CASE STUDY
Intel® AES-NI
Intel Security Solutions

Strengthen Cloud Security with Intel® Advanced Encryption Standard New Instructions

Tier 3 Expands Its Security Portfolio with Intel Security Solutions

If you've ever been river rafting, you might have felt that wearing a life preserver and helmet while navigating calm waters is pointless. But when you're facing the roar of white water rapids, you know that your safety equipment could save your life.

River rafting is not unlike your journey to the cloud. When you virtualized a few core services and consolidated underutilized servers, nobody seemed to notice or care. Now that you're looking at a cloud deployment, you can be sure that lots of people care. Like a life preserver and helmet protect your life on the river, security measures such as Advanced Encryption Standard (AES) encryption can help protect your data in the cloud.

Tier 3 knows the value of protecting data. As a leading provider of enterprise-class cloud software and federated cloud services, Tier 3 helps organizations securely expand their infrastructure into the cloud without incurring large capital expenses or additional administrative overhead.

But it is not enough in today's security-sensitive environment to provide flexible solutions for customers, says Jared Wray, founder and Chief Technology Officer of Tier 3. You also must secure those solutions. In 2006, Wray saw an emerging need for enterprise-class on-demand services and founded Tier 3 to deliver products that help organizations with their infrastructure needs. As the company's solutions and customers evolved over the years, Wray and his team determined that they needed a strong encryption solution that would protect their customers' information without degrading performance. They turned to Intel® Xeon® processor E7 family-based servers with Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) to provide fast, secure encryption solutions for security-sensitive customers.[1]

Securing Rivers of Data

Security is a concern for any company, but it is especially important for those that must adhere to strict internal and external regulations. These organizations need airtight security at all levels of the hardware and software stack, and the push to public cloud strategies has left many unsure of how to protect their data while taking advantage of the benefits of cloud computing.

Enter Tier 3. The company makes cloud benefits available to organizations that have extensive security requirements, such as healthcare and financial-services organizations. Tier 3 provides a multi-layered "Defense in Depth" cloud-security model including an environment with strict security controls, such as:

- Fully auditable authentication and action tracking using the proprietary Tier 3 middleware solution, Control System. This solution authenticates all users and logs all user-initiated actions.

WHAT IS INTEL® AES-NI?

Advanced Encryption Standard (AES) is a symmetric-key encryption algorithm that uses the same cryptographic key for both encryption and decryption. Developed in 2001, AES is now widely used across both private and government systems to protect data that travels across networks and data that resides on storage.

Since encrypting and decrypting data can be processor-intensive, Intel created Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) to increase cryptographic performance. Intel AES-NI is an instruction set found in Intel® Xeon® processors and in Intel® Core™ processors that accelerates AES data encryption. With seven new instructions, Intel AES-NI delivers fast data protection that increases security for individual users and organizations.

Intel AES-NI also helps protect against "side channel" snooping attacks. This type of attack uses software agents to search for processing and memory access patterns on an encrypted system that could help crack the encryption. Intel AES-NI hides elements that the software agents search for, making it harder for the agents to find vulnerabilities in the encryption.

With Intel AES-NI, companies can protect data as it travels across the network, on storage devices, and within applications without sacrificing performance.

- Secure access to services using virtual private networks (VPNs) and multiple authentication layers.
- Zone-based firewalls that isolate each customer's workloads within a private, secure network.
- Data centers that provide strict physical security and full redundancy for power, cooling, networking, and server hardware.

With these and other security solutions already in place, Tier 3 wanted to expand its security portfolio to include data-encryption solutions for customer virtual machines and on the virtual storage area networks (vSANs) that Tier 3 offers customers for enterprise storage and backup.

The Challenge: Increase Security without Impacting Performance

If you encrypt data using software-only AES, you run the risk of bringing a system to its knees, especially if you're encrypting data within virtual machines. The Tier 3 team discovered just how significant the performance impact was when they started testing AES encryption within their VMware vSphere* 4 environment. Without hardware-assisted encryption, they would need to reduce the number of virtual machines running on each host, which would increase hardware and software costs over the entire infrastructure.

To achieve their goal of adding customer-driven AES encryption to their security portfolio, the team needed a solution that wouldn't adversely impact their cloud-infrastructure performance. "We looked for a solution that would give our customers the best encryption protection possible without jeopardizing performance for mission-critical workloads," explains Wray. With these requirements in mind, the Tier 3 team turned to Intel AES-NI.

Intel AES-NI, which is available on Intel® Xeon® processors, helps increase AES performance by embedding specific instructions in the hardware that accelerate and optimize AES encryption. These instructions can significantly increase encryption and decryption performance on the server and storage systems that power today's cloud environments.

Tier 3 uses VMware vSphere 4 as the foundation of their cloud services. VMware vSphere 4 and VMware vSphere* 5 accelerate encryption within virtual machines by letting the virtual machines directly access Intel AES-NI instructions on the host processor. This feature significantly increases encryption performance within virtual machines without taxing the host processors.

Testing the Waters

To determine how Intel AES-NI would affect host performance in the Tier 3 infrastructure, the team deployed a proof-of-concept environment using quad-socket servers with the Intel® Xeon® processor E7 family. Engineers configured the servers with VMware vSphere 4 and enabled Intel AES-NI in the server BIOS. The engineers then configured virtual machines running Windows Server* 2008 R2, a single virtual CPU (vCPU), and 16 GB of RAM, and used PGP* Whole Disk Encryption from Symantec to encrypt the virtual hard disk from within the virtual machines. Testing AES performance inside the virtual machines would show how Intel AES-NI could improve encryption performance across the infrastructure.

Intel® AES-NI Delivers

The team measured the time it took to write varying amounts of data within the virtual machines using custom tools. The engineers then repeated the tests with Intel AES-NI disabled in the BIOS.

With Intel AES-NI enabled, the virtual machines increased encryption performance speeds by an average of 26 percent while significantly reducing CPU load on the host.

By increasing encryption performance and reducing processor load, Intel AES-NI is helping Tier 3 incorporate encryption across its solutions without significantly impacting infrastructure performance. This performance boost also helps reduce infrastructure costs by letting Tier 3 increase consolidation ratios of encrypted virtual machines. Tier 3 plans to enable Intel AES-NI across its entire infrastructure as it expands its data center presence.

Protect Your Data without Sacrificing Performance

Once upon a time, IT had to choose between performance and securing data with software-only encryption solutions. Not anymore. With Intel AES-NI, Tier 3 customers will be able to brave today's digital rapids by taking advantage of strong hardware-assisted encryption within their virtual machines and vSANs without sacrificing performance for mission-critical workloads.

Like Tier 3, you can maximize server density while increasing security with Intel AES-NI. To learn more about how Intel AES-NI can help secure your cloud infrastructure, visit http://www.intel.com/content/www/us/en/architecture-and-technology/advanced-encryption-standard--aes-/data-protection-aes-general-technology.html.

"Intel® AES-NI increased encryption and decryption performance by 26 percent. With Intel AES-NI, we can offer customers a proven data-security solution without affecting system performance."

– Jared Wray,
Chief Technology Officer and Founder, Tier 3

[1] Intel® AES-NI requires a computer system with an AES-NI-enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® Core™ processors. For availability, consult your system manufacturer. For more information, see http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/.

Printed in USA 0812/KB/PRW/PDF Please Recycle 327864-001US