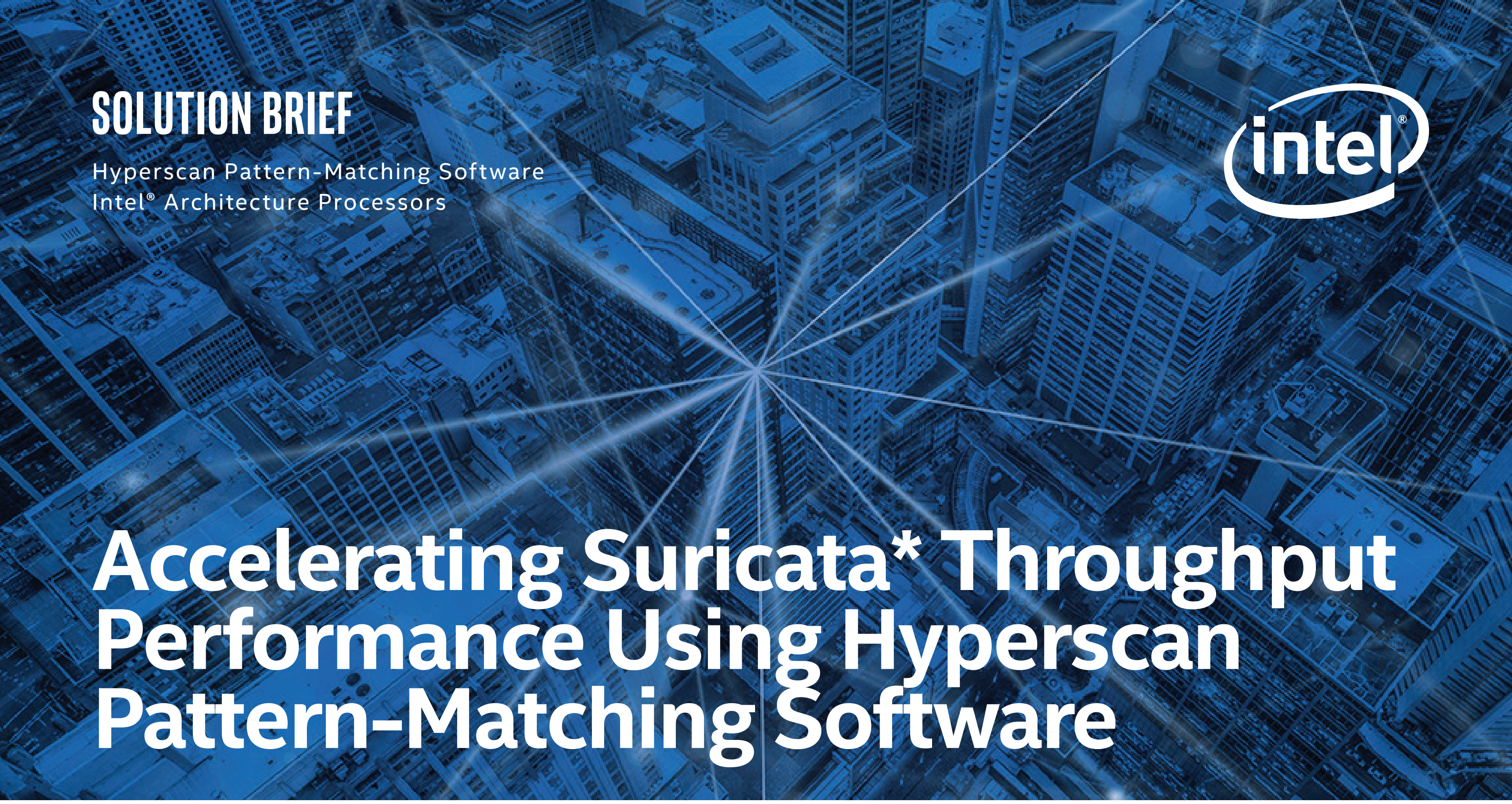

SOLUTION BRIEF

Hyperscan Pattern-Matching Software
Intel® Architecture Processors

Accelerating Suricata* Throughput Performance Using Hyperscan Pattern-Matching Software

Hyperscan enables the Suricata* Network Threat Detection Engine to run up to four times faster.

Hyperscan is now the default literal matching approach used by Suricata on modern Intel Architecture platforms.

Overview

With the rising sophistication of hacking and social engineering exploits, including ransomware worms such as WannaCry, leading top-level cybersecurity professionals are making dire predictions about the vulnerability of U.S. critical infrastructure and businesses. Of the 580 respondents to the 2017 Black Hat Attendee Survey[1],

- 60 percent believe a successful cyber attack on US critical infrastructure will occur in the next two years.
- About two-thirds think their own enterprises will be breached in the next 12 months.[1]

To help combat against such attacks, security professionals rely on solutions such as real-time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM), and offline packet capture (pcap) processing. These solutions typically perform high-speed content inspection by way of pattern matching, which is the ability to inspect all data against a database of security signatures. Many security solutions use the Suricata* network threat detection engine for content inspection because it is high performance, modern, clean, and highly scalable.[2]

Suricata is an open source-based intrusion detection system that was developed and is supported by the Open Information Security Foundation (OISF) under GPLv2 license. Suricata runs on standard, multicore Intel® architecture platforms, giving security solution vendors a cost-effective and flexible path to satisfy a wide range of market needs. The solution is also multi-threaded, enabling it to effectively use the large number of processor cores available on Intel® processors.

With Hyperscan it is possible to increase the throughput performance of Suricata by up to four times.[3] Hyperscan is an open source, high-performance multiple regular expression matching library that was released by Intel in October 2015 and is available at 01.org/hyperscan. Another benefit Hyperscan brings is it uses just one-tenth the fixed memory required by Suricata's default pattern matching implementation.[3]

Suricata Achieves Higher Levels of Performance with Hyperscan

"Hyperscan optimizes the most performance critical section of Suricata to achieve higher throughput, while at the same time allowing Suricata developers to focus on feature development and other optimizations instead of developing pattern matching algorithms themselves," according to Victor Julien, Suricata creator and lead developer.

To showcase the performance improvement Hyperscan brings to Suricata, Intel conducted throughput performance testing on Suricata with Hyperscan enabled. The test setup employed HTTP enterprise traffic from the Ixia AppLibrary* included in IxLoad*. An Ixia traffic generator sent stateful traffic to an Intel® Xeon® Gold 6130 processor–based platform (see Appendix A) running Suricata.

Figure 1 shows the resulting Suricata performance with and without Hyperscan and with one or two processor cores allocated. Test results demonstrated that adding the Hyperscan enabled to Suricata increased its throughput performance by up to four times. Throughput is measured by the total number of packets processed by Suricata without any packet loss.

Also, the Hyperscan implementation scaled nearly linearly with the number of cores, increasing performance by 1.9 times as the number of cores doubled. Performance gains from adding more cores varied by the test scenario.

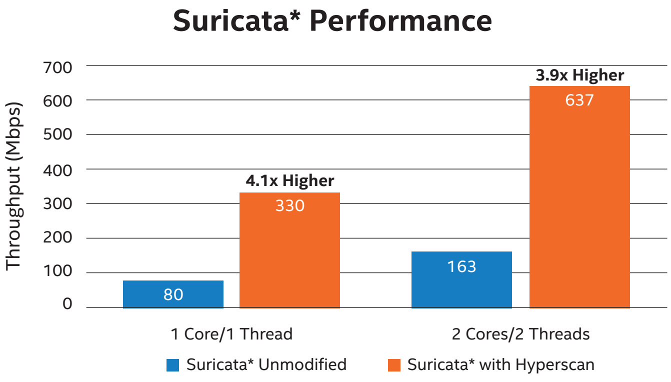

Figure 1. Suricata* performance with and without Hyperscan and with one or two processor cores assigned

Resource Efficiency – Small Memory Footprint

Hyperscan has the ability to compile large pattern databases into a small memory footprint, helping security appliance vendors dramatically reduce memory requirements. When using cache-rich Intel Xeon processors, the database may even be small enough to remain in cache, which can significantly boost throughput. Additionally, Hyperscan significantly minimizes shared-memory contention in multicore systems.

Hyperscan is also highly efficient with respect to fixed system memory. For a typical rule set, it builds a pattern database that is approximately one-tenth the memory size of the corresponding database created by Suricata's native pattern-matching software. Intel's testing demonstrated a savings of approximately 72 MB, as shown in Figure 2 (full configuration details are included in Appendix A).

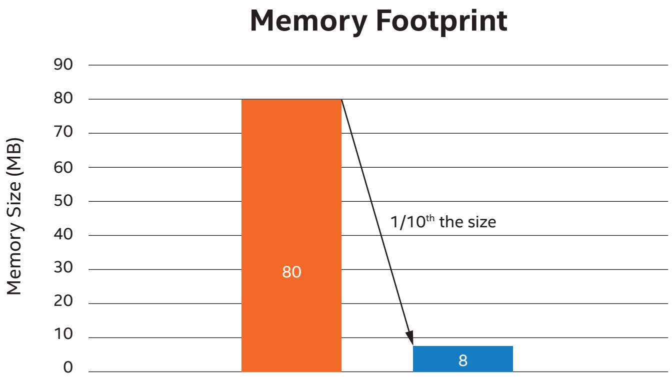

Figure 2. Hyperscan is one-tenth the size of the native Suricata* pattern matcher

Vector Processing Capabilities Improve Performance

The latest version of Hyperscan has been designed to take advantage of vector processing capabilities to execute more pattern-matching operations per clock cycle than is typically possible using standard instructions. This capability is further enhanced in the Intel Xeon Gold 6130 processor, which integrates Intel® Advanced Vector Extensions 512 (Intel® AVX-512), a set of new instructions designed to accelerate many workloads.[4]

High-Performance, Software-Based Security Solution

The combination of Suricata, Hyperscan, and Intel processors gives security solution vendors a high-performance alternative to using custom, purpose-built hardware, like ASICs and FPGAs, that tend to be relatively expensive and inflexible. Suricata runs on Intel Xeon, Intel® Core™, and Intel® Atom™ processors with varying CPU frequencies, numbers of cores, cache sizes, and sockets per board. This flexibility allows vendors to scale network throughput and satisfy the needs of different market segments without the added cost of working with multiple platform architectures.

For more information about Hyperscan, visit http://www.intel.com/content/www/us/en/communications/hyperscan.html

Appendix A: System Configuration

Hardware Platform		
Motherboard		Intel Corporation
CPU	Product	Intel® Xeon® Gold 6130 processor
	Speed (GHz)	2.10 GHz
	Number of CPUs	16 cores / 32 Threads / 2 Sockets
	Stepping	H0
	L1d cache	32 KB
	L12 cache	32 KB
	L2 cache	1,024 KB
	L3 cache	22,528 KB
System Memory	Vendor	Samsung*
	Type	DDR4-2400 RDIMM
	Configured speed	2,400 MHz
	Part number	M393A1G43DB1-CRC
	Size per DIMM	8 GB
	Channel	1 DIMM/Channel, 6 Channels per socket
BIOS	Vendor	Intel Corporation
	Version	Release Date: 12/15/2016
OS	Vendor	Ubuntu 16.04 LTS 64-bit
	Version	4.4.0-75-generic
Network Interface Card		1 x Intel® 82599 dual port PCI Express x8 10Gb Ethernet NIC

Suricata* and Hyperscan Software Setup	
Suricata* version	3.2
Hyperscan version	4.4.1
Suricata ruleset	Emerging Threats
Total no. of signatures processed	13,438

Ixia Setup for Network Traffic Generator	
IxLoad* version	Build 8.20
10 GbE module	PerfectStorm* 10GE
Traffic	HTTP Enterprise from Ixia

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit www.intel.com/benchmarks.

[1] "Portrait of an Imminent Cyberthreat," 2017 Black Hat Attendee Survey, July 2017, pgs. 3-4, www.blackhat.com/docs/us-17/2017-Black-Hat-Attendee Survey.pdf.

[2] https://suricata-ids.org/features

[3] Intel test results using the system configuration shown in Appendix A.

[4] Intel® technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://www.intel.com.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATHMAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548- 4725, or by visiting Intel's Web site at www.intel.com.