Project Amber

Increasing Trust in Confidential Computing

As enterprises increasingly look to multi/hybrid-cloud environments, there's growing interest in a trusted third-party assurance service and new implementation of a trust authority to help build higher confidence in moving sensitive data to the cloud.

Project Amber introduces an innovative approach to objective third-party attestation.

Project Amber Decoded

Project Amber is the code name for Intel's groundbreaking service/SaaS-based implementation of an independent trust authority that provides attestation of workloads in a public/private multi-cloud environment.

Designed to remotely verify and assert trustworthiness of compute assets such as Trusted Execution Environments (TEEs), devices, Roots of Trust, and more, the service is operationally independent from the Cloud/Edge infrastructure provider hosting the confidential computing workloads.

Key Benefits

- Enables enterprises to use a single trust authority regardless of where the workload runs.
- Integrates with a cloud provider's assurance services as a value-add or acts as an independent, third-party assessment, increasing confidence in trustworthiness of sensitive workloads.
- Designed to be cloud-agnostic, Project Amber will support workloads in the public cloud, within private/hybrid cloud and at the edge.

Intel is working with independent software vendors (ISVs) to enable trust services that include Project Amber.

New tools, such as published APIs that enable ISVs to incorporate Project Amber to augment their own software and services, will complement Intel's platforms and technologies and increase value to customers and partners.

Project Amber is Intel's first step in creating a new multi-cloud, multi-TEE service for third-party attestation and will drive forward adoption of confidential computing for the broader industry.

The initial customer pilot, launching by the end of the year, will support confidential compute workloads deployed as bare metal containers, virtual machines (VMs), and containers running in virtual machines using Intel TEEs. The intent is to extend coverage to other TEEs in market in 2023.

SaaS service w/ 99.9% uptime SLA

Multi/Hybrid cloud & Edge Workload support

Multi-TEE support (Initially: Intel® SGX and Intel® TDX)

Federated model for Geo-support

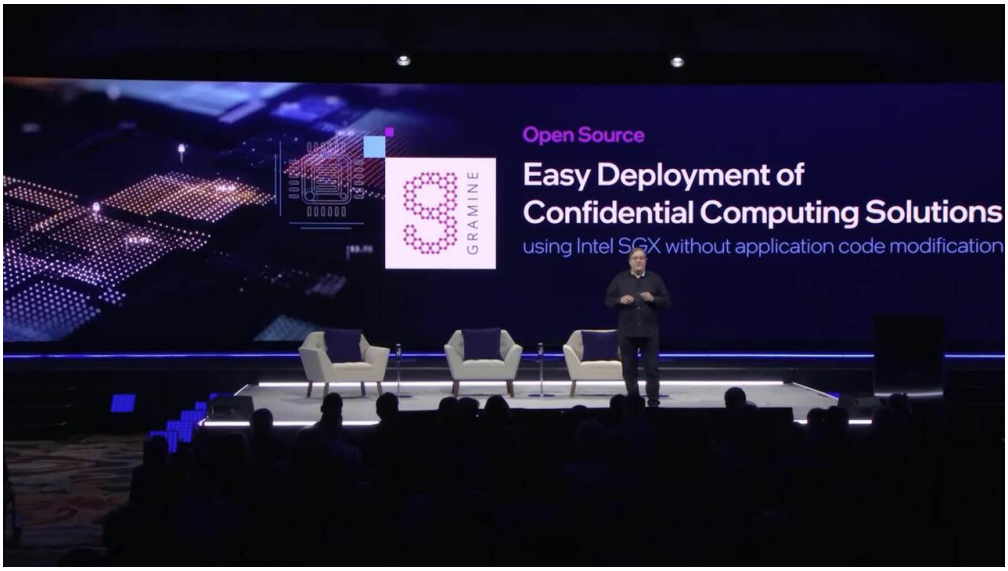
Provable Integrity of Verification Process

CSP agnostic & Multi-cloud deployment

Watch the Launch

Project Amber was introduced during the Intel Vision conference on March 11, by Intel's Chief Technology Officer, Greg Lavender. Watch the Day 2 keynote replay to learn about this innovative service.

Want the highlights? Watch the 5-minute supercut video on YouTube.



" 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. "

-- Greg Lavender

Expert Insight

BLOG: Advancing Confidential Computing with Intel's Project Amber

Nikhil Deshpande, senior director of security, and Raghu Yeluri

, lead security architect, share how next-generation forms of trust are needed to match the rapid shifts in computing infrastructure and enterprise usage, notably multi-cloud, hybrid cloud, and edge computing.

PODCAST: Live from the Green Room; Behind the Scenes of Project Amber

This episode in the Cyber Security Inside series features Raghu Yeluri, senior principal engineer and lead security architect, discussing how Intel's approach to independent attestation is poised to accelerate the adoption of confidential computing.

BLOG: How to Secure Security: The Frontier of Trust

BLOG: Securing AI - and Other Leading Use Cases - with

Confidential Computing

Anil Rao, VP and GM of Systems Architecture and Engineering outlines how confidential computing is a paradigm shift that enables growth of services that run on shared infrastructure, as well as new use cases reliant on collaboration among ecosystem partners.

In this companion blog, Anil Rao explains how Project Amber enhances the security of confidential computing by de-linking attestation and infrastructure, enabling attestation across multiple clouds, without requiring enterprises to invest in such capabilities.

Join the Pilot Program

Project Amber has evolved in collaboration with a number of customers and partners. Now, we're working to pilot the solution to further refine and optimize Project Amber's capabilities and market model.

If you're an enterprise, cloud service or infrastructure provider, ISV, or systems integrator interested in cloud-based or on-prem confidential computing deployment, we want to hear from you.

Contact Intel at ProjectAmber@intel.com to learn how you might be able to participate in the Project Amber pilot program.

What Others are Saying

"Project Amber is cloud-agnostic and designed to stand as a third-party solution to verify and provide an attestation for assets managed by other providers....verifying assets by a third-party offers enterprises a more objective approach to measuring risk than relying on a cloud service provider to testify to the security of their systems." VentureBeat

"With a need for organizations to meet growing security needs, the service focuses on one of the most critical security elements for any organization: trust. Project Amber operates as an independent trust authority in the form of an innovative service-based security implementation code." SiliconANGLE