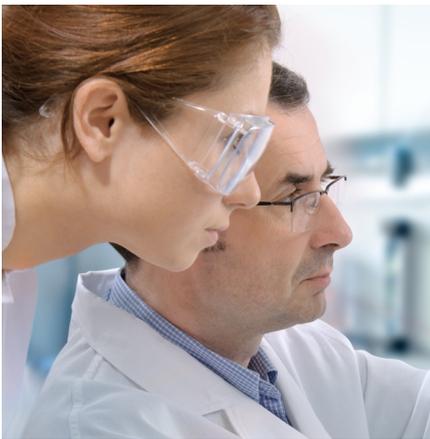




Deploying Intel® Trusted Execution Technology to Enable a Trusted Private High Performance Cloud

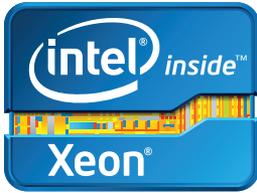


DuPont is one of the world's most dynamic science companies with a global footprint of over 70,000 employees in 90 countries. Its core science has a 212-year-old track record of delivering innovative products and materials, many with household names such as Kevlar®, Teflon®, Tyvek®, and Corian®. To enable the continued development of new approaches and discovery vehicles, DuPont is increasingly relying on a diverse modeling and simulation environment to provide key insights into the discovery process. The need to enable a secure, robust, and dynamic computing environment became clear, and so a partnership was forged with Intel to develop the foundation for a secure high performance computing cloud.

DuPont's research and development global footprint encompasses over 150 R&D facilities, with more than 9,500 scientists and engineers engaged in virtually every field of scientific endeavor. In 2011,¹ nearly \$2 billion was allocated to further the research and development of DuPont's next generation of products and services.

With research areas ranging from nanotechnology and alternative energy to plant genetics, DuPont R&D is taking aim at those societal problems such as feeding the planet, providing alternative and clean energy, protecting the environment, and making the world a safer place.

The complexity of a multi-domain focused, global research initiative presents unique challenges for managing the data and infrastructure to enable collaboration and sharing, while also adhering to those governmental regulations applicable to the various data types. It was decided that the future state architectural design of this environment must be based on a dynamic, yet cost-effective capability, that provides an efficient mechanism to ensure 100 percent compliance with regulatory and security standards.



Designing a Trusted Infrastructure

Technical computing encompasses both the need for ever-increasing computer resources, coupled to a data management framework that provides performance, regulatory, licensing, and security targets. Key requirements included:

- **A high performance infrastructure-as-a-service model:** R&D projects might last from days to years, so DuPont needed a platform that could quickly spin up infrastructure on demand, based on OS, capacity and performance requirements. Of equal importance is the ability to quickly return those resources to the pool once projects are complete.
- **Compliance and security:** DuPont operates in a number of countries, and therefore needed a framework that was aligned with existing compliance and security policies and supported by auditing and reporting tools. Security and intellectual property protection is core to all computational efforts and these must comply with internal and external regulations.

To meet DuPont R&D's unique needs, the Information and Computing Technologies (I&CT) group in DuPont Central Research and Development (CR&D) set out to create a cloud solution that provided the R&D community the elasticity it needed, while maintaining strict governmental and security compliance. Once secure environments were built, DuPont deployed Intel® Trusted Execution Technology (Intel® TXT) to ensure that the computing pools remained trusted, based on the original configurations across both Linux and Windows operating environments.²

Powering DuPont's R&D Cloud with Intel® Xeon® Processors

DuPont CR&D built its cloud foundation on 32-core Dell PowerEdge® R910 servers equipped with Intel® Xeon® processor 7500 series.

Building Trusted Compute Pools with Intel® TXT

Today, data security is at the forefront of most organizations, regardless of business focus. DuPont's research and development efforts required a uniquely hardened infrastructure that complied with both project and regional "geo-fenced" boundaries to ensure sensitive or regulated data was managed according to applicable policies. To help meet these demands, DuPont employed Intel® TXT-enabled Dell PowerEdge servers, coupled with cloud management software from a leading ISV to create policy-driven trusted compute pools that provided the necessary geo-fencing for the environments.

Intel TXT is a set of security enhancements built into select Intel® Xeon® processors and chipsets that creates a root of trust that extends from the hardware to the software stack, including the BIOS, firmware, and hypervisor or operating system. Intel TXT validates the configuration and behavior of server hardware and software against a known good sequence in a tamper-resistant environment at startup, which helps prevent attacks such as BIOS and firmware update attacks, reset attacks, and rootkit hypervisors that would compromise platform integrity and trustworthiness. For example, if an attacker managed to install a rootkit on an Intel TXT-enabled platform, systems management software can use security information provided by Intel TXT to identify the compromised server and then isolate it using automated policies.

The trust information provided by Intel TXT affords additional value when migrating instances between hosts in either a virtualized or cloud environment. Research operations require that sensitive virtual machine instances are isolated to run only on trusted, high integrity hosts within their cloud. DuPont CR&D's cloud

management platform lets administrators create Intel TXT-verified trusted compute pools, and then create policies that restrict virtual machines from migrating among trusted and untrusted hosts and vice versa.

Administrators also have the ability to create trusted application templates that ease deployment of new resources while maintaining security, compliance, and software licensing requirements. When an R&D project requires new resources, I&CT administrators can rapidly establish template-based resources in the cloud that are protected by security policies.

The combination of advanced execution control and sound security allows DuPont to protect and isolate sensitive workloads from potentially harmful attacks while easing virtual machine management, which gives administrators numerous management benefits while increasing the security profile of the environment.

Enabling Data and Application Geo-fencing

Private clouds let organizations more fully leverage infrastructure resources across business units, helping to reduce costs, increase uptime, and simplify systems management. These clouds also can provide for robust disaster-recovery options, such as migrating virtual machines between machines, VM Farms or even in regionally dispersed data centers helping to balance workloads among multiple sites, or move mission-critical virtual machines in the event of a disaster.

But what if your virtual machines contain highly sensitive information that must remain within a country's borders, or applications whose licensing policies restrict the software's use to a specific site? Traditional physical isolation of applications can be difficult in a virtualized cloud environment.

Geo-location-based migration, combined with Intel TXT, lets DuPont CR&D create migration policies that restrict virtual machine migration to trusted servers located in specific geographic areas. DuPont cloud management software enabled administrators to specify policies that established application-specific compute pools based upon geographic zones, thus restricting virtual machine migration to trusted hosts outside of those zones.

Auditing and Compliance Reporting

Intel TXT complements traditional auditing and compliance reporting tools. By restricting virtual machine migration and geographic location through policy-driven cloud management tools, administrators have better insight into where sensitive workloads run, and better control over how new virtual machines are introduced into the infrastructure. And Intel TXT provides a hardware-based infrastructure for reporting and auditing some of these control aspects—which is beneficial in increasingly virtualized, global scale environments.

Intel® TXT: Security and Flexibility without Compromise

DuPont's research-oriented high-performance cloud was readily built using standard technologies, including the use of Intel TXT to help establish the concept of trusted platforms. This unique cloud service provides DuPont R&D with the highly leveraged, on-demand resources it needs to support the growth in modeling, simulation, informatics and analytics while increasing the security and compliance capabilities within the data center.

AT A GLANCE: INTEL® TXT

Intel® Trusted Execution Technology (Intel® TXT) creates a unique foundation of trust that is rooted in the hardware and extends to other areas of the infrastructure. It provides a launch environment that cryptographically measures server hardware and software elements in the launch environment against known good values that are stored within a protected memory area.

At startup, Intel TXT assigns each element in the launch environment a cryptographically unique identifier. These identifiers are then compared with the known good identifiers. If the values align, the boot process continues in a trusted state. If the values do not align, the platform boots into an untrusted state. Systems management software can then detect the platform's untrusted status and take appropriate actions.

At the hardware level, Intel TXT provides:

- A protected execution and memory space where sensitive data can be processed.
- Sealed storage to shield encryption keys and other secrets.
- Verified launch, which enables launch of the measured launch environment into a known good state, with changes detected through cryptographic measurements.
- Attestation, which confirms that a system has correctly invoked the trusted execution environment and enables verified measurement of software running in it.

To find out how Intel® Trusted Execution Technology can help secure your infrastructure, contact your hardware vendor today, or visit www.intel.com/txt.

SOLUTION PROVIDED BY:



¹ DuPont 2011 Annual Review

² No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit www.intel.com/go/intelxt.

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 DEATH MAY 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.

Copyright © 2013 Intel Corporation. All rights reserved. Intel, Xeon, the Xeon badge, and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.