Securafy™

PROACTIVE DEFENSE FOR NETWORKS

PROACTIVE DEFENSE FOR NETWORKS

DATA SHEET

StratoZen's Proactive Defense for Networks (PDN) service leverages our global threat intelligence network and SWATFeed to continuously update blacklists on your firewalls and other devices. Simply subscribe your firewalls, UTMs, and other supporting devices to the PDN feed for automated protection against known malicious sources.

Use Proactive Defense for Networks to automatically block:

- **Inbound traffic from SWATFeed active attackers, TOR exit nodes, botnets, and other malicious sources.**
- **Outbound traffic to ransomware hosts, command & control servers, and other malicious destinations.**

The PDN feed is actively curated and managed by StratoZen's SOC to maintain a high-confidence block list that's updated continuously.

DEFEND YOUR CUSTOMERS

Defend your network automatically by subscribing firewalls, UTMs, and other devices that support blacklist feeds.

SET AND FORGET

The PDN feed is updated every hour to keep blacklists stay up-to-date without requiring your constant attention.

REDUCE NOTIFICATIONS

PDN automatically blocks malicious traffic to reduce the number of incidents that require a response, which reduces the notifications you must address.

> "Proactive Defense for Networks is not a simple threat feed; it's a high-confidence blocklist subscription managed by StratoZen's experts to continuously, and automatically, defend you and your customers from every-changing network threats."
>
> **- Kevin Prince, Founder & CEO, StratoZen**

SWATFEED ACTIVE ATTACKERS

StratoZen's Worldwide Active Threat (SWAT) Feed is a live list of active attackers against StratoZen's own global honeypot network. The list is updated hourly with a short, seven-day retention time for high accuracy and confidence. We also finetune the list to exclude benign research scanners such as the University of Michigan and Shodan.

WHY PROACTIVE DEFENSE FOR NETWORKS?

Evolution, Age and Retention

To be added to PDN, we require a list be updated often, culled for dead or stale addresses, and have active aging policies that remove addresses regularly.

Overlap

Using multiple threat feeds is beneficial but can result in unnecessary overlap. StratoZen monitors for overlaps and removes duplicates to avoid import problems and minimize processing power used by the subscribed devices.

Frequency of Matches

We continuously measure the efficacy of our feeds, as well as other feeds, by analyzing the frequency of matches in our SIEMs. Too few or too many matches could indicate an underlying problem with the list accuracy.

Durability

To remain relevant and actionable, a feed must constantly evolve. StratoZen constantly updates our SWATFeed honeypots to log the latest attacks. We confirm list durability by tracking the rate that new attacker IPs are being added.

Global Visibility

We have unique visibility from our global SIEM network. We see the effectiveness of free and clientpaid lists across thousands of networks. If a threat feed results in many false positives, it's not threat intelligence, it's bad data.

Active SOC Management

Our SOC-as-a-Service team actively manages our PDN feed. When external threats are identified at one client site, our SOC can add those IPs to SWATFeed, blocking the offender for all PDN subscribers within 1 hour.

PROACTIVE DEFENSE NETWORK BLOCKLIST CLASSES

SWATFeed Active Attackers
Live list of active attackers against honeypots deployed around the world. Updated hourly.

TOR Exit Nodes
New and automatically updated list of current TOR exit nodes. Old exit nodes removed at each update. Updated Hourly.

Known Bad IPs
This IP list is a curated composition of other IP lists and best practices. The critical prerequisite for this list is to have no false positives. All IPs listed are considered harmful or inappropriate and should be blocked, without exceptions. Retention on this list is much longer, as most addresses can be barred permanently. Updated Daily.

Ransomware Sites and Hosts
Tracks and monitors IP addresses that are associated with Ransomware, such as Botnets, C&C servers, distribution sites, payment sites, and others. By using data provided by threat feeds, ISPs, as well as national CERTs/ CSIRTs, this provides an upto date overview of current infrastructure used by Ransomware and whether these are actively being used by bad actors to commit fraud. Updated Daily.

Cybercrime Servers
Tracks and monitors IP addresses that are associated with verified cybercrime command and control servers. Updated Daily.