



Abusix Ops

Network abuse management,
automated from report to resolution.

Network abuse starts inside your own infrastructure, often in the form of a compromised mailbox, a hijacked VM, or a botnet node on a residential IP address. You usually see it first as volume, then complaints, feedback loops, and blocklist entries accumulate for days before the actual root cause gets identified.

Abusix Ops gives telcos, ISPs, hosting providers, and cloud providers one platform to ingest, correlate, and act on every abuse report automatically, and in real time. It turns scattered signals into a controlled process: reports are parsed and normalized upon arrival, correlated back to the responsible customer, and handled by playbooks you define. Your abuse desk only sees what needs human judgment. Everything else resolves on its own.

We provide you with automated inbound report handling first, add outbound blocking and graduated enforcement when your policy is ready, and keep the service desk your team already uses as the system of record throughout.

One solution to act on every abuse report, automatically

- ✓ Ingest reports in any format and normalize each to json
- ✓ Resolve IP to the customer who held it at the timestamp
- ✓ Unite 100s of near-identical reports into one account case
- ✓ Notify, throttle, or suspend at thresholds you set
- ✓ Log every action with the trigger behind it
- ✓ Add outbound blocking to protect your reputation

99 %

of network abuse incidents
resolved automatically

60 %

lower MTTR, from
weeks to minutes

55 %

lower spam complaint rate
via outbound blocking

300 %

more abuse cases handled
without adding headcount

3000+

analyst hours
returned per year

From 100s of Tickets to One Account Case — That's Abuse Management at Network Scale

Abuse reports land as plain-text emails, CSVs, and web forms, each with its own format, and none of them can be processed until someone reads them. Abusix Ops ingests third-party reports, spam trap and honeypot data, and your own system logs in real time, parses each, and normalizes them to a machine readable json format. We helped build that open standard, and we are driving v4 adoption into the tooling reporters prefer to use, so the format your desk works in is the format the industry already sends.

An IP address on its own does not tell you who is responsible. Every event is enriched with Abusix threat intelligence and correlated back to the exact customer, IP, or account behind it. Inbound Processing lets you build a decision tree of Resolvers, including an API Resolver that queries your RADIUS server, your billing platform, or any internal system with an endpoint. Customer resolution becomes an easy lookup rather than a matter of gut feelings.

Abusix Ops groups all related events into a single case per account or contract, rather than one ticket per report, so a volume problem appears as a single decision with the full history attached. This mitigates the problem of a single compromised customer generating hundreds of separate reports.

From there, playbooks take over. Cases are classified by type and severity, then routed, escalated, throttled, or blocked at thresholds you control. Your customer is notified automatically, with 50+ classified event types surfaced alongside the case, making it easy for support to explain a block without escalating. Webhooks, API calls, and email notifications on any playbook transition raise, update, and close incidents in the service desk your team uses, meaning you do not need to run a second system of record.

Every action gets logged with the trigger behind it. Enforcement stays consistent by design, and when a regulator, a court, or a customer asks what you did and when, the evidence is retrieved rather than reconstructed under a deadline. Anonymized customer identifiers are a first-class pattern, with resolution mapping that can remain within your own secure zone — making regulated-market compliance transparent and easily addressable.

Hours back to your team, improved risk and exposure management

- ✓ 50+ classified network abuse event types to improve risk management
- ✓ 86M+ security events processed monthly so you don't have to
- ✓ SOC 2 Type II certified, GDPR-ready by design
- ✓ Forward your abuse mailbox and start classifying in minutes
- ✓ Keep the control, the case history, and the final call with your analysts

Abusix Ops Key Features



Any-format Ingestion

Email, CSV, web forms, spam traps, honeypot feeds, and your own system logs: Abusix Ops parses each source and normalizes it to json, so nothing sits in a queue waiting to be reformatted.



Customer Resolution

Build a decision tree of Resolvers, including an API Resolver that queries your RADIUS server, billing platform, or any internal system with an endpoint, and trace an event to the account that held that IP at that timestamp.



Case Correlation

Hundreds of near-identical reports about one compromised customer collapse into a single case, grouped and prioritized by account or contract rather than by ticket count.



Automated Playbooks

Classify by type and severity, then route, escalate, throttle or block at thresholds you set. Customers are notified automatically, and a case only reaches an analyst when thresholds are crossed.



Outbound Protection

Detect and block compromised accounts before they damage your IP reputation. Protecting the outbound mail stream can cut spam complaint rates by up to 55 %.



50+ classified Event Types

Every case carries the classified event detail alongside it, so an agent can tell a customer what happened, when, and what to fix without opening a second tool.



Integrations That Fit Your Stack To Deploy

Webhooks, API calls, and email notifications on any playbook transition raise, update and close incidents in your existing service desk. No second system of record to maintain.



Compliance And Data Residency

SOC 2 Type II certified, with GDPR-ready redaction, isolation, and retention on schedules you define. Anonymized customer identifiers keep resolution mapping inside your own secure zone.

Trusted where abuse volume is highest.

"Abusix is a fundamental piece of our network security infrastructure.

It helps us maintain a strong network reputation and stable operations, while keeping our customers satisfied and secure.

We couldn't be happier with Abusix."

-Security Analyst,
Abuse Response Team,
Telenor Norway

7 of the 10 largest European telcos run on Abusix.

About Abusix

Abusix is the leading network security company that offers solutions for email security and network abuse report handling, blocks email threats with empirically earned threat intelligence, and automates network abuse handling from first report to resolution. Seven of the ten largest European telecommunications companies are Abusix customers. Learn more at abusix.com.