February 27, 2019

RSA 2019: Intel and Partner Ecosystem Offer New Silicon-Enabled Security Solutions

SANTA CLARA, Calif.--(BUSINESS WIRE)-- Today, Intel along with customers and industry partners announced several solutions designed to scale and accelerate the adoption of hardware-enabled security across data center, cloud, network and edge. From OEMs to cloud service providers (CSPs) and independent software vendors (ISVs), Intel continues to help lead the industry and advance security tools and resources that help improve the security and privacy of application processing in the cloud, provide platform-level threat detection and shrink the attack surface.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20190227005169/en/

Intel introduced the Intel SGX Card in February 2019. It is a new way to help extend application memory protections using Intel Software Guard Extensions in existing data center infrastructure. (Credit: Intel Corporation)

> *"Hardware-based security technologies are a top priority for cloud providers aiming to address enterprise scaling challenges. Trusted execution technologies such as Intel SGX are now readily available in a wide range of platforms helping to fuel innovation in the digital security ecosystem and further assist in implementation roll-out."*
> - Dimitrios Pavlakis, industry analyst, ABI Research.

Intel SGX for the Data Center

Helping protect customer data in the cloud is a top priority for cloud service providers. Intel® Software Guard Extensions (Intel® SGX) was designed to help create more secure environments without having to trust the integrity of all the layers of the system. The technology isolates specific application code and data to run in private regions of memory, or enclaves. Intel SGX is currently used by top cloud providers, including Alibaba Cloud*, Baidu*, IBM Cloud Data Guard* and Microsoft Azure* for various projects to help protect customer data at runtime. Today, Intel announced new products and ecosystem solutions that enable Intel SGX to be used even more broadly in the data center.

Scaling Intel SGX for the Cloud: Intel introduced the Intel SGX Card, a new way to help extend application memory protections using Intel SGX in existing data center infrastructure. Though Intel SGX technology will be available on future multi-socket Intel® Xeon® Scalable processors, there is pressing demand for its security benefits in this space today. Intel is accelerating deployment of Intel SGX technology for the vast majority of cloud servers deployed today with the Intel SGX Card. Additional benefits offer access to larger, non-enclave memory spaces, and some additional side-channel protections when compartmentalizing sensitive data to a separate processor and associated cache.

Availability is targeted for later this year.

To enable cloud adoption of Intel SGX at scale, Intel and industry partners are also introducing new tools and capabilities that enhance operational control, simplify development and support emerging workloads.

Operational Control: Intel is delivering a new capability called flexible launch control that enables a company's data center operations to set and manage their own unique security policies for launching enclaves as well as providing controlled access to sensitive platform identification information. This capability is currently available on Intel SGX-enabled Intel® Xeon® E Processors and some Intel NUC's.

New Developer Tools: Fortanix* launched its Enclave Development Platform* (EDP), the open-source software development kit (SDK) that uses the state-of-the-art security properties of the Rust programming language and Intel SGX to deliver a more secure application development platform. Developers can build enclaves with Rust to help improve protection from development vulnerabilities and outsider attacks. The Fortanix EDP is fully integrated with the Rust compiler allowing developers to immediately build, sell or distribute the secure applications they create.

Scale For Emerging Workloads: Baidu announced a preview of its Intel SGX-enabled MesaTEE* that delivers artificial intelligence algorithm protection for cloud and edge computing devices.

Advancing Threat Detection

Intel is helping lead the industry with hardware-enhanced security technology by delivering new capabilities to Intel® Threat Detection Technology (Intel® TDT), a set of silicon-level capabilities that helps detect classes of threats. First introduced last year and deployed across 50 million enterprise clients, Intel TDT is experiencing broad adoption and expanding platform support to Linux and virtual machines.

Intel Threat Detection Technology Evolves: Intel is expanding Intel TDT capabilities in 2019 to include support for Linux on servers in virtualized data center and cloud environments. Intel TDT combines platform-level telemetry infrastructure and machine learning models to detect targeted attacks. Detection alerts based on the heuristics are sent to the security service provider (ISV) for remediation. Integration of the Intel TDT stack into the existing ISV solutions results in improved performance and lower incidences of false positives. At RSA Conference, Intel will demonstrate Intel TDT on Linux using Intel-developed heuristics to detect unauthorized execution of specific cryptomining workloads.

SentinelOne: SentinelOne* (S1) is the first licensee to have adapted Intel TDT's accelerated memory scanning (AMS) technology for detection of cryptomining. With Intel TDT, S1's customers running Windows will enjoy up to 10-times faster pre-execution scanning and 4-times faster detection with immediate roll back of uncovered threats.[1]

Shrinking the Attack Surface

Intel's security open-source initiatives and community partners are equipping the ecosystem with tools to help reduce the attack surface in platforms and products before they are

deployed at scale.

Device Design: Intel is announcing Host-based Firmware Analyzer, a new tool for the TianoCore* open-source firmware community. Intel is applying best practices used by software developers and helping lead the industry in delivering a framework that automates the testing of firmware components prior to system integration. The Host-based Firmware Analyzer allows developers to run open-source advanced tools, such as fuzz testing, symbolic execution and address sanitizers in an OS environment. This tool is targeted for availability in the first half of this year.

Secure Device Onboarding: For secure device provisioning and management of internet of things (IoT) devices before they are activated on corporate networks, Mocana* announced full integration of Mocana TrustCenter™ with the Intel® Secure Device Onboard service. This solution reduces the burden on OEMs to pre-load customer specific credentials in the supply chain and delivers a model where cloud selection and configuration happen dynamically when first powered on.

Defending Firmware: Intel and Eclypsium* announced a collaboration that helps organizations manage the entire hardware and firmware attack surface for threats. The Eclypsium Platform, now generally available, extends Intel's secure foundation by analyzing the system configuration and ensuring the latest firmware is deployed.

Scaling Enterprise Endpoint Protection: Qnext* announced integration of Intel SGX in remote access of its sharing and collaboration platform FileFlex*. Intel SGX helps improve FileFlex Enterprise security for Microsoft Office 365 users when accessing files and folders from source locations at the edge of the network.

Where to See Intel at 2019 RSA

Next week at RSA Conference, Intel will be joined by industry customers and partners in demonstrating the latest security solutions services. Visit Intel at Booth 6173 for hands-on demonstrations and more information.

About Intel

Intel (NASDAQ: INTC), a leader in the semiconductor industry, is shaping the data-centric future with computing and communications technology that is the foundation of the world's innovations. The company's engineering expertise is helping address the world's greatest challenges as well as helping secure, power and connect billions of devices and the infrastructure of the smart, connected world – from the cloud to the network to the edge and everything in between. Find more information about Intel at newsroom.intel.com and intel.com.

[1] Independent benchmark testing from Passmark Software Source: https://www.sentinelone.com/press/sentinelone-collaborates-intel-cryptominers

View source version on businesswire.com:
https://www.businesswire.com/news/home/20190227005169/en/

Leigh Rosenwald
503-784-7492
leigh.rosenwald@intel.com

Source: Intel Corporation