Contribution ID: **28** Type: **not specified**

Confidential Computing MC

CFP ends on September 30th (CLOSED)
The Confidential Computing microconferences of the past years have been a significant catalyst for better supporting trusted execution workloads in the Linux virtualization and general software stack. Since the last occurrence of the microconference AMD SEV-SNP and Intel TDX support for KVM were merged into the mainline Linux kernel as well as support for the Linux kernel running in ARM CCA environments.

But the open source software stack for confidential computing is still far from being complete. There remain many problems to be solved and functionality to enable. Some of the most important ongoing developments are:

-Support for large-page backing of confidential virtual machines (CVM).
- Privilege separation features in KVM via VM planes.
- Live migration of CVMs.
- Secure VM Service Module architecture and Linux support.
- Trusted I/O software architecture.
- Further topics to discuss are:
- Possible solutions for the full CVM (remote) attestation problem.
- Linux as a CVM operating system across hypervisors.
- Performance of CVMs.

The Confidential Computing microconference of 2025 wants to bring open source developers working on these topics together into productive discussions and to collaborate on solutions for the open problems.

Key attendees:
Ashish Kalra ashish.kalra@amd.com
Borislav Petkov bp@alien8.de
Dan Williams dan.j.williams@intel.com
Daniel P. Berrangé berrange@redhat.com
Dr. David Alan Gilbert dgilbert@redhat.com
David Hansen dhansen@linux.intel.com
David Kaplan David.Kaplan@amd.com
David Rientjes rientjes@google.com
Dhaval Giani dhaval.giani@amd.com
Dionna Amalie Glaze dionnaglaze@google.com
Elena Reshetova elena.reshetova@intel.com
James Bottomley James.Bottomley@HansenPartnership.com
Joerg Roedel joro@8bytes.org
Kirill A. Shutemov kirill.shutemov@linux.intel.com
Michael Roth michael.roth@amd.com
Mike Rapoport rppt@kernel.org
Paolo Bonzini pbonzini@redhat.com
Peter Fang peter.fang@intel.com
Peter Gonda pgonda@google.com
Sean Christopherson seanjc@google.com
Stefano Garzarella sgarzare@redhat.com
Tom Lendacky thomas.lendacky@amd.com

Primary authors: GIANI, Dhaval; ROEDEL, Joerg (AMD)

Presenters: GIANI, Dhaval; ROEDEL, Joerg (AMD)