Security Must Be Open Source

Beyond the idealism:
A pragmatic framework for distributed trust, tooling, and vulnerability management.

CONFIDENTIAL COMPUTING CONSORTIUM

Who am I?

Mike Bursell
Executive Director, CCC

https://www.linkedin.com/in/mikebursell/

https://aliceevebob.com

Co-founder: Enarx project https://enarx.dev

Author: *Trust in Computing Systems and the Cloud* (Wiley, 2021)

Who am I?

Mike Bursell
Executive Director, CCC

https://www.linkedin.com/in/mikebursell/

https://aliceevebob.com

Co-founder: Enarx project https://enarx.dev

Author: *Trust in Computing Systems and the Cloud* (Wiley, 2021)

“Grey-beard”

Who am I?

Mike Bursell
Executive Director, CCC

https://www.linkedin.com/in/mikebursell/

https://aliceevebob.com

Co-founder: Enarx project https://enarx.dev

Author: *Trust in Computing Systems and the Cloud* (Wiley, 2021)

“Grey-beard”

Who am I?

Mike Bursell
Executive Director, CCC

https://www.linkedin.com/in/mikebursell/

https://aliceevebob.com

Co-founder: Enarx project https://enarx.dev

Author: *Trust in Computing Systems and the Cloud* (Wiley, 2021)

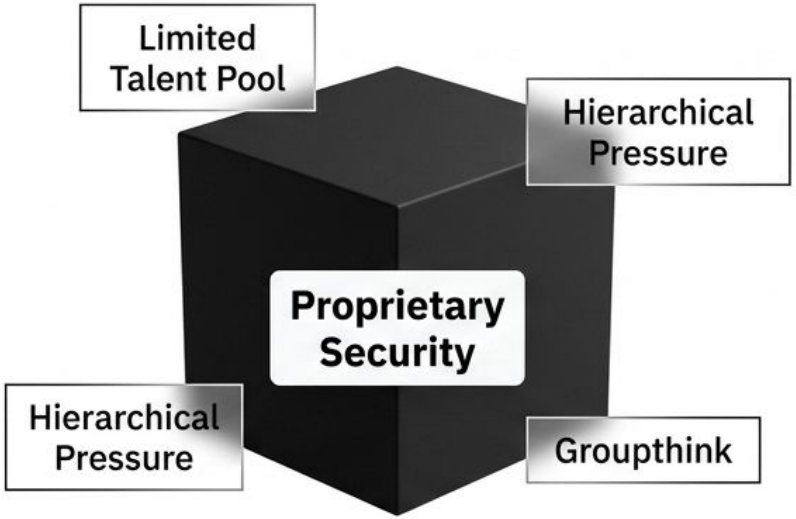
“Grey-beard”

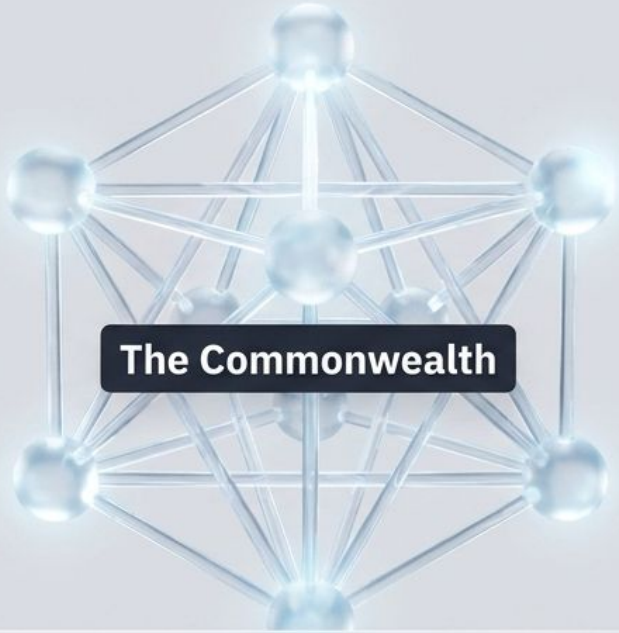
Our agenda

- Trust
- From one to many
- Enterprise scale
- Vulnerabilities & Disclosures
- Visibility

CONFIDENTIAL COMPUTING CONSORTIUM

Moving Beyond the Magic Wand





1. The Limitation: No matter how good proprietary architects are, the talent pool is inherently limited.

2. The Reality: Open source is not automatically secure just by being open.

3. The Agenda: We must examine the real mechanisms of trust, tooling, consumption models, and the messy realities of vulnerability management.

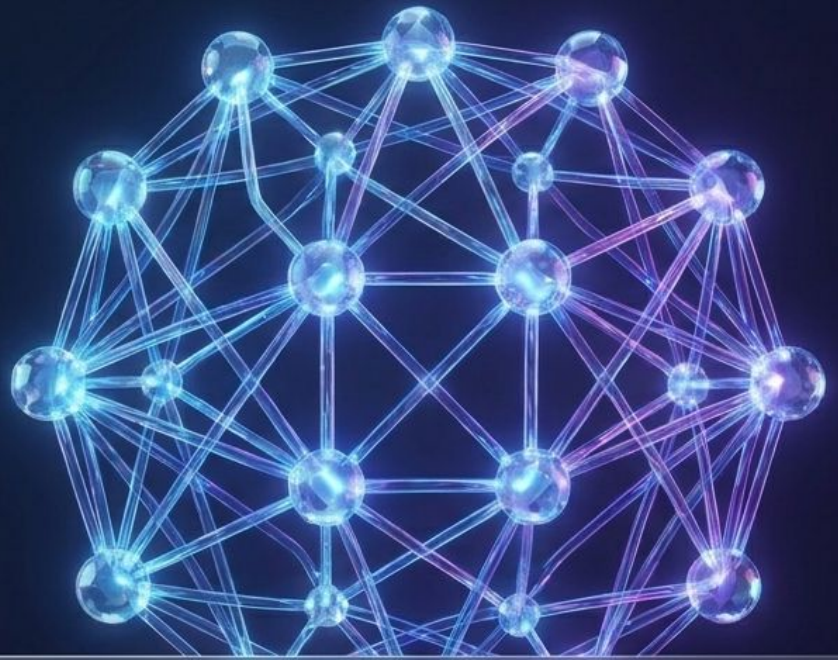
Trust

The Evolution of Digital Trust

Transitive Trust (Legacy Model)

Entity A trusts Entity B because Entity C trusts it. (Linear dependency)

Distributed Trust (The Wisdom of the Crowd)



Trust in open source is a positive feedback loop. Your impact on the code can be equal to that of the original creators, transforming passive consumption into active verification through a Community of Practice.

The Utilitarian Dilemma of the Commonwealth

The Commonwealth:
Our shared heritage, experience, and knowledge.

The Caveat:
Open source relies on classical utilitarianism—the belief that the net human happiness promoted outweighs the harm.

Benign Actors

Malicious Actors

The Reality:
There is no foolproof license that restricts usage strictly to good actors. The same code securing global banking is available to state-sponsored attackers, and good is entirely subjective.

Operationalizing Trust at the Source

Sigstore: Establishing the standard for signing, verifying, and protecting software components.

SLSA: Safeguarding artifact integrity across the entire software supply chain.

Takeaway: Trust is no longer a handshake; it is cryptographically signed and programmatically verified by the community.

From one to many

Debunking the Many Eyes Hypothesis

The Myth

Given enough eyeballs, all bugs are shallow.

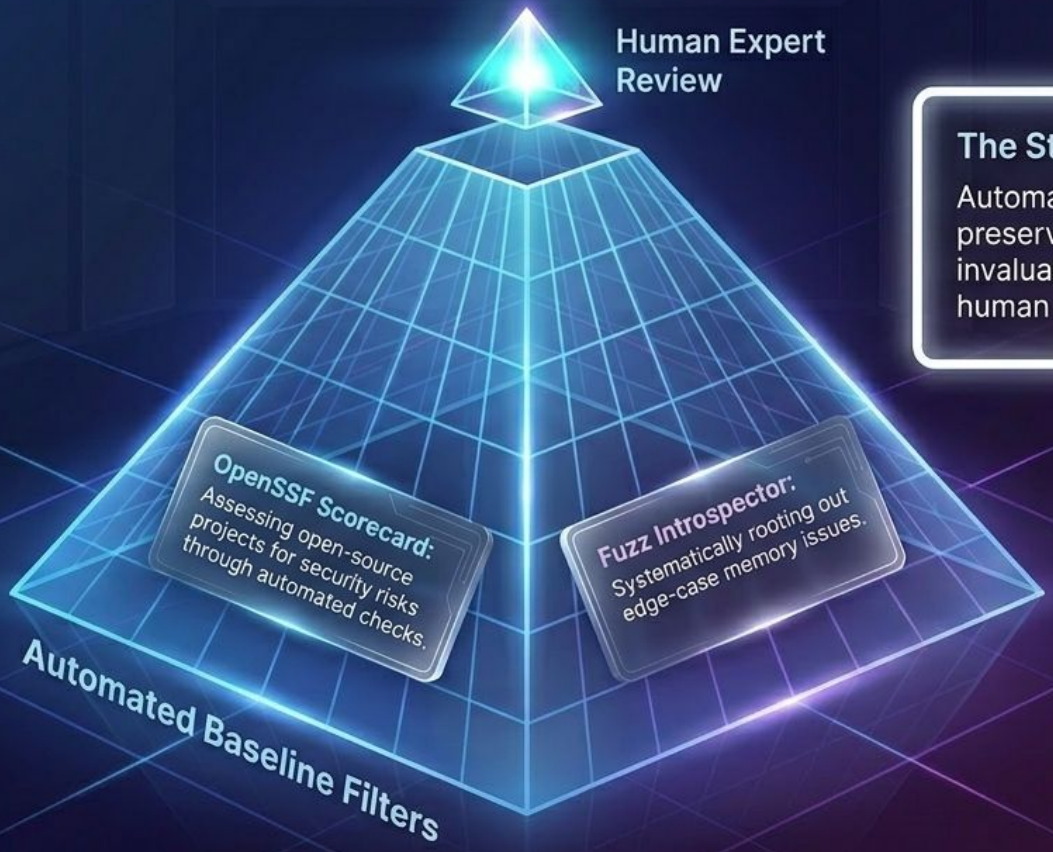
The Fallacy

The dangerous assumption of if you build it, they will come.

The Reality

For complex security functionality (like crypto primitives), the number of suitably qualified, expert eyes is incredibly low. We don't just need many eyes; we need expert eyes.

Augmenting Human Eyes with Automation



The Strategy:

Automate the baseline to preserve the scarce, invaluable resource of expert human attention.

Enterprise scale

CONFIDENTIAL COMPUTING CONSORTIUM

The Enterprise Fork in the Road

Consuming a Project

DIY compilation, tracking versions internally.

Hidden Cost

Internal productization. You abandon the commonwealth's economies of scale and must hire duplicate security expertise to backport patches.

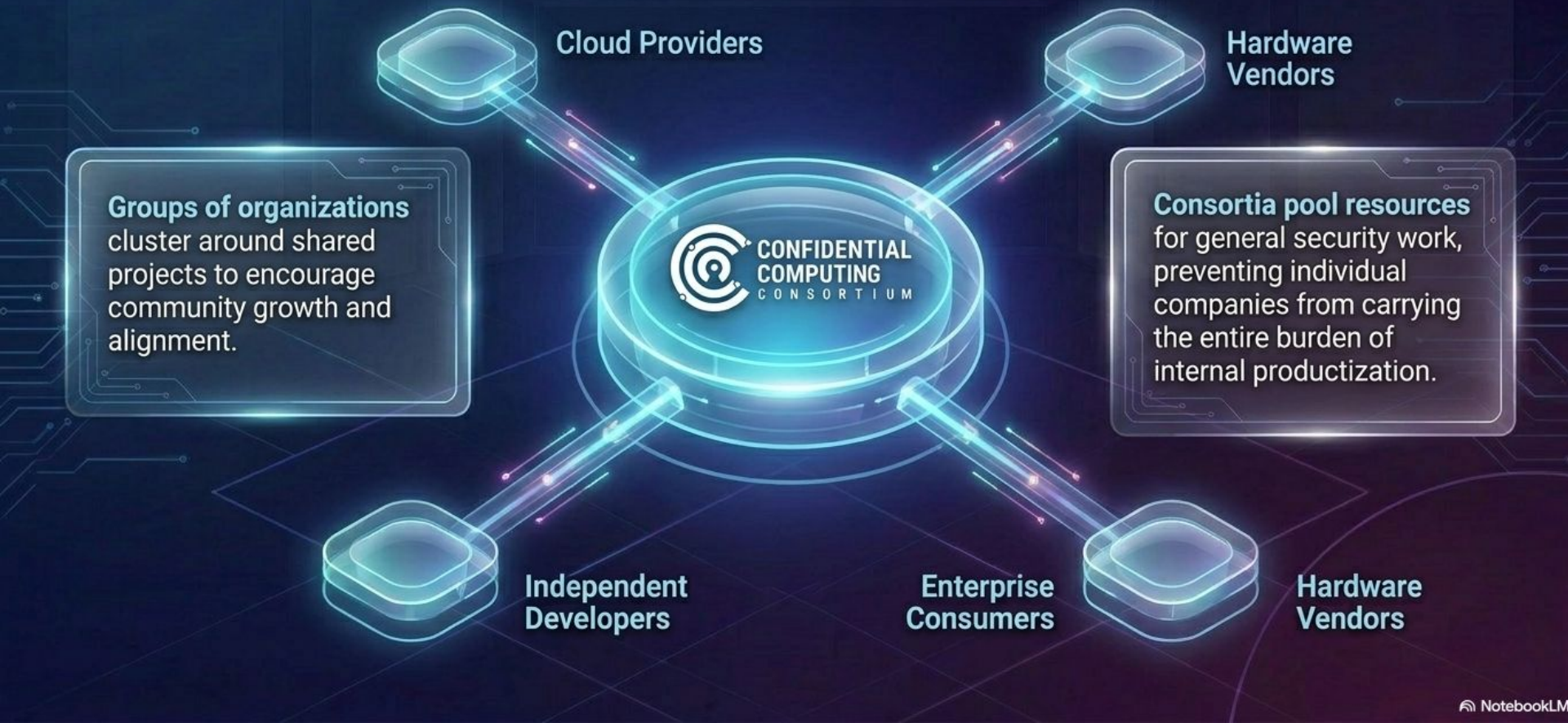
Consuming a Product

Vendor-supported, pre-packaged, tested.

Benefit

Economies of scale and scope. The vendor manages embargoed security fixes and upstream alignment.

Consortia as the Bridge to Scale



Open Collaboration in Confidential Computing

dstack

A developer-friendly, security-first SDK that simplifies the deployment of containerized applications into Trusted Execution Environments (TEEs).

Veraison

Building software components specifically designed to construct robust Attestation Attestation Verification Services.

Key Takeaway: These are not just projects; they are the standardized building blocks for a broader secure ecosystem.

The Risks of Vendor and Community Abandonment

Ecosystem Failure

The Vendor Risk

If a vendor goes bankrupt or drops a productised open-source project, you are left supporting an internal fork.

The Community Risk

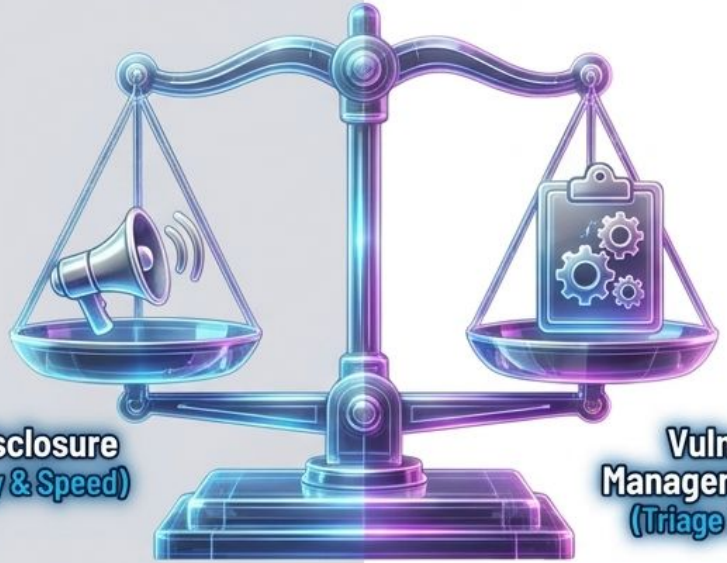
If a community abandons a fork, code without an active community becomes dead code.

The Open Source Advantage: Unlike proprietary software, you retain the source code and the legal right to form a new consortium or hire a new vendor.

Vulnerabilities & Disclosures

CONFIDENTIAL COMPUTING CONSORTIUM

Security Disclosure vs. Vulnerability Management



Security Disclosure
(Transparency & Speed)

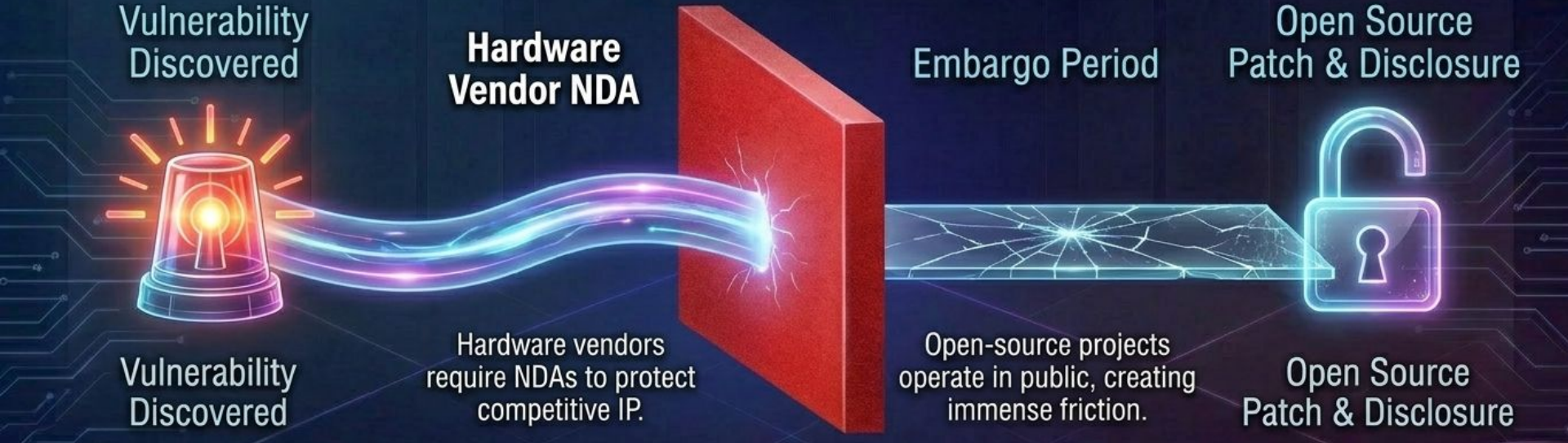
Vulnerability Management Process
(Triage & Mitigation)

Disclosure is sexy for headlines, but Management is how the industry survives.

Cover-ups are fatal to community trust, but uncontrolled immediate disclosure puts users at extreme risk. Open source requires a rigorous, mature VMP.

CONFIDENTIAL COMPUTING CONSORTIUM

The Coordination Paradox



The Paradox: How does an open community secretly patch code for unreleased hardware vulnerabilities without leaking the existence of the flaw?

The Fragility of Embargoes and Exclusion

The Exclusion Tax: NDAs fundamentally exclude independent, non-affiliated community members from critical security work, violating the open ethos.

The Leak Risk: The more individuals brought under an NDA to write a patch, the higher the mathematical probability of a leak.

The Reality: Embargoes are inherently fragile stopgaps, not permanent security solutions.

Standardizing the Chaos of Disclosure

When the embargo lifts, the standardized ecosystem can react programmatically, translating secret triage into public defense.

CONFIDENTIAL COMPUTING CONSORTIUM

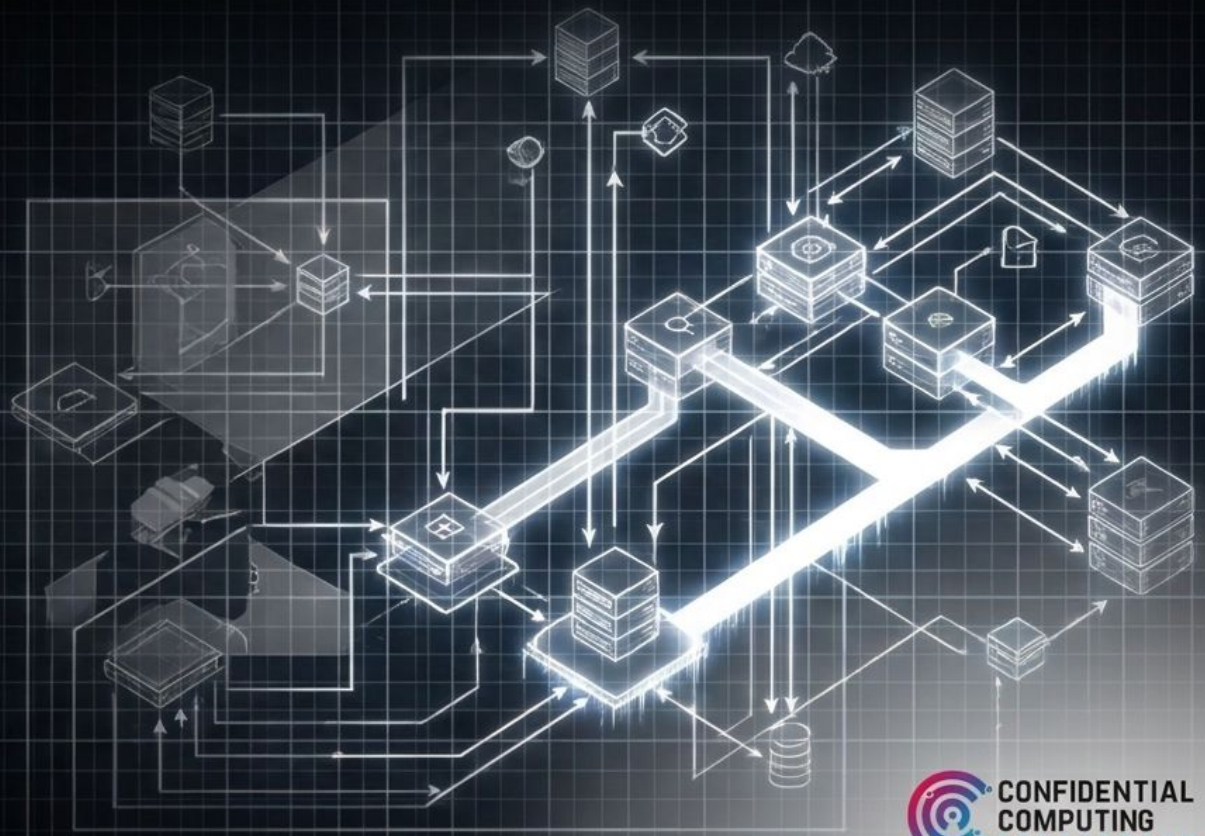
Visibility

You Cannot Secure What You Cannot See

There are not enough security experts to audit every line of code.

Architectural diagrams are mandatory. They force abstraction, reveal hidden dependencies, and trace critical data flows.

A project without a clear architectural diagram is inherently insecure because its emergent properties are invisible.



CONFIDENTIAL COMPUTING CONSORTIUM

Diagrams as Inclusivity Tools

Linguistic Profiles: Bridges gaps for those whose first language is not English.

Cognitive Profiles: Supports visual versus textual thinkers.

Legal Perspectives: Clarifies compliance boundaries.

Management Perspectives: Aligns business logic with engineering.

Visual architecture is not just documentation; it is a critical mechanism for cognitive and global diversity, creating a single source of truth.

The Overhead Tax of True Openness

- Creating and updating architectural diagrams takes engineering time.
- Maintaining VMTs and navigating NDAs requires legal overhead.
- Verifying identity through Zero-Knowledge Proofs slows onboarding.

The Reality: Pragmatic security means accepting friction. The days of “move fast and break things” in open source security are officially over.

The Transparent Vault

The Synthesis: Open source is not a magic wand. It is a rigorous, demanding framework. But a commonwealth of human knowledge, augmented by automation, guided by strict process, and built by verified humans is the only scalable future for global security.

CONFIDENTIAL COMPUTING CONSORTIUM

Questions