WHITE PAPER

Improve Server Security and Protect Your Business in the Cloud

Build your trusted user environments on a solid security foundation with IBM Cloud and Intel® TXT[1]

EXECUTIVE SUMMARY

In this whitepaper, we'll discuss a highly scalable architecture called Intel® Trusted Execution Technology (TXT) and how it provides hardware-based security technologies to build a solid security foundation on IBM Cloud.

Powered by intel® Cloud Technology

IBM®

A Partnership for Peace of Mind

Protecting your data and applications is important, especially when you leverage cloud infrastructure. In an onsite data center environment, physical access to hardware and control over security makes that protection relatively easy. But on-premises data centers are prohibitively expensive and don't provide the same flexibility and scalability as cloud provider resources.

Cloud and virtualization technologies are better suited to today's dynamic workloads. They also introduce new, evolving security challenges that require increasingly capable security tools and techniques. As attacks on infrastructure continue to grow in volume and sophistication, you need to know that your information is secure, offsite hardware can be verified and trusted, and your cloud environment meets rigorous compliance requirements.

IBM Cloud and Intel® TXT together provide that peace of mind.

As a premier Infrastructure as a Service (IaaS) provider, IBM Cloud provisions bare metal and virtual servers powered by Intel® Xeon® processors, setting an industry benchmark for secure processing in data centers around the world. These building blocks facilitate better regulatory compliance and increase the security and availability of infrastructures by addressing the growing security threats across physical and virtual infrastructures.

Providing hardware-based verification

Intel® TXT works with commercial software to avert BIOS and firmware abnormalities such as unknown changes, attacks, and malicious rootkit installations. Intel® TXT is a robust security foundation that ensures your select IBM Cloud servers can:

- Establish a **dynamic root of trust for measurement** (DRTM)
- Launch systems into a known good state
- Verify the **integrity** of key platform components
- Verify that servers physically reside in a **trusted geography**
- Establish **visibility, control, and compliance** by ensuring that your cloud workloads run on trusted compute pools
- Ensure that computing pools remain trusted based on their original configurations
- Provide **data protection** in case of improper shutdown

How Intel® TXT Works to Protect You

Take action before software boots

Intel® TXT, a hardware-based technology, adds a strong, tamper-resistant layer to other launch-environment protection solutions. With Intel® TXT enabled on IBM Cloud bare metal servers, firmware assures security safeguards—even down to boot hardware. At this level, Intel® TXT takes effect long before traditional software-based security solutions start to intervene.

When enabled on IBM Cloud servers, Intel® TXT technologies promote pervasive data encryption, encourage secure connection usage, protect infrastructure, and build higher security assurance for regulatory compliance.

Establish the root of trust at system launch

Intel® TXT provides a processor-based evaluation of a system's critical firmware and software components at launch by measuring and storing a known good system configuration. When a system launches in the cloud, Intel® TXT compares the system's key platform software to your known good configuration measurement and then determines if the information matches: firmware, BIOS, operating system, and/or hypervisor code.

Combined with the root-of-trust capability, the verification step uses policies to permit or deny a workload from running on a server system. For example, allowed actions could include: continue to launch or launch but flag that the launch configuration was at an unknown state.

Create trusted compute pools

The measurements made by Intel® TXT provide a new control point for creating trusted pools of servers. In a trusted pool, each platform demonstrates the integrity of key components in the launch process. If a platform cannot be verified, it can be dropped out of the pool and remediated.

For example, with Intel® TXT on your IBM Cloud bare metal servers, you can tag systems and workloads in the trusted pool with security policies. You can then locally or remotely monitor, control, and audit the access and execution of applications and workloads. You can also use geo-tagging to restrict workloads to IBM Cloud servers in approved locations—or use policy tools to make sure sensitive data is decrypted only on servers at approved data centers based on privacy policies, regulations, or applicable laws.

Host Location	Geotag	Trusted
Server 202	Seattle, WA USA	✓
Server 241	Sydney, Australia AUS	✓
Server 260	Paris, France EUR	✗
Server 336	Singapore, APAC	✓
Server 342	Dallas, TX USA	✓
Server 351	Dallas, TX USA	✗

These advanced Intel® TXT-based security capabilities are particularly useful in industries with stringent compliance regulations or those that handle large amounts of sensitive data.

Improve auditing and compliance

Intel® TXT provides a rigorous enforcement point for launch-time integrity. Through application programming interfaces (APIs), Intel® TXT also plugs into a reporting mechanism that offers visibility into system status to support auditing and compliance.[2]

With a foundation based on Intel® TXT, your bare metal IBM Cloud environments are more powerful components of your company’s security portfolio.

Make the cloud work for you with Intel® TXT

Intel® Cloud Technology with Intel® TXT helps power and protect the IBM Cloud infrastructure stack from the processor up. Intel® TXT starts with a root of trust and a measured launch environment that significantly improves protection from attacks or unknowns. This increases information security, improves threat and vulnerability management, enhances identity and access management, increases application security, and improves the physical security of your systems.

How do you get Intel® TXT on your server?

Simple: Just add Intel® TXT support when you configure your eligible IBM Cloud bare metal server.

What can you do next?

- Take a few simple steps to safeguard your data: **https://ibm.co/safeguard**
- Dive into our security documentation: **http://ibm.co/securitydocs**
- Learn more about Intel® TXT: **http://www.intel.com/txt**
- Get started with Intel® TXT on IBM Cloud: **http://www.ibm.com/inteltxt**
- Send an email **sales@bluemix.net** or call us at **866-398-7638**

[1] No computer system can provide absolute security. Requires an enabled Intel® processor, enabled chipset, firmware, software, and may require a subscription with a capable service provider (may not be available in all countries). Intel® assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof. For more information, visit http://www.intel.com/go/txt.

[2] With the use of software provided by IBM Cloud partners. Separate software might be required to take full advantage of some use models.

IBM Corporation New Orchard Road Armonk, NY 10504

Produced in the United States of America July 2017