

## Solution Brief

### Modular Security Architecture

Check Point\* IPS Software Blade

Intel® Xeon® Processor E5540 with Quad-Core Technology



**Check Point**  
SOFTWARE TECHNOLOGIES LTD.

## Top 5 Reasons to Deploy Modular Security Architecture

For IT professionals, it seems like security solutions are proliferating as fast as security threats. Security environments are growing in complexity because it's necessary to continually add more and more functions, like firewalls, intrusion prevention systems (IPS), IPsec VPN and antivirus, just to name a few. When these functions are supported by distinct appliances, they can be difficult to integrate, test and manage.

Instead of deploying disparate security boxes, enterprises are migrating to independent security modules that all run on a single platform, simplifying integration and management. These security modules can be deployed on a gateway or management system by just 'turning on' functionality – no hardware, firmware or driver upgrades required. This flexibility enables IT organizations to deploy security functions dynamically, as needed, with lower total cost of ownership. The migration to modular security architecture has accelerated, in part due to power-efficient multi-core processors that deliver exceptional performance in a relatively small form factor. Today's processors support over 15 gigabit per second (Gbps) IPS throughput, so enterprises can have robust protection without sacrificing network speed. This solution brief explores the key advantages of deploying modular security architecture in enterprise infrastructure.

## Introducing the Software Blade Architecture

Check Point\* Software Technologies has developed a unique Software Blade architecture to enable IT organizations to consolidate security functions onto a single system while still maintaining network performance service level agreements (SLAs). The Check Point Software Blade Architecture features independent and flexible security modules that allow organizations to select the functions they want in a custom security solution. Similar to various hardware blades running in self-contained chassis, software blades are modular, interoperable security functions that share a common platform, called a 'container', as illustrated in Figure 1. The container, running on a multi-core processor-based server, controls software blade operations and ensures efficiency, scalability and central manageability. Like hardware blades, software blades can be added, swapped or removed, as needed.

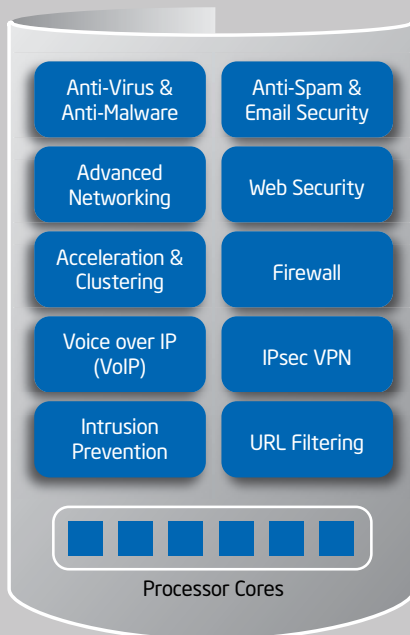


Figure 1. Software Blade 'Container' for Security Functions

## Modular Security Architecture

Neutralizing emerging threats requires an adaptable security solution that brings enhanced security features on-line quickly. What could be faster than just activating a software function that's already present on the security platform? This is achievable with independent software security modules running on a powerful, general-purpose server equipped with the latest multi-core processors. In contrast, many of today's security appliances are based on specialized hardware with relatively fixed capabilities, which limits their performance value over time. The following discusses five reasons why IT departments should consider adopting modular security architecture.

### Top 5 Reasons to Deploy Modular Security Architecture

**Flexibility** – When business needs change, modular security architecture enables relatively simple configuration and policy upgrades and modifications. IT organizations can implement new functions or move functions to another hardware platform in a seamless manner, with no downtime, because systems are preloaded and pre-validated with a comprehensive set of security functions (Figure 1). System performance simply scales with the number of active processor cores and security functions, which allows the solution to address today's and tomorrow's needs.

**Cost** – IT organizations can tailor their gateways to run the exact security functions required to enforce policy and thus avoid overhead for unused security functions. The security solution is consolidated on one platform, as opposed to multiple independent solutions, reducing hardware footprint, rack space, cabling and utility costs. Modular security solutions also use general-purpose hardware, which is typically less expensive than specialty hardware.

**Latency** – A security environment comprising various security appliances can be susceptible to bottlenecks that increase latency. For example, content-based analysis is often a bottleneck, as shown in Figure 2, although just 10 percent of the traffic is normally subjected to deep packet inspection. Alternatively, delay can be reduced by inspecting traffic once for both firewall and IPS protection, which is achievable through enhanced security function coordination enabled by modular architecture.

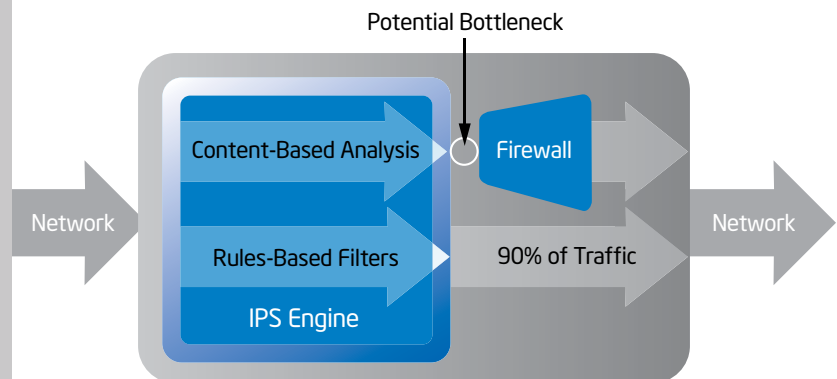


Figure 2. IPS Exception Handling

**Security policy cohesion** – It's crucial to have the right level of security at every enforcement point and at all layers of the network in order to effectively reduce exposure to security threats. Without a central management capability, it can be difficult to orchestrate a cohesive security policy across enterprise infrastructure that comprises many security touch points. By design, equipment based on modular architecture is centrally managed, making it easier to dictate traffic flow and apply security functions judiciously.

**Efficiency** – With a single comprehensive modular security system, it's no longer necessary to support multiple security devices, which reduces the number of administrative tasks, such as updating, monitoring, event analysis and reporting. Deployment time and costs are reduced because new security functions are easily added to the existing security infrastructure. A single system with central management software increases efficiency and operational effectiveness and curtails errors and oversights.

## Check Point\* IPS Software Blade

Information security professionals are looking for the right level of protection at the right level of investment. They are aligning IT security projects with business needs, amidst declining budgets. However, security products often take a 'one-size fits all' approach, which may not support special security needs or could force companies to pay for unused functionality.

Helping IT departments achieve their cost/performance goals, Check Point\* Software Blade Architecture delivers a simple, flexible and manageable total security solution. A key component of the solution is the IPS Software Blade that can be integrated into any Check Point Security Gateway or appliance with other security functions such as firewall, VPN and VoIP security. The IPS Software Blade provides complete intrusion prevention and threat coverage for clients, servers, OS and other vulnerabilities, at multi-gigabit speeds. This security solution employs a multi-tier threat detection engine that combines signatures, protocol validation, anomaly detection, behavioral analysis and other methods to provide the highest levels of network IPS protection.

The IPS Software Blade only performs deep inspection on the relevant sections of the traffic, which reduces overhead, increases accuracy and offers greater network security without degrading gateway performance. Figure 3 illustrates how the IPS Software Blade is integrated into a broader security framework.

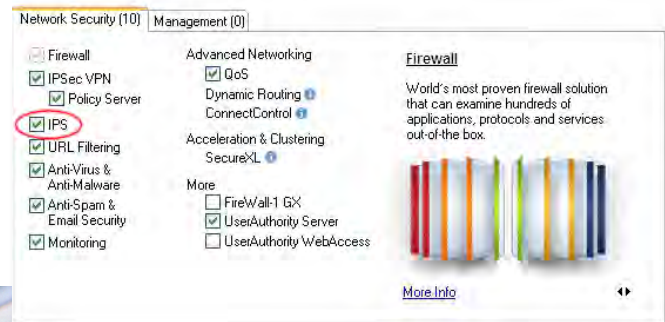
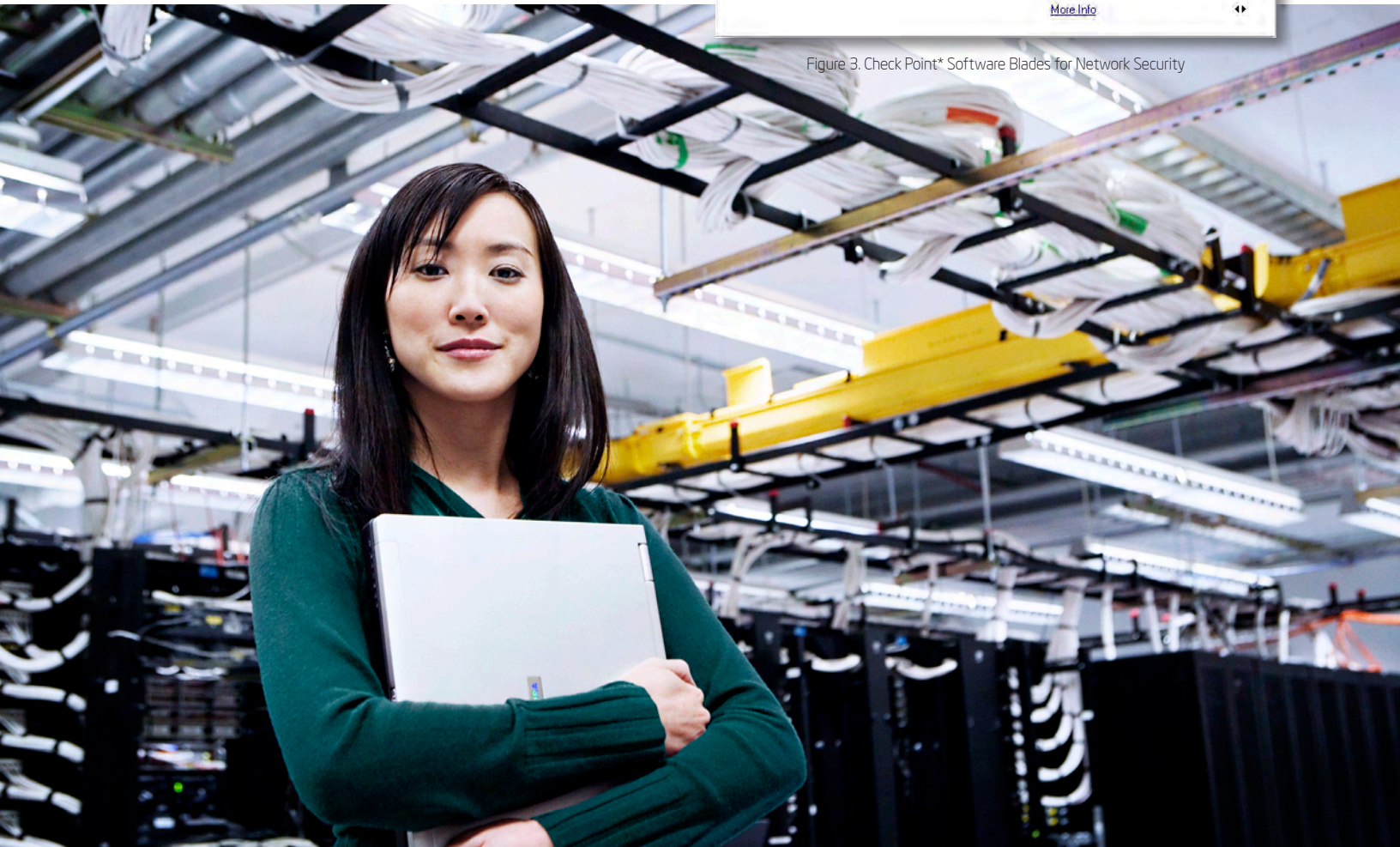


Figure 3. Check Point\* Software Blades for Network Security



## Fast Deployment and Optimized Performance

The Check Point IPS Software Blade ships with predefined default and recommended profiles, which provide an out-of-the-box configuration tuned to optimize security or performance. An optional profiling mode sets the existing protections to detect-only, enabling IT departments to evaluate their profiles without risking disruption. Granular protection control allows administrators to define signature and protection activation rules that match the corporate security requirements for their network assets.

Security performance metrics are captured on an easy-to-read dashboard, shown in Figure 4. In addition to fast deployment and optimized performance, the Check Point Software Blade Architecture provides benefits addressing flexibility, TCO (total cost of ownership), consolidation and investment protection, as described in Table 1.

Features	Benefits
Comprehensive set of security modules	Increases deployment flexibility
15 Gbps IPS and complete security protection	Delivers guaranteed performance
Simple deployment and central management	Lowers TCO
Easy migration and scaling	Simplifies consolidation
New security functions (Check Point* Software Blades)	Protects investment run on existing platforms

Table 1. Key Benefits of the Check Point\* Software Blade Architecture

## Improving Processor Microarchitecture

Multi-core processors are a critical ingredient in a system running modular security software. Security functions running on dedicated processor cores are in effect deterministic because they're not interrupted by other software tasks. Multi-core technology advances are also delivering ever-increasing levels of performance, while keeping power consumption in check. For example, the Intel® Xeon® processor 5500<sup>4</sup> series has greater overall performance and power efficiency compared to its predecessor, the Intel® Xeon® processor 5300 series, both quad-core processors. The combination of the Intel Xeon processor 5500 series and the Check Point Software Blade Architecture has increased IPS throughput by 3.3<sup>5</sup> times over successive generations of Check Point Solutions, as shown in Figure 5.

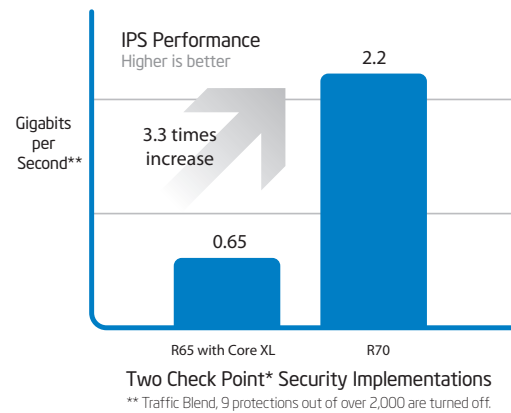


Figure 5. IPS Throughput for Two Generations of Check Point\* Solutions

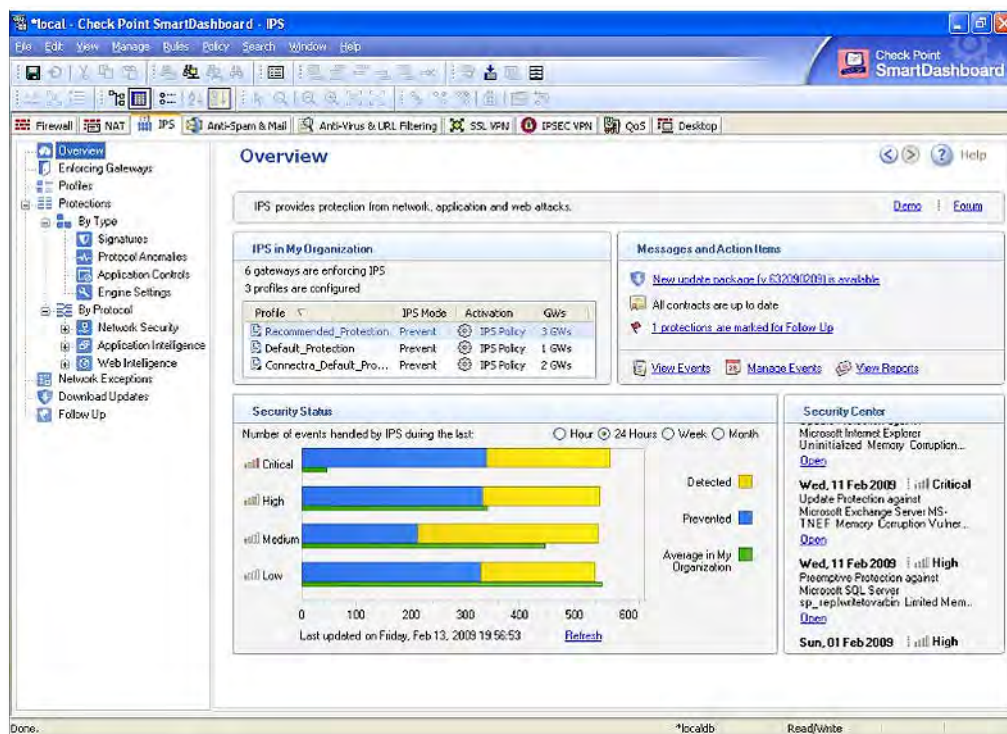
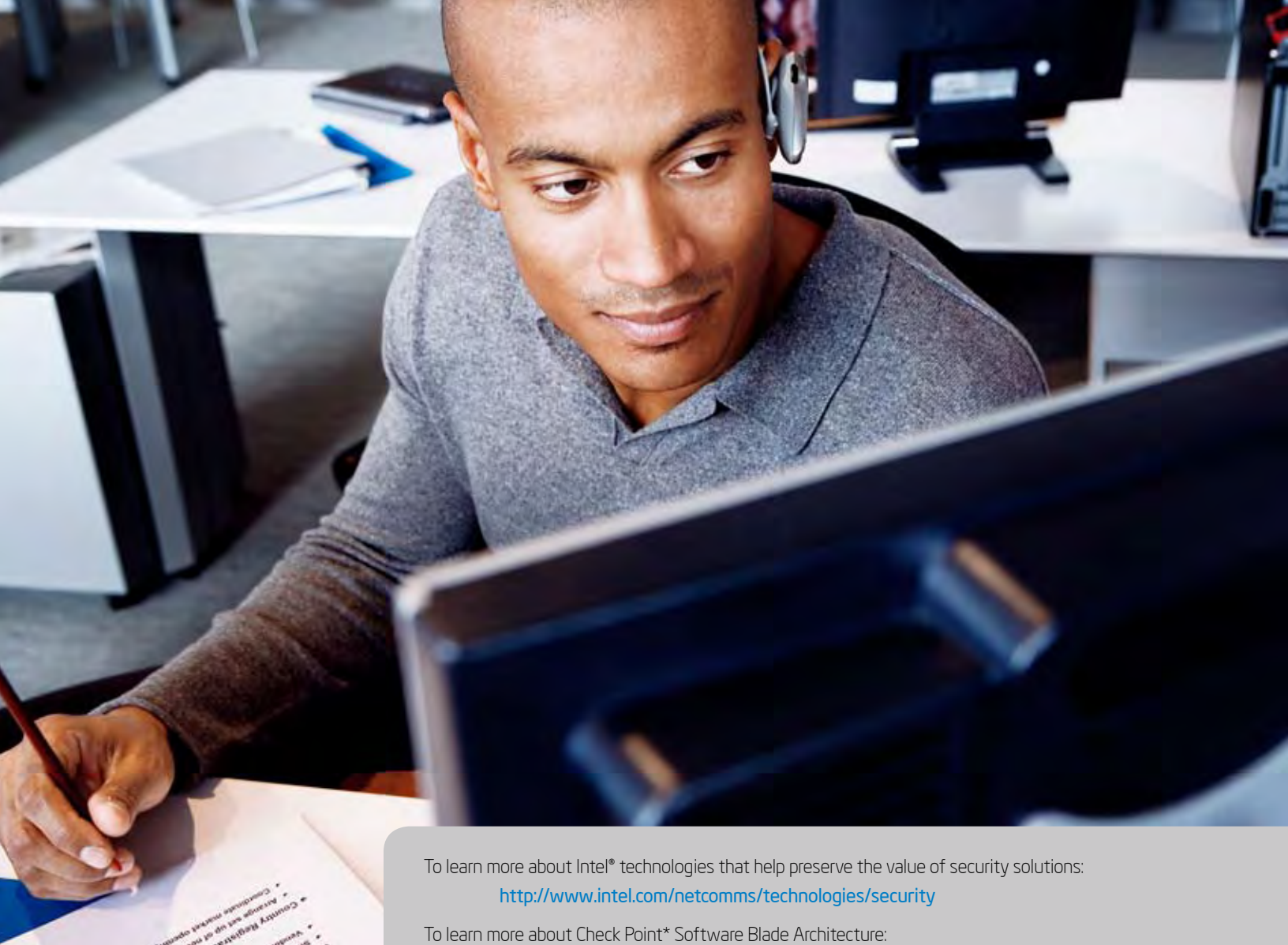


Figure 4. The IPS Management Tab Within the Check Point\* SmartDashboard



To learn more about Intel® technologies that help preserve the value of security solutions:

<http://www.intel.com/netcomms/technologies/security>

To learn more about Check Point\* Software Blade Architecture:

<http://www.checkpoint.com/products/softwareblades/architecture>

Intel has made many significant changes to its processor architecture that increase compute performance and power efficiency. The performance increase is a result of various architectural enhancements, such as adding a thread per processing core, integrating L3 cache memory on-chip and migrating to faster memory technology. Figure 6 illustrates these microarchitecture changes, showing the key difference between the Intel Xeon processor 5300 and 5500 series.

1. **Intel® Hyper-Threading Technology:** Adds a second thread to each core, which increases processing capacity.
2. **L3 cache added on:** Integrates an additional cache memory system (shared by all four cores) that eliminates redundant copies in other caches and offers a low latency mechanism for cores sharing data.
3. **Memory controller added on-chip:** Reduces memory latency, processor system footprint and power consumption.
4. **Faster system memory and more channels:** Increases memory bandwidth.

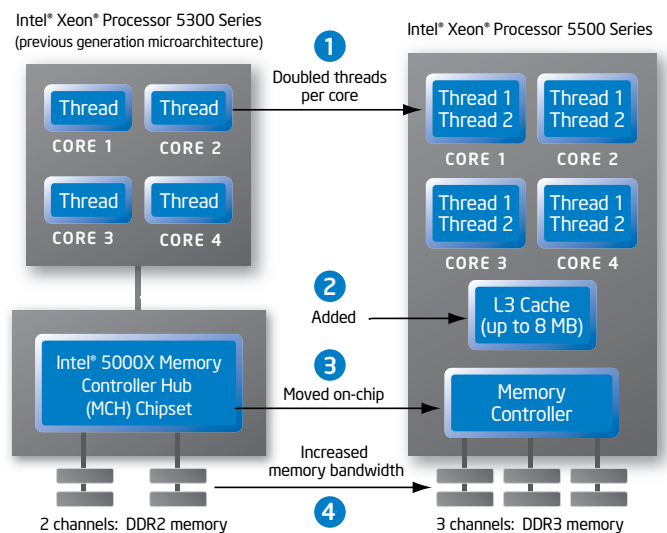
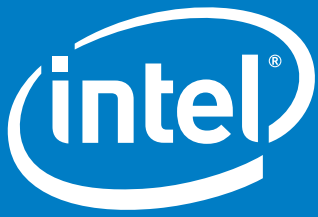


Figure 6. Intel® Xeon® Processor E5540 with Quad-Core Technology Enhancements



www.intel.com

<sup>^</sup> Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families.

See [www.intel.com/products/processor\\_number](http://www.intel.com/products/processor_number) for details.

<sup>†</sup> Performance tests and ratings are measured using specific computer systems and/or components and reflect approximate performance of Intel® products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products,

visit [http://www.intel.com/performance/resources/benchmark\\_limitations.htm](http://www.intel.com/performance/resources/benchmark_limitations.htm)

Copyright © 2009 Intel Corporation. All rights reserved. Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. or its subsidiaries in the United States and other countries.

\*Other names and brands may be claimed as the property of others.

Printed in USA 0409/MS/SD/XX/PDF Please Recycle Order No. 321793-001US