SNORT3

SNORT

snort.org @snort

Snort 3 – Now available!

Welcome to Snort 3. Snort is an open-source intrusion prevention system (IPS) capable of real-time traffic analysis and packet logging. Snort 3 is the next step in our years-long journey of protecting users' networks from unwanted traffic, malicious software and spam and phishing documents.

New features

There are many benefits of upgrading to Snort 3. Some of the major new features and improvements in Snort 3 include:

- New rule parser and rule syntax.
- Support for multiple packet-processing threads, which frees up more memory for packet processing.
- Use of a shared configuration and attribute table.
- Access to more than 200 plugins.
- Rewritten TCP handling.
- Improved shared object rules, including the ability to add rules for zero-day vulnerabilities.
- New performance monitor.
- New rule remarks and comments that are inside of the rule itself.

For a comparison of Snort 3 features in relation to Snort 2, please see the chart on page 2.

Want to learn more?

We encourage everyone to shift over to Snort 3 from any versions of Snort 2. You can download the source from snort.org or pull it from GitHub. While moving to Snort 3 comes with a lot of improvements, we understand that not everyone can switch right away. This will allow any users who can't upgrade quickly plenty of time to get everything in order.

We have several resources and tools that can help whether you are brand new to Snort or migrating from Snort 2:

- Snort 101 videos covering Snort 3, including how to install and configure it, how to write rules and Snort 3 logging.
- How rules work differently in Snort 3
- Snort 3 GitHub page
- Improve Snort 3 performance with Hyperscan
- How the RNA inspector works in Snort 3
- Talos Takes "Snort 101" episode

If you have any questions, utilize one of our mailing lists to reach out to us, or refer to the Snort Resources page. You can always find the latest information on our Snort 3 website.

Snort 3 Comparison Chart

Feature	Snort 2	Snort 3
Packet threads	One per process	Any number per process
Config memory use	N processes * M GB	M GB total, more for packets
Config reload	N processes, slower	One thread that can be pinned to separate cores
Startup	Single-threaded, slower	Multithreaded, faster
Plugins	Limited to preprocs and outputs	Full plugin system with more than 200 plugins
DAQ	2.X, run to completion	3.X, vector input, multiple outstanding packets
DAQ Modules	Only legacy modules	Stacked modules, IOCTLs, file, socket and text modules
PCAP readback speed	X Mbits/sec for Max-Detect	2X with AC, 4X with hyperscan
IP Layers	Two max	Arbitrary and configurable limits
IP reputation	Complex with shared memory	Simplified process memory
Stream TCP	Complex implementation	New and improved implementation
Service detection	AppID only, port configs required	Autodetection, most port configs optional
HTTP inspector	Partly stateful	Fully stateful
Port scan detection	High, medium and low thresholds only	Fully configurable detection thresholds
Config parsing	Report one error and quit	Report all errors
Command line	Some overlapping with config file	Set to override any config filefrom the command line
Default config	Complex, needs tuning	Simplified, effective
Policy examples	None	Tweaks to fit all standard Talos policies
Policy bindings	One level	Nested
Rule syntax	Inconsistent and requires line escapes	Uniform system with arbitrary whitespace
Rule parsing	Buggy with limited warnings	Robust with numerous optional warnings
Rule comments	comments only	#, #begin/#end marks, C-style and rem options
Alert file rules	No	Yes
Alert service rules	No	Yes
Fast-pattern buffers	Six available	14 available
SO rule features	Restricted functionality	True superset of text rules
Simple SO rules	No	Yes
Dump built-in stubs	No (SO stubs only)	Yes
Runtime tracing	No (debug tracing and misc logs only)	Yes
Documentation	LaTeX-based PDF, READMEs	ASCII docs, text, HTML and PDFs
Command-line help	No	Yes
Source code	470,000 lines of C, with an average of 400 lines per file	389,000 lines of C++, with an average of 200 lines per file
Distribution	Snort.org tarballs, with updates coming every six months	GitHub repo, with updates coming every two weeks