CASE STUDY

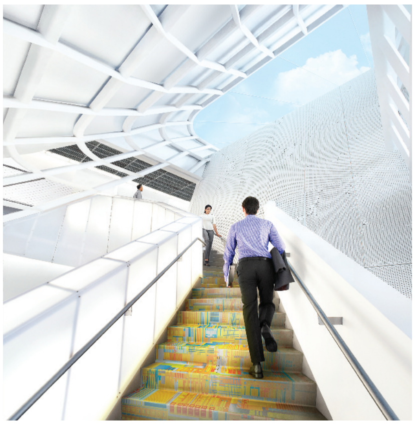
Intel® Xeon® Processor E5 and E7 Families
Intel® Trusted Execution Technology (Intel® TXT)

Communications/Media
Cloud Security

Making the cloud more transparent

CompatibleOne collaborates with Intel® to develop automated cloud brokerage service, using Intel® Trusted Execution Technology[1] to boost confidence in the security of cloud services

CompatibleOne is a research and development (R&D) project comprising 13 companies that are developing an innovative new cloud brokerage service that lets customers automatically provision workloads in the cloud across a choice of compatible service providers. CompatibleOne's software lets customers identify services that can meet the service level agreements (SLAs) they require from suitable providers based on criteria such as cost, location, security, and the processing and storage capacity required. From the outset, CompatibleOne has collaborated with Intel to refine the technical and commercial side of its offering. Its service uses Intel® Trusted Execution Technology (Intel® TXT) to confirm the integrity of the server hardware, BIOS and hypervisor components on which cloud workloads are run. By establishing a root of trust from the hardware up, customers can ensure their data is processed in a trusted environment.



CompatibleOne

> "The aim of CompatibleOne is to foster a more open, transparent approach to cloud computing. Incorporating the security capabilities of Intel® Trusted Execution Technology into our platform supports this objective by providing customers with additional reassurance about the integrity and security of the compute pools used to handle their data."
>
> Jean-Pierre Laisne,
> Project Lead, CompatibleOne

CHALLENGES

- **Understanding needs:** When developing its new cloud brokerage service, a priority for CompatibleOne was gaining a detailed understanding of the practical requirements of both potential users and cloud service providers
- **Simple solution:** It recognized that a service that offers easy-to-understand access to the right type of cloud resources based on a list of user-configurable criteria would fulfill the requirements of a wide range of potential users
- **Gaining trust:** To encourage further cloud adoption, CompatibleOne realized it needed to reassure customers that their workloads will be processed on secure servers in a trusted state

SOLUTIONS

- **Root of trust:** Intel TXT in Intel® server processors allows cloud operators to verify the integrity of server hardware and other basic operating components such as BIOS, firmware and hypervisor software
- **Trusted cloud:** CompatibleOne incorporated the additional security checks enabled by Intel TXT into the configuration options available to users of its service
- **Right choice:** Bringing the extra protection offered by Intel TXT directly to users makes it easier for them to source cloud services that meet their specific requirements

IMPACT

- **Improved appeal:** Intel® technology allows CompatibleOne to enhance its cloud brokerage offering by providing users with even greater control over where their data is processed
- **Business confidence:** Reassuring customers about the security of cloud workloads has the potential to encourage further adoption of cloud services for business use
- **Open approach:** By placing greater emphasis on cloud providers to demonstrate the security of their hardware resources CompatibleOne is helping drive greater transparency in the industry

An open approach

CompatibleOne is an R&D project working to improve access to cloud services for both established organizations and entrepreneurs. With the fast growth of the cloud industry and the standards underpinning the technology, the process of selecting a suitable cloud service can be complex and potentially confusing for end users. In response, CompatibleOne developed a way of commissioning cloud workloads that preserves flexibility and choice and helps protect users from the threat of vendor lock-in.

CompatibleOne's solution, which it is testing before launch, is an open source and open-standard cloud brokerage platform that makes it easy for users to connect with the most suitable cloud service provider available, based on their specific needs. The platform supports a range of cloud delivery formats including platform-as-a-service (PaaS), infrastructure-as-a-service (IaaS) and software-as-a-service (SaaS) and different deployment configurations including public, private, hybrid and community clouds.

CompatibleOne enhances the security options available to cloud end users with Intel TXT compatibility

Using CompatibleOne's platform, end users can automatically provision cloud workloads using suitable services from a wide range of participating providers. To ensure the platform meets a range of potential usage scenarios, CompatibleOne has designed it to let users filter potential providers according to criteria such as where their servers are located, the operating environment they support, the processing and storage resources available, and cost.

Confidence in the cloud

With the security of data in the cloud a key concern for individuals and businesses, CompatibleOne recognized the need to make secure processes a central part of the way its platform operated. From the start of the project, it collaborated with experts from Intel to establish the technical resources required to deliver a secure service.

While evaluating available data center technologies, CompatibleOne identified the potential for Intel TXT in the Intel® Xeon® processor E5 and E7 families to enhance the data security credentials of its cloud brokerage service. Intel TXT provides a way to check the integrity of the servers handling cloud workloads before they are run. It does so by letting cloud operators take reference measurements of how the server hardware and pre-launch software components – such as BIOS, firmware and hypervisors – present when running in a known, secure state. Later, when the server is booted up, Intel TXT automatically compares the configuration of hardware and software at that moment with the reference snapshot created earlier. If any discrepancies indicate a hardware or software component has been tampered with, Intel TXT can automatically prevent workloads from being executed on that server.

By establishing a root of trust from the hardware level up for the servers used to process cloud workloads, Intel TXT enables cloud operators to offer trusted compute pools that are verified as running in a safe state.

Sharing the benefits

When developing its brokerage service, CompatibleOne saw an opportunity to incorporate the additional security assurances offered by Intel TXT into the list of options end users can configure to determine which cloud service providers are suitable for their requirements. CompatibleOne worked with Intel and service operators to test both the practical performance of the technology and how customers wanted to use it. When offering the Intel TXT-backed security options to users, CompatibleOne presents the technology in terms of its practical implications for data security rather than a detailed account of how the process works. This ensures non-technical users can still understand how it can benefit them.

By making Intel TXT part of its platform's security offering, CompatibleOne is helping bring the latest advances in security technology to a general end user audience and broadening the range of options available for end users to configure. As it develops its business ecosystem, CompatibleOne sees this as a key commercial differentiator.

CompatibleOne also hopes the additional functionality Intel TXT can offer about the security of cloud workloads will remove another barrier to the adoption of cloud services.

Lessons Learned

CompatibleOne's work with Intel has highlighted the potential for advanced server technologies such as Intel TXT to provide more choice and greater security for end users of cloud services. By collaborating with Intel and cloud service providers, it is harnessing the potential of Intel TXT to increase users' trust in the security and dependability of both its own automated brokerage platform and the compatible services it provides access to.

In particular, it hopes to attract interest from businesses that need to ensure their IT infrastructure complies with the data security standards set out by regulators.

Greater transparency

By making Intel TXT a way for users of its service to choose among cloud services, CompatibleOne is encouraging cloud operators to offer greater transparency about the data center resources they use to deliver their services.

This supports CompatibleOne's wider aims of fostering a more open and flexible approach to cloud computing. By designing its platform to make it simpler for end users to connect with the right service provider, it plans to make the process of provisioning cloud workloads more accessible, encouraging further uptake. The open, automated approach at the heart of the platform supports greater choice in the cloud and will help users mitigate the strategic risk of vendor lock-in.

Find the solution that's right for your organization. Contact your Intel representative, visit Intel's Business Success Stories for IT Managers (**www.intel.co.uk/Itcasestudies**) or explore the Intel.co.uk IT Center (**www.intel.co.uk/itcenter**).

This document and the information given are for the convenience of Intel's customer base and are provided "AS IS" WITH NO WARRANTIES WHATSOEVER, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. Receipt or possession of this document does not grant any license to any of the intellectual property described, displayed, or contained herein. Intel® products are not intended for use in medical, lifesaving, life-sustaining, critical control, or safety systems, or in nuclear facility applications.

[1] 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 http://www.intel.com/technology/security

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. For more information go to http://www.intel.com/performance

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