Netsurion®

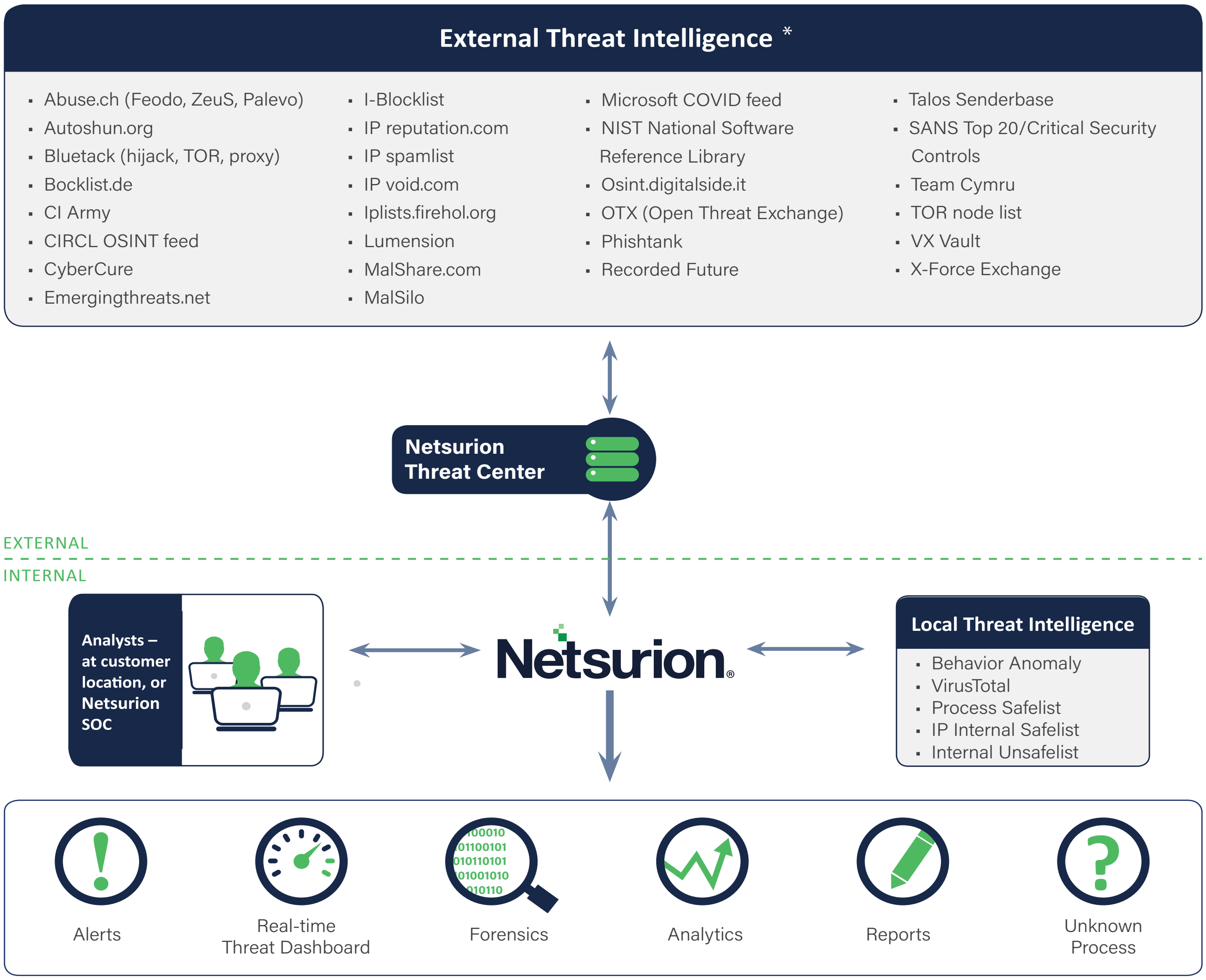
# Netsurion Threat Center

## Better decision making with threat context and cybersecurity expertise

The Netsurion Threat Center integrates technology, processes, and cybersecurity expertise to accelerate threat detection and response. We enable you to make better security decisions with greater speed and confidence. The Netsurion Threat Center is a combination of a threat intelligence platform and a team of security analysts who focus on emerging threats across the internet and those active in the Netsurion community.

Threats are dynamic and attack vectors change constantly. Respond quickly and minimize damage by using the rich context enabled by threat intelligence and Indicators of Compromise (IoCs).

The Netsurion Threat Center platform incorporates threat intelligence from various providers, including global open source feeds, those curated by the threat team at Netsurion, and contributions from the Netsurion community.  Netsurion SOC analysts leverage this data to reduce false positives, detect hidden threats, and prioritize your most concerning alarms. The Netsurion Console ingests these consolidated feeds from the Netsurion Threat Center and can combine them with commercial feeds subscribed to by the customer as well as rules specific to the installation. These consolidated feeds provide the optimum mix of threat intelligence: global, community, and local.



### External Threat Intelligence *

- Abuse.ch (Feodo, ZeuS, Palevo)
- Autoshun.org
- Bluetack (hijack, TOR, proxy)
- Bocklist.de
- CI Army
- CIRCL OSINT feed
- CyberCure
- Emergingthreats.net
- I-Blocklist
- IP reputation.com
- IP spamlist
- IP void.com
- Iplists.firehol.org
- Lumension
- MalShare.com
- MalSilo
- Microsoft COVID feed
- NIST National Software Reference Library
- Osint.digitalside.it
- OTX (Open Threat Exchange)
- Phishtank
- Recorded Future
- Talos Senderbase
- SANS Top 20/Critical Security Controls
- Team Cymru
- TOR node list
- VX Vault
- X-Force Exchange

Netsurion Threat Center

EXTERNAL

INTERNAL

Analysts – at customer location, or Netsurion SOC

Netsurion®

### Local Threat Intelligence

- Behavior Anomaly
- VirusTotal
- Process Safelist
- IP Internal Safelist
- Internal Unsafelist

Global threat feeds are correlated for greater effectiveness and coverage. Local or community information augment comprehensive global feed data to provide optimum coverage. The Netsurion Threat Center combines that data with insights from internal sources such as:

- Behavior anomalies
- Process safelists
- IP internal safelists
- Internal unsafelists
- Contributions from our Netsurion SOC analysts as well as analysts at customer sites

## Benefits of Netsurion Threat Center

- Improve alerting by elevating the priority of rules that reference IoCs determined by current threat intelligence. These include public IP addresses with poor reputation, URLs, domain names and malware as well as MD5 hashes.
- Be notified automatically if an external IP address with a poor reputation communicates with assets behind your firewall
- Detect compromised systems that “phone home” from inside your network
- Review a history of IP addresses and incidents based on collected threat intelligence data to provide context for previous events and alerts related to specific IP addresses
- Correlate the presence of IoCs everywhere within your network for comprehensive remedial action

## How it Works

The Netsurion Threat Center continuously imports up-to-date information about top attackers, spammers, poisoned URLs and malware domains from a variety of threat feeds such as EmergingThreats.net, IPReputation.com, IPVoid.com, the NSRL and SANS.

These threat sources contain:

- Known Command and Control (C&C) hosts
- Attack response rules – data that systems on your network are likely to send back to a host after they have been compromised
- Compromised hosts
- Systems of known spammers
- Rules for detecting exploits, SQL injection, etc.
- User-Agent strings for known malware
- Web server attack detection rules

Internal sources of relevant intelligence provide another valuable layer of threat intelligence integration and monitoring. Also known as safelisting, internal intelligence includes a catalog of what is known and acceptable to the organization and is included in your threat Intelligence integration. The Netsurion Console will automatically generate, aggregate, and manage your internal and external intelligence feeds available from the Netsurion Threat Center.

The Netsurion Threat Center enables insightful context and actionable information for better decisions and a more proactive cyber defense.

* Threat feeds are constantly evaluated for effectiveness and may be adjusted.