IMPLEMENTATION SUMMARY

Security Solution Implementation Summary

Intel Corporation
Datacenter Network
Solutions Group

Authors

Eduardo Castro
Solution Software Engineer,
Intel Corporation

Tarek Radi
Lead Technical Program Manager,
Intel Corporation

Table of Contents

1.0 Introduction

This Solution Implementation document presents how network function virtualization infrastructure (NFVI) and virtual network functions (VNFs) may be applied to create a complete and performant virtualized security solution. This solution may lead to a reduction of total costs of ownership and a faster response to scaling needs over the infrastructure built with the use of traditional, physical appliances.

The primary audiences for this document are architects and engineers planning to implement their own virtualized security architectures. Readers should use this document as a demonstration of how effective protection against internal-to-internal attacks is possible in SDN/NFV.

This document can also assist those who are interested in implementing security protection mechanisms in an SDN/NFV world.

It is important to note that the details contained herein are just an example of one way of applying security functions for a customer. Intel does not aim to promote or recommend any specific hardware, software, or supplier mentioned in this document. In addition, Intel does not aim to tie customers to any specific software and hardware stack.

2.0 Solution Overview

Cerner Corporation, Intel Corporation, and Midokura have teamed up to deliver a complete OpenStack based virtual security solution that provides visibility and control against malicious activity within the software-defined data center of Cerner Corporation, securing east-west traffic.

Cerner Corporation is a healthcare electronic medical records services provider, expanding its direction toward gathering and analyzing the world's healthcare data to make the delivery of healthcare more efficient. Cerner's technologies connect people and systems at more than 18,000 facilities worldwide, such as hospitals, ambulatory, and physician offices.

Cerner Corporation is providing its services with private clouds. One of the results of the strict security policy in Cerner is the use of physical intrusion prevention and detection systems (IPS/IDS) located at the edge of the data centers. Currently any traffic at Cerner's private cloud must be redirected to remote, physical IPS/IDS for packet inspection. Although such an architecture model is acceptable for north-south traffic, a trombone effect appears when traffic goes between virtual machines (VMs) located in the same data center.

Figure 1 describes the currently used architecture and shows an example of traffic between the two VMs located at the same host server within the cloud. The virtual extensible LAN (VXLAN) traffic from VM1 is redirected via the Midokura Enterprise MidoNet* vSwitch to the router and the gateway at the edge of the cloud, and reaches the physical IPS/IDS device. Once the traffic is inspected, it is sent back through the gateway to the cloud, and through the router and vSwitch it reaches the target VM2.

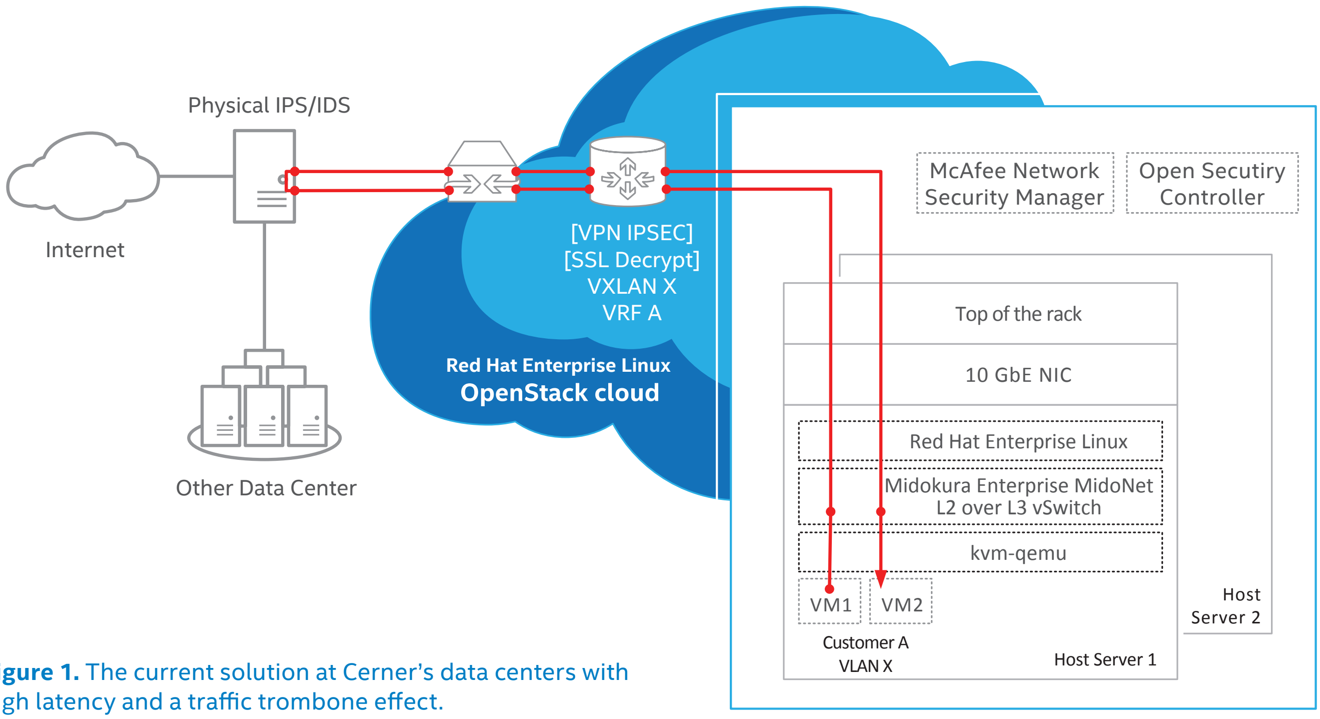

Figure 1. The current solution at Cerner's data centers with high latency and a traffic trombone effect.

Such flow characterizes high latency and may potentially lead to congestions on the links connecting clouds and IPS/IDS devices.

The proposed solution eliminates this problem as traffic is inspected locally within the cloud through the use of virtual security functions. In this solution, we do not replace the physical IPS/IDS appliances. These are now used to inspect the north-south traffic and east-west traffic coming from outside the cloud.

To support inspection of the east-west traffic within the same cloud, we installed virtual IPS (vIPS) functions at each compute node of the cloud. Figure 2 describes the scenario where the connectivity is established between two VMs on the same compute node. In this case, the traffic from VM1 flows via the MidoNet switch to the vIPS on the same node. After inspection, the MidoNet switch redirects the traffic to the target VM2.

Alternatively, if the traffic flows out from a VM located at another compute node (e.g. on Host Server 2) and a different tenant of the same cloud, the OpenStack router will be utilized to pass the traffic via the MidoNet virtual switch to the target VM2 on Host Server 1.

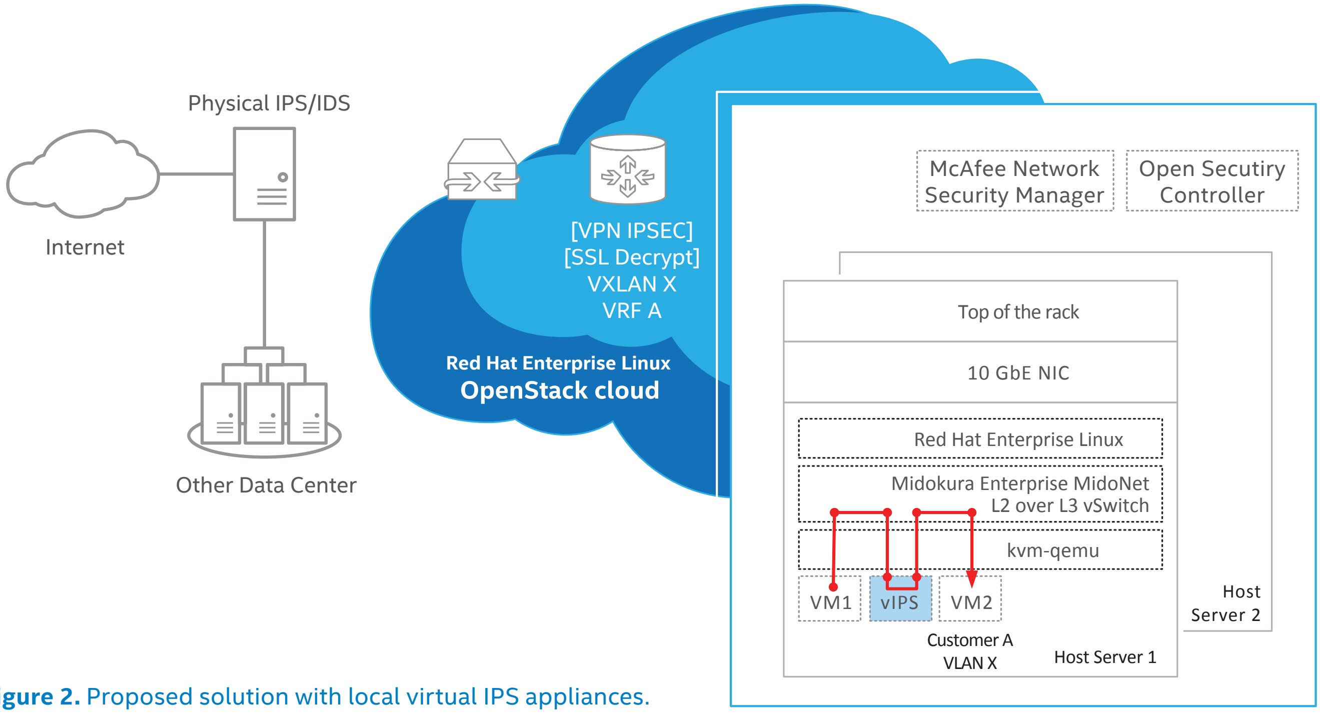

Figure 2. Proposed solution with local virtual IPS appliances.

With the use of the OpenStack cloud, the scalability of the cloud is easy, and deployment of virtual functions is done in an automated manner. With this solution, we managed to maintain at least the same level of security, as with the use of physical IPS appliances without sacrificing performance.

The solution is using the Intel® Open Network Platform reference architecture as a spring board. Deployment is done on standard high volume servers based on Intel® Xeon® processor E5 2699 v3 processors running Red Hat Enterprise Linux 7.1. Table 1 provides the details on the server configuration.

All the servers present the similar configuration. The two servers based on Intel® Server Board S2600WT2 were dedicated to Controller/Compute1 and Compute2, while Supermicro SuperServers* were used in Compute 3 and Analytic Server.

The 40 GbE QSFP+ port on the Intel® Ethernet Controller XL710-BM1-based card is used for the Data Network, while the External and Management networks were using 1 GbE ports controlled by the Intel® Ethernet Controller I350. The network connectivity and physical topology is presented in Figure 3.

The cloud and VNF orchestration is provided by Red Hat OpenStack Platform 7. Midokura has supplied the solution with Midokura Enterprise MidoNet 5.02, an enterprise-grade virtual switch, and the Midokura plug-in for Open Security Controller (OSC), acting as the SDN controller. This scalable solution is VNF agnostic, and the services are delivered through the OSC 2.5 and the vIPS functions. Table 2 lists all the software components of the solution.

Table 1. Specification of servers.

SERVER	SPECIFICATION	NODES
2× Intel® Server	• Intel® Server Board S2600WT2 • Dual Intel® Xeon® processor E5-2699 v3, 2.30 GHz, 45 MB cache, total 36 cores and 72 virtual cores reported in BIOS • Memory: 16× 8 GB (total 128 GB) 2133 MHz DDR4 • 2× 1 GbE ports via Intel® Ethernet Controller I350 (rev 01) • 1× 40 GbE QSFP+ via Intel® Ethernet Controller XL710-BM1 (rev 02) • Storage: 1 TB HDD, 7200 RPM	• Controller/Compute1 • Compute2
2× Supermicro SuperServer* 6028U-TR4+	• Supermicro X10DRU-i+ Motherboard • Dual Intel® Xeon® processor E5-2699 v3, 2.30 GHz, 45 MB cache, total 36 cores and 72 virtual cores reported in BIOS • Memory: 8× 16 GB (total 128 GB) 2133 MHz DDR4 • 4× 1 GbE ports via AOC-2UR68-i4G Intel® Ethernet Controller I350 (rev 01) • 1× 40 GbE QSFP+ via Intel Ethernet Controller XL710-BM1 (rev 02) • Storage: 2 TB HDD	• Compute3 • Analytic Server

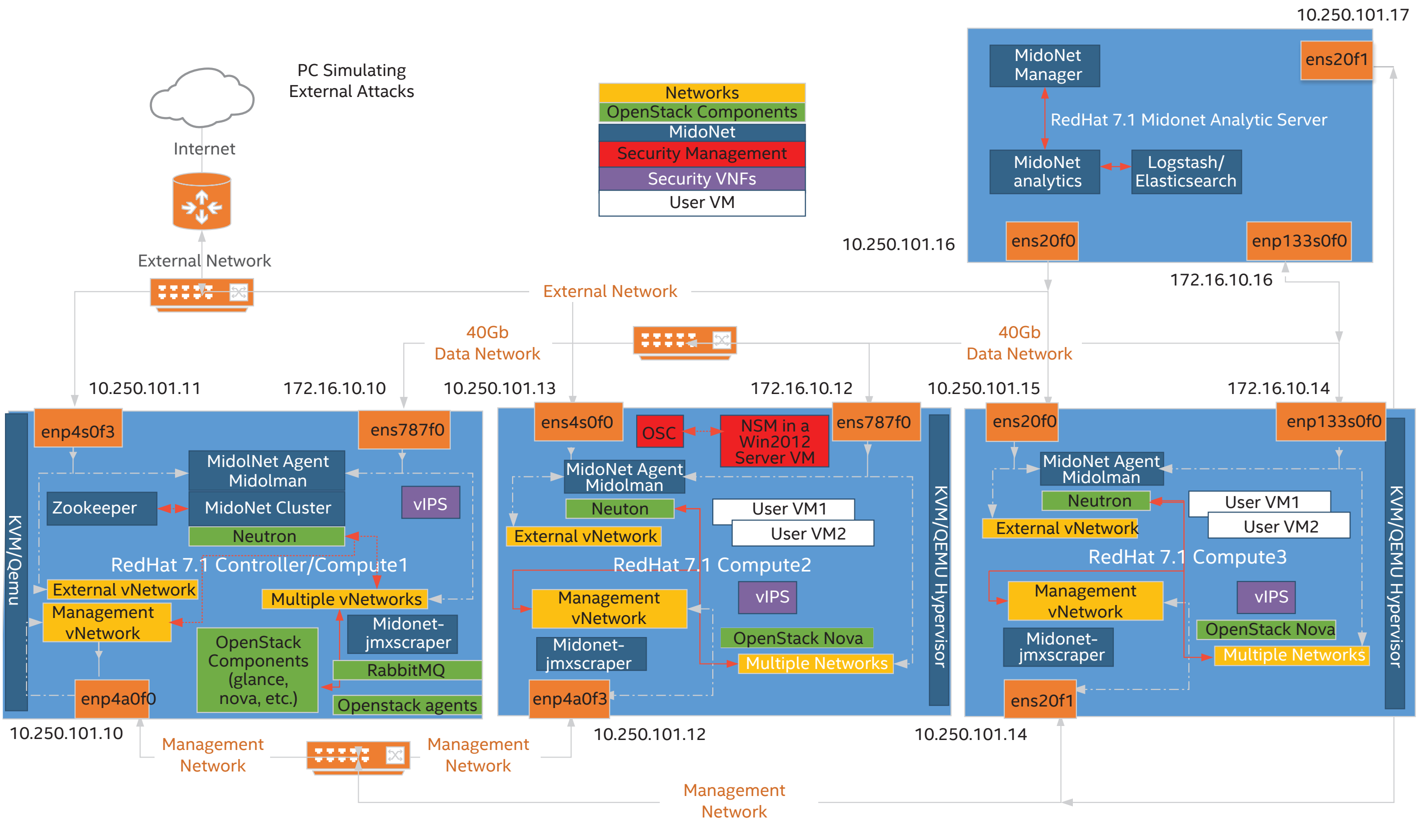

Figure 3. Physical setup.

The Analytic Server provides with the network telemetry data and functions that are supplied by Midokura Enterprise MidoNet and is deployed to enable robust security and network management.

To fully utilize the capabilities of analytic functions, Midokura and Intel Security implemented a new feature in SDN controller that uses 6-tuple signature in the API. This implementation enhances the traditionally used 5 tuple based traffic filtering policy (i.e., using source and destination IP addresses and ports, and protocol information) with information on the flow timestamp of a VM.

OSC and the SDN controller can query the telemetry database on Midokura Enterprise MidoNet Analytic Server to get all the information about the attacker including its private IP and the actual name of the VM, even if it is on a different tenant, and even the attacker traffic is not inspected by vIPS. With this feature, it is not required to protect all the VMs but only the destination VM. Specifically, implementation is a change in the API signature of the SDN controller and the vIPS API that allows you to get information about the source VM and the destination VM of the attack.

Table 2. Software components.

FUNCTION	PRODUCT
Operating system	Red Hat Enterprise Linux* 7.1
Hypervisor	qemu-kvm* 2.1.2
Infrastructure orchestration	Red Hat OpenStack Platform 7
Virtual switching	Midokura Enterprise MidoNet* 5.0.2
SDN controller	Midokura MidoNet plug-in version 1.0034
Security function policy management	Open Security Controller 2.5
Security appliance management	McAfee® Network Security Manager 8.3.7.500.2
Virtual security function with vIPS	McAfee® Network Security Platform virtual sensor 8.1.7.40 (vIPS)
Virtual load balancer	F5 BIG-IP-12.0.0.0.0.606
Network analytics	Midokura Enterprise MidoNet 5.01

3.0 Demo: Cross-Tenant Cross-Machine Attack

Tenants in OpenStack are different projects that represent different customers of Cerner. The demo was designed to simulate two different customers inside the cloud, and perform the attack from one project to another.

The demo shows the interaction of VMs in a multi-tenant environment, where one VM represents the attacker (in Tenant 2) and the other VM is the destination of the attack (in Tenant 1). The MidoNet SDN controller redirects the traffic for inspection to the Security Tenant (Intel ISC Tenant), containing security functions, that is, OSC, McAfee® Network Security Manager and vIPS. The vIPS performs analysis of the packets. If packets correspond to the malicious activity, these will be blocked; otherwise, packets will continue the normal data path.

The details of the demonstration, including setup and output, can be found in the Solution Implementation Installation Guide: https://networkbuilders.intel.com/network-technologies/solution-blueprints

Demo Setup

Scenario #1

a) Protect Load Balancer only (on controller)

b) Access LB (with & without attack)

c) View results in Real Time Threat Analyzer

Scenario #2

a) Protect Web3 only (on compute)

b) Access LB (with & without attack)

c) When LB uses Web3, it is protected

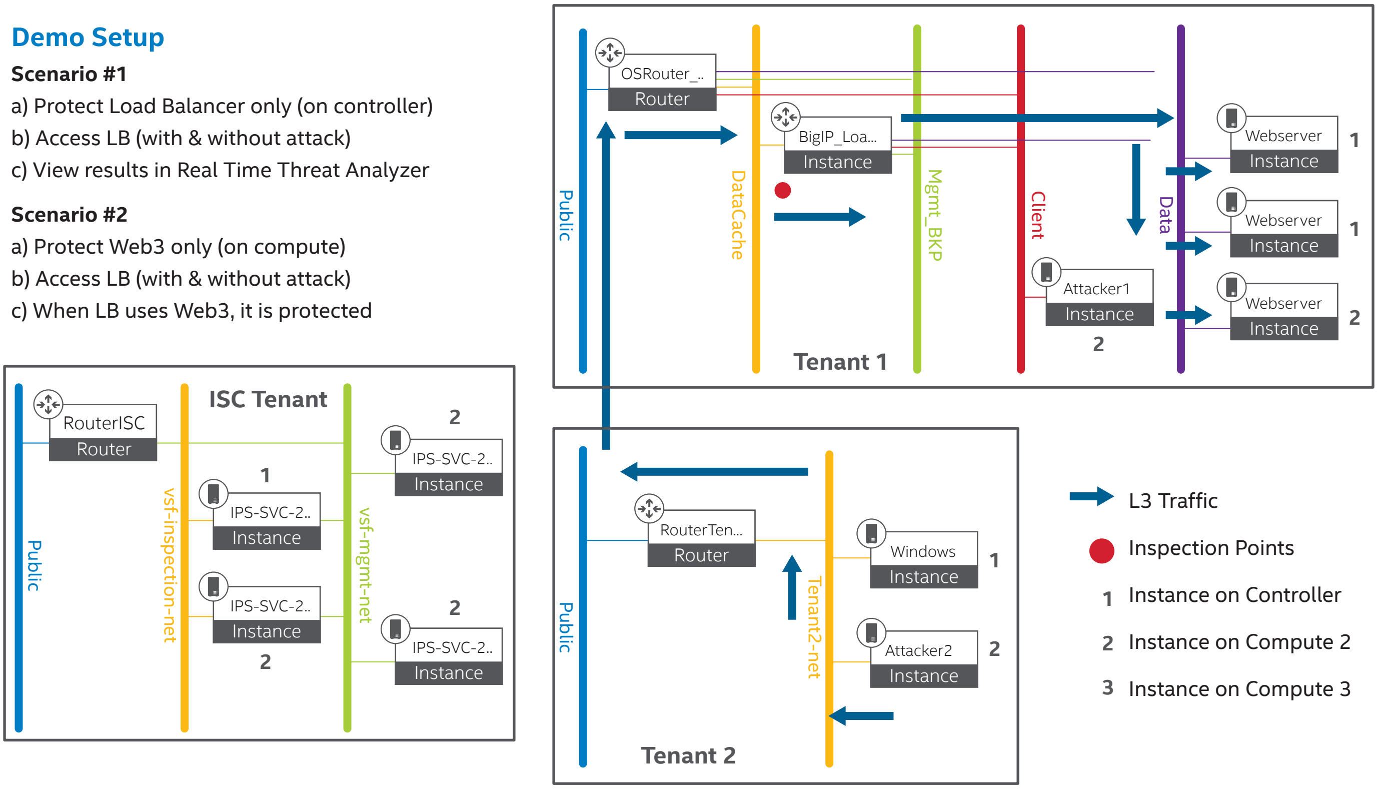

Figure 4. Demo: Cross-tenant cross-machine attack

4.0 Next Steps

- To learn more about the technologies mentioned in this paper, please follow the links.
- To learn more about Intel's technology for NFV, attend the courses available in the Intel® Network Builders University at https://networkbuilders.intel.com/university.
- To learn more about Intel® Network Builders partners for NFV products, visit https://networkbuilders.intel.com/solutionscatalog.
- To build a test bed using the Intel® Open Network Platform Reference Architecture, download the documentation at https://01.org/packet-processing/intel%C2%AE-onp.
- To get the highest performance from your NFV systems, specify compatibility with the Data Plane Development Kit in your infrastructure and VNF procurements.
- To get the highest return on investment from your NFV systems, specify use of Enhanced Platform Awareness in your orchestration, infrastructure, and VNF procurements.

Appendix A: References

NAME	REFERENCE
Case Study: Intel® Server Technologies Provide Healthy Outcomes for Cerner and Its Clients	http://media12.connectedsocialmedia.com/intel/04/7986/Cerner_Healthy_Outcomes.pdf
F5 BIG-IP	https://www.f5.com/pdf/products/big-ip-local-traffic-manager-ds.pdf
Open Security Controller	http://www.intel.com/content/dam/www/public/us/en/documents/datasheets/open-security-controller-datasheet.pdf
McAfee® Network Security Manager	http://www.intel.com/content/dam/www/public/us/en/documents/datasheets/open-security-controller-datasheet.pdf
McAfee® Network Security Platform virtual sensor	http://www.mcafee.com/us/resources/data-sheets/ds-virtual-network-security-platform.pdf
Midokura Enterprise MidoNet*	http://www.midokura.com/midonet-enterprise/
Red Hat Enterprise Linux* 7	https://www.redhat.com/en/resources/red-hat-enterprise-linux-server
Red Hat OpenStack Platform 7	https://access.redhat.com/documentation/en/red-hat-openstack-platform?version=7/

Appendix B: Acronyms and Abbreviations

ABBREVIATION	DESCRIPTION
HDD	Hard Disk Drive
OSC	Open Security Controller
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
LB	Load Balancer
NFV	Network Functions Virtualization
NSM	McAfee® Network Security Manager
SDN	Software-Defined Networking
vIPS	Virtual Intrusion Prevention System
VM	Virtual Machine
VNF	Virtualized Network Functions
VXLAN	Virtual eXtensible LAN

By using this document, in addition to any agreements you have with Intel, you accept the terms set forth below.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

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.

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.

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.

Intel technologies may require enabled hardware, specific software, or services activation. Check with your system manufacturer or retailer. Tests document performance of components on a particular test, in specific systems. Differences in hardware, software, or configuration will affect actual performance. Consult other sources of information to evaluate performance as you consider your purchase. For more complete information about performance and benchmark results, visit http://www.intel.com/performance.

All products, computer systems, dates and figures specified are preliminary based on current expectations, and are subject to change without notice. Results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

No computer system can be absolutely secure. Intel does not assume any liability for lost or stolen data or systems or any damages resulting from such losses.

Intel does not control or audit third-party websites referenced in this document. You should visit the referenced website and confirm whether referenced data are accurate.

Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights.