Improve Server Security and Protect Your Business in the Cloud

SoftLayer, an IBM Company, uses Intel® Trusted Execution Technology (Intel® TXT)[1] to provide security controls to help ensure that your workloads are running on trusted hardware.

The protection of your data and applications is important, especially when leveraging cloud infrastructure. In an on-site data center environment, physical access to hardware and control over security makes that protection relatively easy, but on-site data centers are prohibitively expensive and don't provide the same flexibility and scalability of off-site cloud resources.

These cloud and virtualization technologies are better suited to today's dynamic workloads, but 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, that off-site hardware can be verified and trusted, and that your cloud environment can meet rigorous compliance requirements.

SoftLayer and Intel TXT provide that peace of mind.

As the premier infrastructure as a service (IaaS) provider, SoftLayer provisions bare metal and virtual servers powered by Intel® Xeon® processors in data centers around the world. This geographic diversity provides unparalleled performance, and it also presents unique security and compliance challenges. To address those challenges, SoftLayer offers Intel TXT on select bare metal servers to simplify the process of building a cloud environment that measures, monitors, and verifies the integrity of the entire system from the processor level up.

Providing hardware-based verification

Intel TXT works with commercial software to help ward off BIOS and firmware abnormalities like unknown changes, attacks, and malicious rootkit installations. Intel TXT is a robust security foundation that can help ensure that your select SoftLayer servers:

- **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**

1. No computer system can provide absolute security. Requires an enabled Intel® processor, enabled chipset, firmware, software, 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

Powered by intel Cloud Technology

SOFTLAYER® an IBM Company

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 SoftLayer bare metal servers, security safeguards can be more assured through firmware, even down to boot hardware. At this level, Intel TXT can take effect long before traditional software-based security solutions start to intervene.

This is the root of trust: sophisticated technologies which work at a level where software cannot.

When enabled on SoftLayer servers, Intel TXT technologies promote pervasive data encryption, encourage the use of more secure connections, 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 allows you to use 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.

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

For example, with Intel TXT on your SoftLayer 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 SoftLayer servers in approved locations. Or use policy tools to help make sure sensitive data is decrypted only on servers at approved data centers based on privacy policies, regulations, or applicable laws.

These advanced Intel TXT-based security capabilities are particularly useful in industries with stringent compliance regulations or which 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 can offer visibility into system status to support auditing and compliance.[2] With a foundation based on Intel TXT, your bare metal SoftLayer environments are more trusted components of your company's security portfolio.

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

Make the cloud work for you with Intel TXT

Intel® Cloud Technology with Intel TXT helps power and protect the SoftLayer infrastructure stack from the processor up. Intel TXT starts with a root of trust and a measured launch environment that can significantly improve protection from attacks or unknowns. This helps you increase information security, improve threat and vulnerability management, enhance identity and accesss management, increase application security, and improve 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 SoftLayer bare metal server.

Learn More

To learn more about Intel Cloud Technology, visit **intel.com/txt**

To get started with Intel TXT on SoftLayer, visit **softlayer.com/intel-txt**

If you have any additional questions, email **sales@softlayer.com** or call us toll free: **866.398.7638.**

Powered by intel Cloud Technology

SOFTLAYER® an IBM Company