



# Intel Partners with VMware to Strengthen Security in the Cloud

**Combination of New Hardware and Software Capabilities to Better Protect Data and Reduce Threats to Cloud Datacenters**

## NEWS HIGHLIGHTS

- VMware vSphere® 5.1 will support Intel® Trusted Execution Technology (Intel® TXT), providing hardware-backed assurance for integrity of virtualized environments to better protect data and reduce threats to cloud data centers.
- Dupont, one of the largest global R&D organizations, is using Intel TXT to strengthen security and compliance policies in their private cloud.

SANTA CLARA, Calif.--(BUSINESS WIRE)-- Although companies are expanding their use of cloud computing to realize improved agility and efficiencies, concerns about security remains a top barrier to adoption. Today, Intel Corporation announced new collaboration with VMware and will deliver a platform for trusted cloud that combines [Intel® Trusted Execution Technology](#) (Intel® TXT) with the new release of VMware vSphere® 5.1, the leading platform for building cloud infrastructures. With hardware-enhanced security capabilities integrated into the processor, Intel TXT combined with VMware vSphere 5.1 will provide a hardened and high-integrity platform to run business-critical applications in private and public cloud environments.

## Platform integrity for data protection and control

In cloud datacenters, servers are typically virtualized and shared across multiple departments or customers and are no longer dedicated to specific lines of business. This has created new security concerns. The difference can be compared to owning your own home vs. living in an apartment complex. When owning a home, one has significant control over its security and protection -- everything from locks, secure fences to home security systems. This is similar to today's enterprise IT security. But when one lives in an apartment, it is a multi-tenant environment with multiple people sharing the same building resources, generating higher concerns about security. Someone accessing the apartment via a shared fire escape or maybe a landlord entering the apartment when a tenant is not there heightens security concerns. This situation is similar to having less control in your cloud computing environment.

In a recent global [survey](#) of IT professionals conducted by Intel about cloud security, 61 percent of IT pros expressed concern about a lack of control and insight about security capabilities of these shared, virtualized datacenter resources. IT pros also have concerns about not having adequate tools to protect against cyber-attacks and 57 percent will not put sensitive data that must meet specific compliance requirements into cloud datacenters.

Furthermore, 55 percent worry about loss of control of data stored off premise in public cloud provider datacenters.

Intel TXT is a built-in security capability that is part of servers based on [Intel® Xeon® processor E3, E5 and E7 series](#). When combined with VMware vSphere 5.1, organizations will be able to better address these challenges through increased infrastructure integrity and having greater control over the security status of servers in virtualized clouds. Companies can also realize operational efficiencies by making it easier to move virtual machines across clouds to “known good” trusted pools of servers, while at the same time, better meet compliance requirements and automate remote audit processes. To make it easier to deploy these security capabilities, Intel and VMware have developed solution reference architecture, or recipes, via the [Intel Cloud Builders](#) program.

“Intel TXT provides hardware enforcement to help overcome some of the most challenging aspects of cloud security, including detection and prevention of bios attacks and evolving forms of stealthy malware, such as rootkits,” said Jason Waxman, general manager, Intel Cloud Infrastructure Group. “VMware vSphere 5.1 support of TXT is essential to building a foundation of trust in virtualized infrastructures and the cloud and is ready for deployment.”

“VMware is pleased to partner with Intel to support Intel TXT in VMware vSphere® 5.1,” said Bogomil Balkansky, senior vice president, Cloud Infrastructure Products, VMware. “The combined capabilities bring a trusted security solution for cloud environments. With VMware vSphere 5.1 and Intel TXT, we are empowering our customers to have the confidence to put their sensitive data and business-critical workloads in the cloud.”

### **Case study: Dupont**

Dupont, one of the largest research and development organizations in the world with more than 9,500 scientists and engineers, is a leader in high-performance cloud computing. Research and development projects might last from a few months to several years. Dupont needed a platform that could provide infrastructure on demand, and then return resources to the pool once projects were completed. Since Dupont’s research and development efforts were spread across the globe, they also required an infrastructure that complied with regional regulations and kept sensitive information safe and within geographic borders.

“When extending cloud in a global way, compliance and regulation require capabilities such as geo-fencing, bursting and encryption when migrating to a public cloud, as well as support for vendor cloud services where terms and agreements play a key role,” said Dr. Hai Zhu, manager, Dupont Central Research & Development. “The compliance engine can be supported through the platform itself with such technologies as Intel TXT to monitor these systems.”

Intel (NASDAQ: INTC) is a world leader in computing innovation. The company designs and builds the essential technologies that serve as the foundation for the world’s computing devices. Additional information about Intel is available at [newsroom.intel.com](http://newsroom.intel.com) and [blogs.intel.com](http://blogs.intel.com).

Intel, Intel Xeon and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

VMware and VMware vSphere are registered trademarks and/or trademarks of VMware, Inc. in the United States and/or other jurisdictions. The use of the word “partner” or “partnership” does not imply a legal partnership relationship between VMware and any other company.

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

Intel Corporation  
Radoslaw Walczyk, 408-765-0012  
[radoslaw.walczyk@intel.com](mailto:radoslaw.walczyk@intel.com)

Source: Intel Corporation