

CASE STUDY

Intel® Xeon® Processor E5 Family

Intel® Trusted Execution Technology

Financial Services

Cloud Security



Investors profit steadily from high-speed, secure cloud

Taiwan Stock Exchange builds a cloud infrastructure on Intel® Xeon® processor E5 family and Intel® Trusted Execution Technology (Intel® TXT), delivering rapid yet secure transactions for brokerage firms



The Taiwan Stock Exchange (TWSE) provides a full range of trading and securities services including securities listing, market surveillance, investor services, and security for electronic data and communications. Officially launched in 1962, the TWSE has been the platform for the trading of securities in Taiwan.

CHALLENGES

- **Improve information transmission.** Ensure that the IT system can deliver timely information and process and transmit at high speed.
- **Ensure integrity of data.** Assist in the integration of information systems at brokerage firms, and ensure the secure delivery of highly sensitive news updates and other data.
- **Effectively cope with global trends.** IT systems must be able to deliver fast and convenient trades to compete against overseas exchanges.

SOLUTIONS

- **Deploy cloud computing platform using Intel® Xeon® processor E5 family.** Build a data center that will integrate transaction data with other services and enable quick access to a high-speed, high-quality transaction system.
- **Use Intel TXT and software solutions from VMware, HyTrust, and McAfee.** Ensure data integrity with Intel TXT that provides transmitted data packages with a label that can be uniquely identified, while using McAfee security technology to address data security issues for cloud computing platforms.
- **Maximize limited resources.** Focus on maintaining one hardware platform during migration and achieving integration with the systems of the various brokerage houses so that brokerage houses can concentrate their limited resources on enhancing services for customers, enabling them to be more competitive.

IMPACT

- **Secure cloud infrastructure.** Built a joint, phased proof of concept (PoC) to improve hardware-based security.
- **Improved overall trust and security.** Created a foundation of trust, visibility, and control in the cloud computing infrastructure with Intel TXT, integrated with software application solutions.
- **Streamlined operations.** Integrating McAfee security technology's flexible automation capability streamlined workflows, dramatically reducing the cost and complexity of security and compliance administration.

Cloud computing platform running on Intel® Xeon® processor E5 family-based servers and built with Intel® TXT ensures data integrity in securities trading



"For IT services that demand high levels of speed and data integrity, implementing security filters using Intel® processors is more efficient than relying on software filters. We have also been able to develop stable and efficient software services for securities trading on our Intel-based cloud computing platform.

We can now easily provide reference information required by authorities or regulators and gain approval from high-level decision makers."

*Lin Huodeng
Deputy General Manager
Taiwan Stock Exchange*

Need for high-speed processing and reliable transmission

Trading on a stock exchange relies heavily on IT, since millions of trades transacted daily are processed by IT systems. Investors make decisions based on the information at hand. With portfolios at stake, the demands on data quality and accuracy are high.

To cope with the heavy load and stringent requirements of its business, the TWSE dedicates its effort to building and maintaining information services and the infrastructure on which they run. "Just imagine: If a company name is published in error in a news release, it could cause investors to shift their attention to other investment targets. The losses that companies and investors might suffer due to such an error could be very serious. There is simply no room for error," explains Lin Huodeng, deputy general manager at TWSE.

The IT system that supports a stock exchange needs to be able to deliver timely information, which means processing and transmitting at high speed. The delivery of news updates and other data is also highly time-sensitive. As the organization responsible for overseeing securities and exchange in Taiwan, the TWSE must take the lead, helping integrate information systems at other brokerage firms whenever there are changes to business or securities regulations. This means the TWSE's IT infrastructure must be resilient yet agile.

Globalization trends also affect TWSE. In key international markets such as Europe and the U.S., the use of IT can differentiate an exchange from its competition. "All stock exchanges are very sensitive to system delays," explains Lin. "Our system must be fast enough to grab all customer orders as they stream in. This motivates us at the TWSE to constantly improve our hardware and software infrastructure, and to create a trading environment that enables us to compete internationally."

Increasing competitiveness with cloud

In the past, information services played a supporting role to the business operations, even at the stock exchange. Today, IT strategy is now an integral part of the overall business strategy at TWSE. IT staff are no longer back-room supporting cast members. They now need to better understand how they can add value to the business. TWSE is harnessing the benefits of cloud computing and actively rolling out software as a service (SaaS) solutions.

"In Taiwan, brokerage firms are all considered partners of the stock exchange," says Lin. "TWSE is currently developing a range of cloud-based services that can be provided downstream to the brokerage houses. The use of a cloud computing platform means that TWSE can focus on maintaining only one hardware platform during the migration to cloud infrastructure, while achieving integration with the systems of the various brokerage houses. For brokerage houses, there is now no need to invest heavily into building a data center to integrate transaction data with other services. Smaller brokerage houses can concentrate their limited resources on enhancing services for their customers. This is helping the securities market in Taiwan become more competitive."

Cloud services take on the challenge of ensuring transaction integrity

Rolling out new services means new challenges. Cloud services are no exception. TWSE had to address data security challenges including:

- Routing of data transmitted to and from the cloud
- Deciding which machine room the data passes through
- Ensuring transaction systems can verify the source of the data received
- Identifying and blocking information that has been tampered with during the process of transmission over the cloud network

Lin reveals that if a transaction is tampered with, it could result in losses for the investor or the broker. Such a scenario would create a lot of uncertainty in the market, increasing risks.

For this project, TWSE needed to build a more secure foundation for sensitive cloud workloads by establishing trusted compute pools (TCPs) to provide the additional elements of security, visibility, and control needed to put more applications and workloads into its cloud infrastructure. From this initial PoC deployment, TWSE expects many other business units to be able to more effectively use cloud infrastructure to increase business agility, reduce costs, and improve asset utilization without compromising security.

By interacting with Intel and industry peers, Lin came to better understand that Intel-based systems integrated with software solutions could help address issues of data security on cloud computing platforms.

Intel TXT, which includes support and capabilities in the microprocessor, chipset, I/O subsystems, and other platform components, is designed to measure the execution environment and protect sensitive information from software-based attacks. It operates with Trusted Platform Module (TPM), an industry-standard device that can securely store artifacts used to verify integrity of the platform.

TWSE's Intel TXT-based solution works by providing a root of trust—a processor-based, tamper-resistant environment that compares firmware, BIOS, and operating system or hypervisor code to known-good configurations to establish a measured, trusted environment prior to launch. If integrity and trust are not verified in the launch process, Intel TXT identifies that the code has been compromised, thus protecting the system and remediating the problem. This hardware-based verification is less susceptible to tampering by hackers, thus making it safer than software-based filters.

To enhance the management of the virtualized infrastructure, VMware vCenter Server* 5.1 with VMware ESXi* 5.1 hypervisor were also employed to allow enterprises to use their own security certificates when securing remote sessions. VMware ESXi 5.1 provides support to Intel TXT by enabling remote platform attestation measurements to detect possible malicious changes to BIOS and other critical base software components of the servers.

TWSE then built a comprehensive cloud computing environment for securities trading. Services are being developed and tested by simulating a live operating environment. This cloud computing platform runs on servers powered by Intel Xeon processors, built with Intel TXT to ensure data integrity. Since Intel TXT can evaluate and report on platform integrity using attestation mechanisms, it was able to provide valuable insights and controls when used in the context of cloud computing models. This allows other key software—virtualization, cloud orchestration and management, and security policy applications—to understand and use platform integrity attributes to control workloads and data, and better address security risks by keeping sensitive or regulated workloads separate from platforms with unknown integrity status. This is a concept that Intel and like-minded solution companies call TCPs.

Lessons learned

- Brokerage houses need to focus on building a data center that integrates transaction data with other services, allowing quick access to a high-speed, high-quality transaction system.
- Intel-based systems integrated with software application solutions from VMware, HyTrust, and McAfee are ideal for addressing issues of data security on cloud computing platforms.
- Intel TXT provides transmitted data packages with a label that can be uniquely identified to ensure data integrity.

"For IT services that demand high speed and a high level of data integrity, implementing security filters using Intel hardware is more efficient than relying on software filters," explained Lin.

TCPs are physical or logical groupings of computing platforms in a data center that have demonstrated integrity of key controlling components (e.g., BIOS and hypervisor) in the launch process. Intel TXT provides a hardware-based mechanism for verifying and reporting on platform trust as a foundation for creating trusted pools.

Platform trust status is attested at launch. If the launch is trusted, that platform can be added to the trusted pool. Within this pool, systems and workloads can be tagged with security policies. The access and execution of apps and workloads can also be monitored, controlled and audited.

Creating TCPs is a way to aggregate trusted systems and segregate them from untrusted resources. It provides an infrastructure to support the separation of higher-value, more sensitive workloads from commodity applications and data. The principle of operation is to:

- Create a part of the cloud to meet the specific and varying security requirements of users
- Control access to an identified portion of the cloud so that only approved workloads and applications get deployed there
- Enable audits of that portion of the cloud so that users can verify compliance

Such TCPs, enabled by Intel TXT, allow IT to gain the benefits of the dynamic cloud environment while still enforcing higher levels of protection for critical workloads. Also, use of TCPs eliminates the need for air-gapped clusters of servers.

To integrate and extend security and platform trust, TWSE has also deployed McAfee ePolicy Orchestrator* security monitoring software. McAfee ePolicy Orchestrator delivers unified security management through an open platform, simplified risk and compliance management, and provides security intelligence across endpoints, networks, data and compliance solutions. It also helps manage security, streamline and automate compliance processes, and increase overall visibility across security management activities.

Through the use of these complementary security systems, TWSE can monitor and control the state of security in its cloud computing environment. By integrating McAfee's security SaaS solutions, it can identify potential threats early on.

"For IT services that demand high speed and a high level of data integrity, implementing security filters using Intel hardware is more efficient than relying on software filters," explained Lin. "When balancing the demands of speed and

security, a hardware-based solution provides better results. We have been able to develop stable and efficient software services for securities trading on our cloud computing platform with Intel. We are also fully prepared for other services that may come online in the future."

Analyzing the massive amount of data available using business intelligence or customer relationship management tools can also help identify new business opportunities. Lin is looking forward to having the capacity to consolidate information from various market sources in the new environment. This will enable higher-level analyses, strengthen back-end processes, and create new business opportunities.

For more information on how TWSE developed its secure cloud infrastructure through Intel TXT, visit <http://www.intel.com/content/www/us/en/cloud-computing/cloud-computing-txt-xeon-twse-whitepaper.html>.

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

Solution Providers By:



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.

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.

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>.

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

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