May 11, 2022

Intel Introduces Project Amber for Cloud-to-Edge and On-Premises Trust Assurance

Provides customers and partners a security foundation for confidential computing, secure and responsible AI, and quantum-resistant crypto into the quantum era.

NEWS HIGHLIGHTS

- A new Intel service (code-named Project Amber) provides organizations with remote verification of trustworthiness in cloud, edge and on-premises environments.
- Intel accelerates responsible and secure AI deployments in collaboration with BeeKeeperAI and University of Pennsylvania's Perelman School of Medicine.
- Company details strategy for quantum-resistant cryptography by 2030 that starts with the 3rd Generation Intel® Xeon® Scalable platform.

GRAPEVINE, Texas--(BUSINESS WIRE)-- Today, during Day 2 of its inaugural Intel Vision event, Intel turned its focus to how it will meet the growing security needs of organizations today and help them prepare for the challenges of tomorrow. Focusing on one of the most critical security elements for any organization – trust – Intel introduced an independent trust authority in the form of an innovative service-based security implementation code-named Project Amber. The company also demonstrated its focus on enabling secure and responsible AI, and outlined its strategy to further build quantum-resistant cryptography for the coming quantum computing era.

This press release features multimedia. View the full release here: https://www.businesswire.com/news/home/20220511005333/en/

At its inaugural Intel Vision event on May 10-11, 2022, Intel announced advancements across silicon, software and services, showcasing how it

More Context: Intel Labs at Intel Vision 2022 | Intel Vision 2022 (Press Kit) | | Intel Vision 2022 Day 2 Keynote (Livestream/Replay) | Intel Vision 2022: Day 2 Keynote (Live Blog) | Intel Announces New Cloud-to-Edge Technologies to Solve Challenges of Today and Tomorrow (News) | Intel's Habana Labs Launches Second-

brings together technologies and the ecosystem to unlock business value for customers today and in the future. (Credit: Intel Corporation)

Generation AI Processors for Training and Inferencing (News) | 12th Gen Intel Core HX Processors Launch as World's Best Mobile Workstation Platform (News)

"As organizations continue to capitalize on the value of the cloud, security has never been more top of mind. Trust goes hand in hand with security, and it is what our customers expect and require when delivering on Intel technology," said Greg Lavender, chief technology officer, senior vice president and general manager of the Software and Advanced Technology Group at Intel. "With the introduction of Project Amber, Intel is taking confidential computing to the next level in our commitment to a zero-trust approach to attestation and the verification of compute assets at the network, edge and in the cloud."

Trust Assurance for the Hybrid Workforce

Businesses operate in and depend on the cloud to support remote workforces that require multiple devices, uninterrupted access and collaboration tools. Technology solutions need to secure data not only in memory and in transit, but also in use – protecting valuable assets and minimizing attack surfaces. Project Amber provides organizations with remote verification of the trustworthiness of a compute asset in cloud, edge and on-premises environments. This service operates independent of the infrastructure provider hosting the confidential compute workloads.

Confidential computing, the protection of data in use by performing computation in a hardware-based trusted execution environment (TEE), is a growing market. Intel® Software Guard Extensions (Intel® SGX) available on the Intel® Xeon® Scalable platform is one of the main technologies powering confidential computing today, enabling cloud-use cases that are beneficial for organizations that handle sensitive data on a regular basis.

The foundational basis of trust in a confidential computing environment is established via a process called attestation. The verification of this trustworthiness is a critical requirement for customers to protect their data and intellectual property as they move sensitive workloads to the cloud. To raise trust assurance and drive forward the promise of confidential computing for the broader industry, Intel announced Project Amber as the first step in creating a new multi-cloud, multi-TEE service for third-party attestation:

- Designed to be cloud-agnostic, this service will support confidential computing workloads in the public cloud, within private/hybrid cloud and at the edge. Interposing a third party to provide attestation helps provide objectivity and independence to enhance confidential computing assurance to users.
- In its first version, Project Amber intends to support confidential compute workloads deployed as bare metal containers, virtual machines (VMs) and containers running in virtual machines using Intel TEEs. The initial release will support Intel TEEs, with plans to extend coverage to platforms, devices and other TEEs in the future.
- Intel is also working with independent software vendors (ISVs) to enable trust services that include Project Amber. New software tools, such as published APIs that enable ISVs to incorporate Project Amber to augment software and services, will complement Intel's platforms and technologies, and bring more value to customers and partners.

Intel plans to launch a customer pilot of Project Amber in the second half of 2022, followed by general availability in the first half of 2023.

Paving the Way for Secure and Responsible AI

Artificial intelligence (AI) propels technology even further, enabling insights and automation to handle greater scale. With this proliferation of sensitive information, the threat landscape grows, as do the surrounding security concerns. That's why Intel is committed to developing artificial intelligence that is secure and responsible. Highlighting the criticality of AI outcomes being used as a force for good, Intel emphasized the key question technologists should ask before they decide to continue pursuing development: Does the technology contribute to improving our society?

Maintaining data integrity, accuracy and privacy is at the heart of Intel's industry-leading research efforts. Intel demonstrated how it is accelerating AI deployments in ways that are responsible and secure to help customers and partners solve complex problems:

- BeeKeeperAI uses Intel SGX hardware-based security capabilities and Microsoft Azure's confidential computing infrastructure to provide a zero-trust platform. It enables an AI algorithm to compute against multiple real-world clinical datasets without compromising the privacy of the data or the intellectual property of the algorithm model. This is accelerating healthcare AI development and deployment innovation by more than 30% to 40% when compared to the current method.
- Intel's research partnership with the University of Pennsylvania, Perelman School of Medicine's Federated Tumor Segmentation, or FeTS initiative, uses a set of Intel hardware and open-source software technologies to improve the training of AI models to locate brain tumors. Intel technology helps ensure each institution can participate in improving the fidelity and quality of the inferencing algorithms by using Open Federated Learning (OpenFL). OpenFL enabled 55 institutions across six continents to collaborate while preserving the security and privacy of their individual datasets. The result is an AI model that improves efforts to locate tumors by 33%.

The responsible use of AI also serves as an example of how the industry can come together and pave the path for deployment across verticals that include healthcare, financial services, manufacturing, retail and entertainment, among others.

Quantum-Resistant Cryptography for a Secure Quantum Computing Future

As quantum technology continues to develop, post-quantum experts anticipate a moment in the next 10 to 15 years when, as an industry, it will reach a similar situation as the "millennium bug." Many call it "Y2Q."

Quantum computing impacts both symmetric and public key cryptography, and will require the entire ecosystem to bring ingenuity and collaboration to find solutions. To be Y2Q-ready or quantum-resistant by 2030, the time to act is now. Intel is developing a rich cryptography technology pipeline to lead the industry with innovations that are quantum-resistant, including the built-in crypto acceleration in the 3rd Generation Intel Xeon Scalable platform that provides next-generation security without sacrificing performance.

Intel is working proactively to address threats posed by quantum computers. The company

developed crypto guidelines for Intel products, actively contributed to post-quantum crypto standardization efforts and is evaluating the new families of crypto algorithms being considered for standardization by the National Institute of Standards and Technology (NIST).

Intel has adopted a phased approach to address threats posed by quantum computing:

- Address the problem of data harvesting by increasing key and digest sizes for symmetric crypto algorithms.
- Increase robustness of code signing applications such as authentication of firmware and software with quantum-resistant algorithms. This helps guard against attacks that break classical crypto to run malicious code.
- Secure the internet with post-quantum crypto algorithms standardized by NIST. This includes key encapsulation and digital signature algorithms fundamental to securing transactions over the web.

Security technologies must accommodate not just the needs of today, but those of tomorrow. Intel's breadth and depth of hardware and software technologies enable customers to derive additional value from their existing platforms.

About Intel

Intel (Nasdaq: INTC) is an industry leader, creating world-changing technology that enables global progress and enriches lives. Inspired by Moore's Law, we continuously work to advance the design and manufacturing of semiconductors to help address our customers' greatest challenges. By embedding intelligence in the cloud, network, edge and every kind of computing device, we unleash the potential of data to transform business and society for the better. To learn more about Intel's innovations, go to newsroom.intel.com and intel.com.

View source version on businesswire.com:
https://www.businesswire.com/news/home/20220511005333/en/

Danielle Coe
1-206-498-2857
intelPR@we-worldwide.com

Source: Intel Corporation