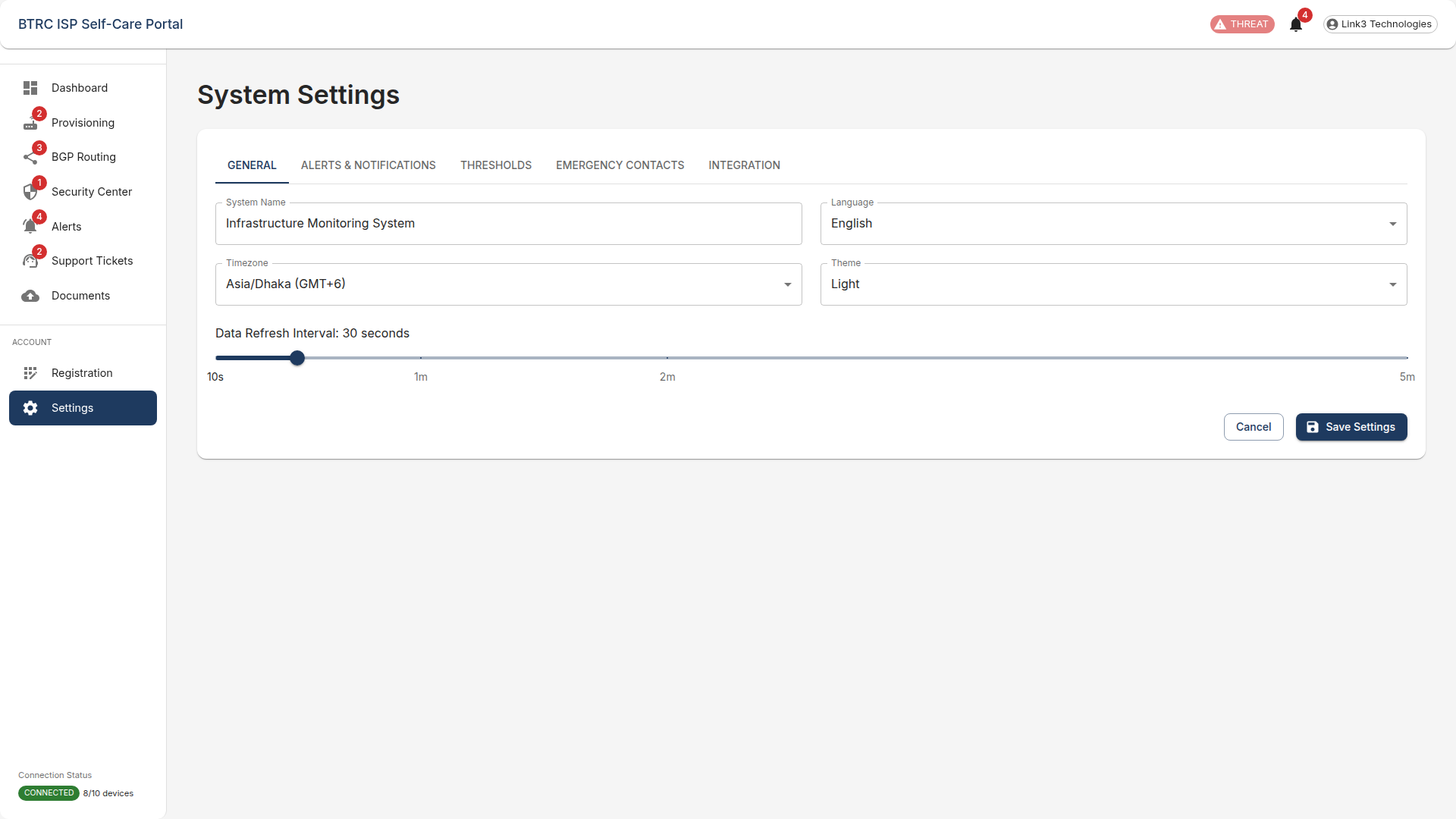
*Screenshot 26: ISP Portal Interface*



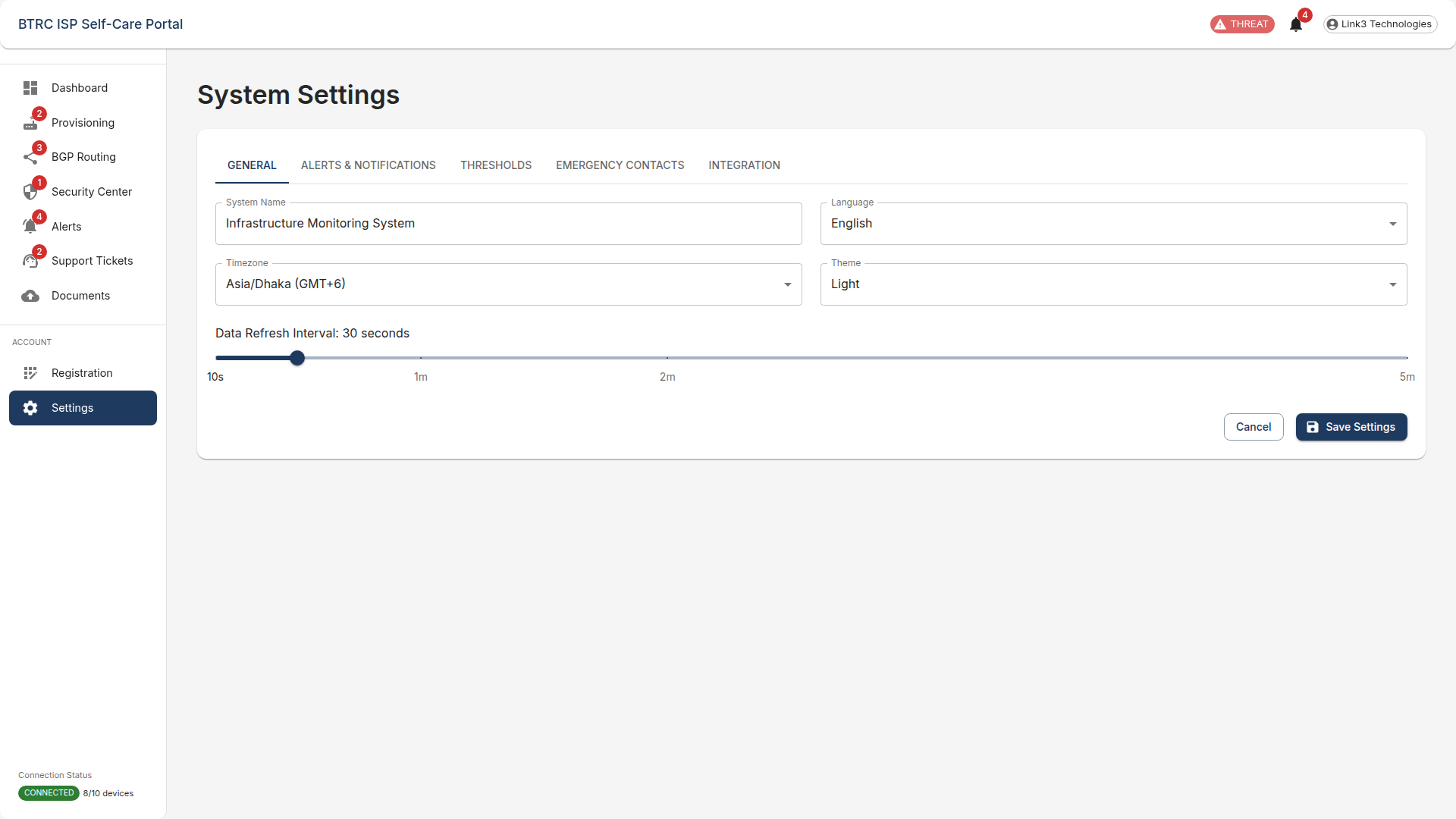
*Screenshot 27: ISP Portal Interface*



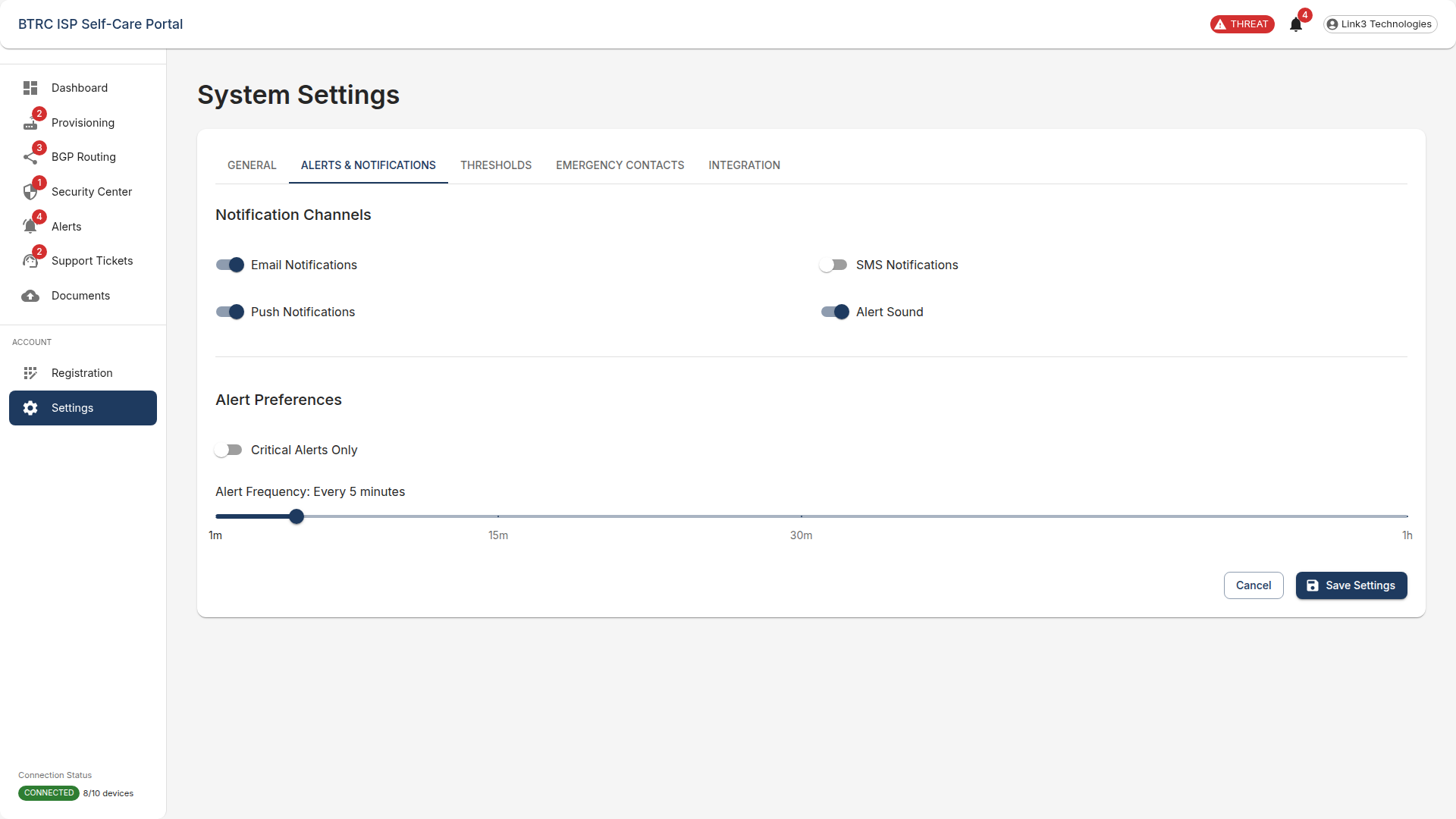
*Screenshot 28: ISP Portal Interface*



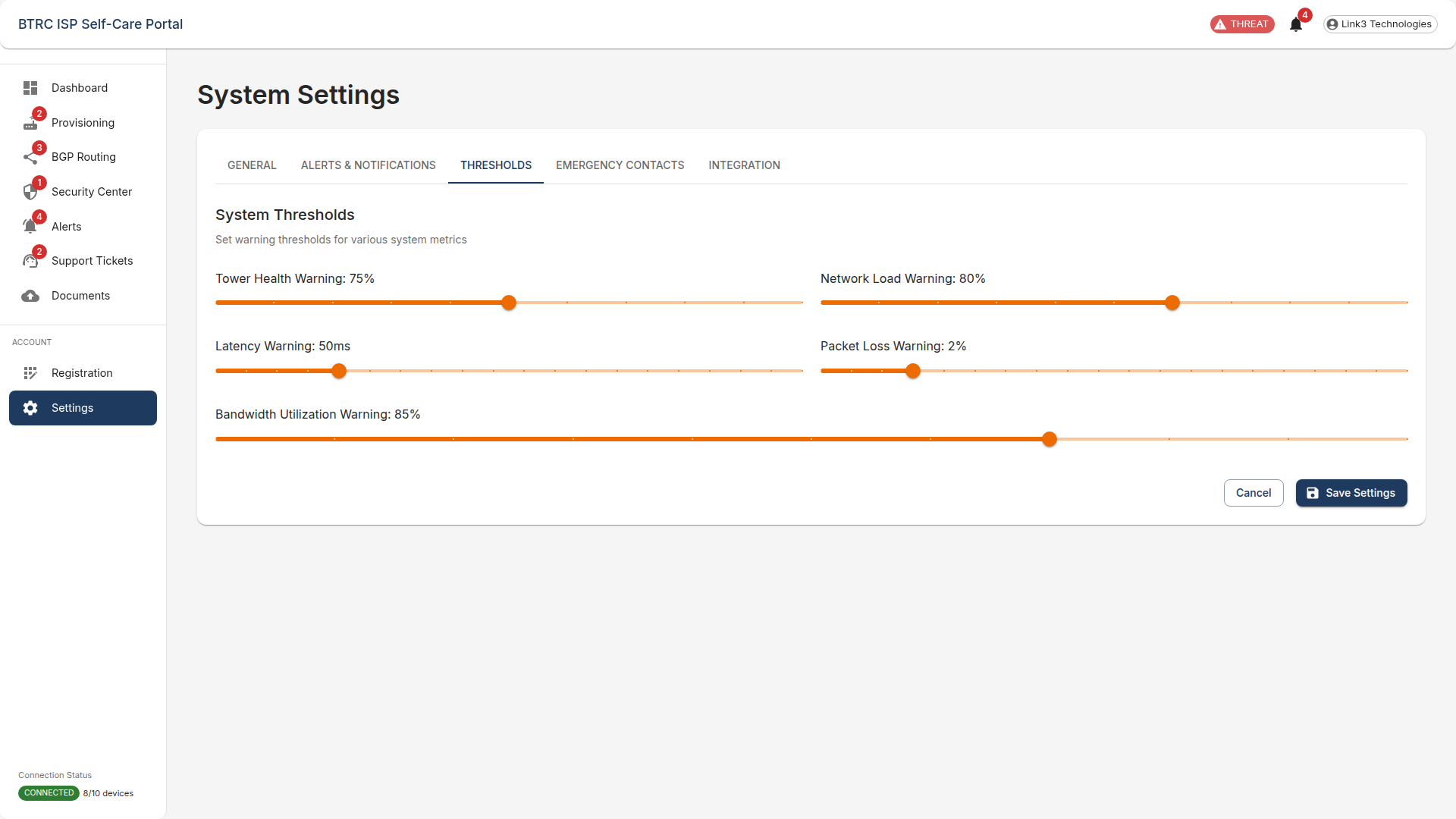
*Screenshot 29: ISP Portal Interface*



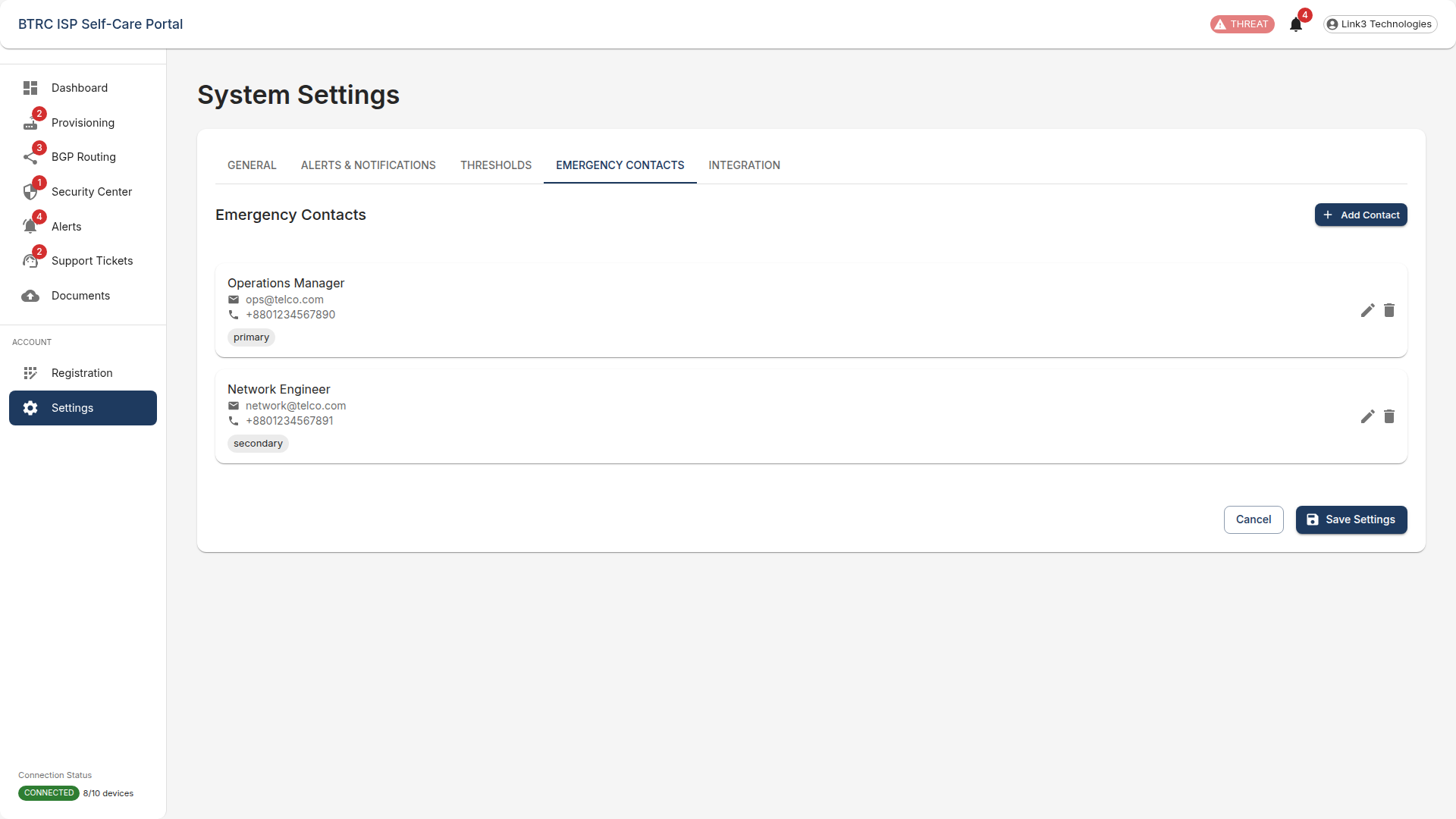
*Screenshot 30: ISP Portal Interface*



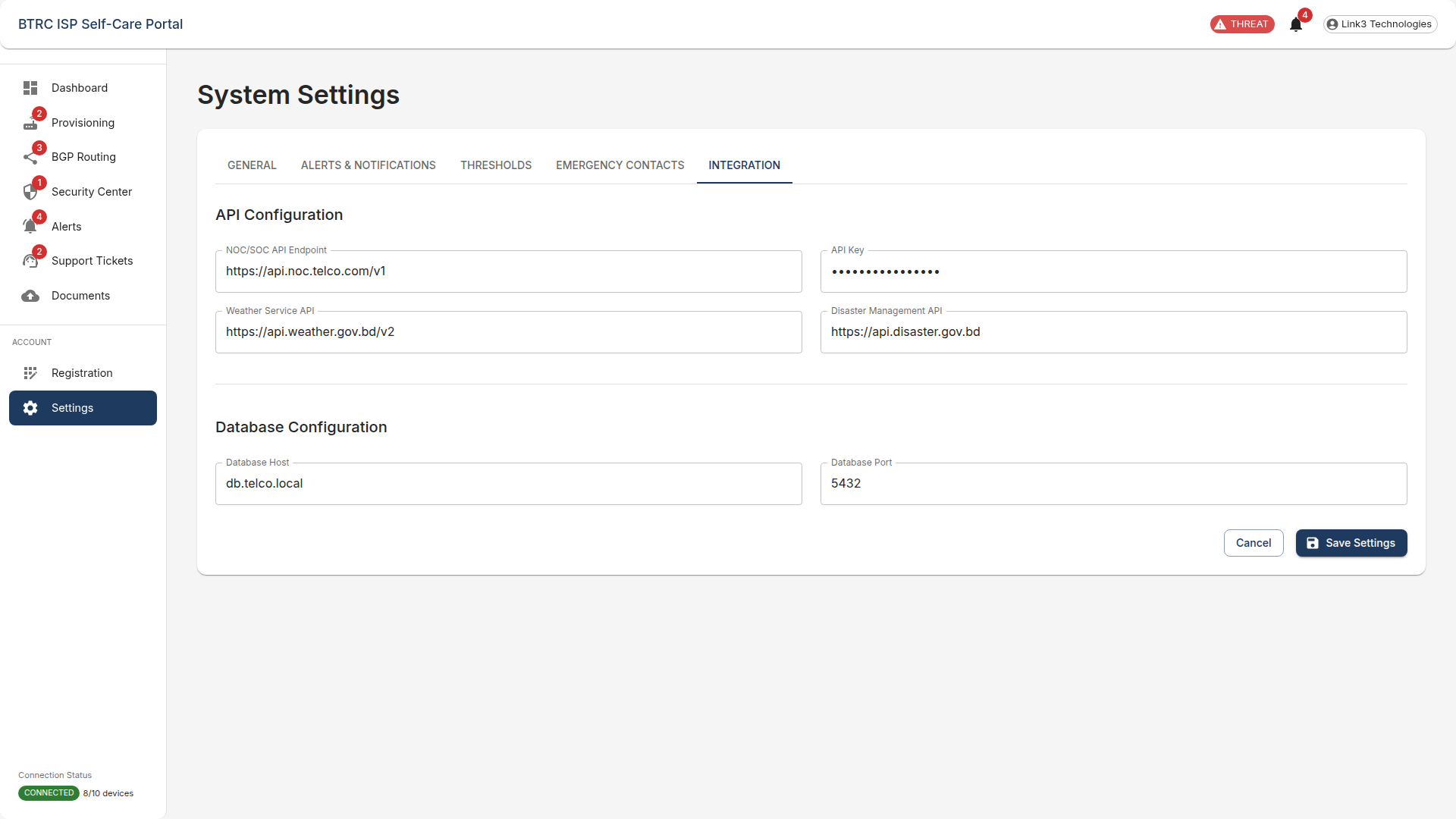
*Screenshot 31: ISP Portal Interface*



*Screenshot 32: ISP Portal Interface*



*Screenshot 33: ISP Portal Interface*



*Screenshot 34: ISP Portal Interface*