

Network Abuse Security, Orchestration, Automation, and Response

A BETTER APPROACH TO NETWORK PROVIDER SECURITY

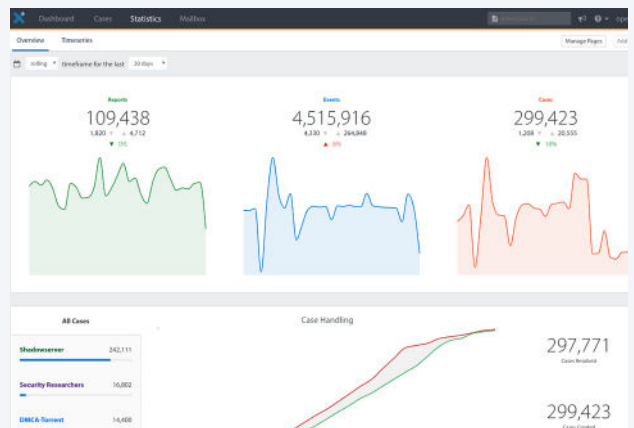
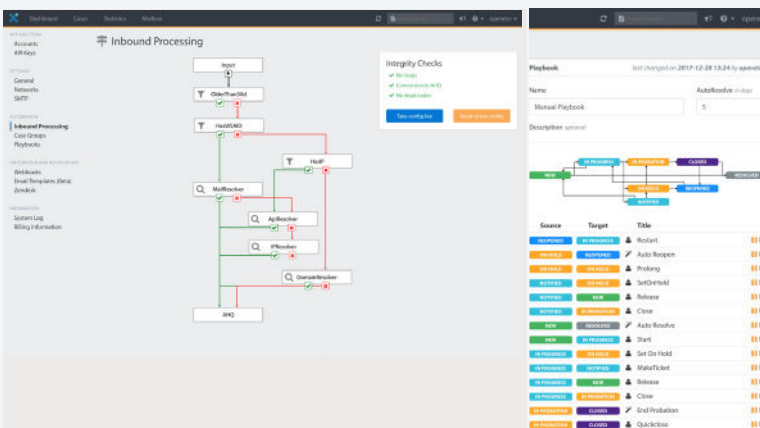
Three donut charts and a line chart showing COVID-19 statistics for the United States.

The donut charts represent the distribution of cases by state for three different dates:

- 276,574:** Shows a distribution with California (blue) being the largest state, followed by New York (orange), Texas (green), and others.
- 29,434,380:** Shows a similar distribution with California (blue) being the largest state, followed by New York (orange), Texas (green), and others.
- 241:** Shows a distribution with California (blue) being the largest state, followed by New York (orange), Texas (green), and others.

The line chart shows the daily new cases over time, with peaks around March 20, March 24, March 27, and April 22.

Protect your network, your business reputation & your customers



Abusix's Guardian Ops is the industry's first security and abuse orchestration platform that identifies and neutralizes the abuse and nefarious use of service provider networks in real time. It provides the necessary visibility that access and hosting providers need to protect their network and keep their customers safe.



ORCHESTRATION

Just as an orchestra brings together a group of instrumentalists to create a symphony, Guardian Ops allows you to easily orchestrate different data and technology elements you need to make informed decisions and take necessary actions for abuse and security events.



Data Integrations

- Guardian Ops supports both templated email and API integrations with other informational systems.
- Data enrichment services that integrate with Guardian Ops include whois, blacklist, phishing service or malware reporting services and countless others..



Infrastructure Integration

- Guardian Ops API integrations are used to resolve subscriber information and also use data elements in decision making like subscriber subscription date, class of service, etc; making workflows smarter and improving automation decisioning.



Service Integrations

- Webhook or API integrations with upstream systems like ticketing, CRM, MTAs, provisioning, wall gardens, billing, customer web portals and others are easy to configure.
- Guardian Ops templating integrates with your SMTP mail platform.
- Guardian Ops integrates into upstream systems like RT, Salesforce, Zendesk, jira to name a few, helping orchestrate the bridge between you, your support organization and subscribers.



AUTOMATION

Guardian Ops fully automates security and abuse workflows, increases subscriber alert speed, raises productivity and dramatically improves network security while lowering support costs, thus making your network unattractive for bad actors and their bots.



Event Normalization

- Guardian Ops automatically parses inbound abuse reports from over 500+ formats received from over 7,000 reporting sources, including arf, acns, iodef, Shadowserver, etc. forever freeing you from parser maintenance.
- Abusix's Guardian Intel allows you to see a real-time view of botnet activity within your network, to prevent being blacklisted.
- OSINT or edge security alerting in the form of any web, log, stream or email source may be injected via the Guardian Ops API, providing you a single pane of 'subscriber security glass'
- Automatically identify the reported endpoint regardless of whether the report is an IP, domain or URL report, eliminating the need to look up subscriber information manually.



Event Clustering

- Automatically connect related subscriber events together in a case, regardless if the endpoint is static, dynamic or a shared resource like MTAs, web hosting or other services,
- Data is automatically enriched by tagging network ranges, subscriber service level, abuse type, vulnerability, malware, and more.
- Automation ensures that events are clustered within a defined time horizon allowing you to deal only with what's current vs old mails that were recently complained about.
- Clustering occurs on three tiers; by (1) subscriber, (2) subcategory of license, resource or subaccount, and (3) abuse type case.



Playbook Rules and Triggers

- Playbook groups allow you to automate case prioritization with drag and drop so you always focus on what your organization cares about most.
- Playbooks easily mold to your existing policies and rules for enforcement.
- Customizable automated rule processing allows you to handle subscriber abuse events individually or as cases.
- Escalations for reinforcement subscriber performance requirements with each new email in a sequence are easy to create.
- Sharing of abuse report and case information with your subscribers is simple with our integrated report sharing feature.
- Workflows can easily escalate cases to internal security teams and/or legal stakeholders by email, text, slack or other systems that notify or get approvals when case threat levels are escalated.
- Make security and risk assessments earlier lowering overall network operations and support costs.
- Playbooks allow you to naturally and continually make incremental process improvements to your automated, semi-automated and manual workflow processes, reducing organizational costs and dramatically decreasing legal risk.



RESPONSE

Guardian Ops allows you to help users in a uniform consistent manner, enforce your acceptable use policies (AUP), thus keeping your network clean and robust for your users and increasing customer satisfaction, all while lowering your organizational risk, ensuring safe harbor protection and maximizing profits by ensuring your network is being used as intended

- Greatly simplify network operator security operations by providing a single pane of glass for all subscriber security and abuse related issues, while assuring a safer more secure network by lowering MTTR (mean time to respond).
- Reduce subscriber security and vulnerability issues, network abuse, thereby improving the reputation of your network and reducing blacklistings.
- Act on fraud, copyright and phish notifications in real time and catch repeat offenders; thereby dramatically reducing legal risk.
- Improve subscriber response to compromised machine notifications, customer care and quality of service; thus increasing subscriber satisfaction and retention.



REPORTING

With Guardian Ops you can report on priorities determined by business context metrics such as risk management and efficiency. This allows abuse and security teams to prioritize abuse and security operations activities, response to events & threats and automate most mundane activities through playbooks.

- See your inbound mail and case queue in a standardized view separating reports from spam.
- Prioritization of the cases by any of the 100+ preconfigured sub-filters making viewing and reporting on cases super simple.
- Easily see subscriber case histogram and all the underlying data to make better decisions.
- Understand overall network abuse trending by abuse types, abuse reporter, malware, infections flows and status easily to track trends and make strategic subscriber campaign decisions.

SYSTEM REQUIREMENTS

- A web browser
- A forwarding abuse@ address

ABOUT ABUSIX

Abusix is an industry-acclaimed leader in network abuse management and email security solutions. With advanced technology, Abusix helps telecommunications, technology enterprises, and network providers fight spam, phishing, and other cyber threats, ensuring operational integrity and network protection. Abusix is the go-to partner for securing digital environments and safeguarding against evolving online risks.



Contact us to learn more about **Guardian Ops**

✉ sales@abusix.com

☎ +1 (855) 522-8749

🌐 www.abusix.com

Disclaimer: This datasheet is for informational purposes only. Abusix makes no warranties, express or implied, in this summary. Companies, names, and/or data used in screens and sample output are fictitious unless otherwise noted.