Protecting people's privacy online with

Confidential computing

People want personalized experiences but they don't want their personal information passed around the internet

Protecting people's **privacy and security** online is fundamental to ensuring that we can all trust the internet, and feel safe using it. Responsible companies that have collected first party data from their customers - with the right permissions in place - naturally want to keep that data safe and maintain the trust of their customers.

But matching customer data - comparing client lists across multiple companies for marketing measurement purposes - has always been a privacy challenge. And how can organizations ensure that people's data is not gathered for one purpose, and used for another? To meet these challenges, we're using confidential computing, a technology that transforms how data is used and protected.

With confidential computing, we can build trust, accountability and responsibility

Confidential computing means that data is processed in a **Trusted Execution Environment**. Put simply, this limits how data can be used and who can access it, while bringing new transparency to the process through **attestation**, or external auditing. The first application of confidential computing in Google's Ads products is with confidential matching.

Confidential computing ensures a security barrier that creates a guarantee of how data is used, and is already used in banking and healthcare. For example, MonetaGo uses confidential computing for enhanced financial fraud detection. Confidential computing is **private by design**, and already widely used to protect sensitive data like passwords and financial information.

Privacy enhancing technology

Privacy enhancing technologies (PETs) aim to to deliver measurable utility and verifiable privacy. Earning people's trust and protecting information is essential to Google's business, which is why we have been innovating in PETs for decades.

To help strengthen digital privacy while continuing to support business growth, we're investing in **confidential computing,** a privacy enhancing technology. We believe that building confidential technology based on core privacy principles will help the advertising industry develop stronger standards.

Building trust in digital advertising

Now that we're incorporating confidential computing into our ads products, when an advertiser uploads a client list, no one, including Google, can access it. It's encrypted end-to-end. Not only that, every business has the option to review and verify that the technology is working exactly as they intended, in line with its privacy policies. This new privacy and security feature will be available for all of our advertisers at no additional cost.

Trust is essential for long term business success. Advertising technology has enabled healthy competition, innovation, and efficiency in digital advertising. As we continue to innovate, we must balance privacy and utility in digital advertising to build trust and support advertisers and publishers. Confidential computing helps deliver on the promise that companies make to their customers: we will keep your information safe.

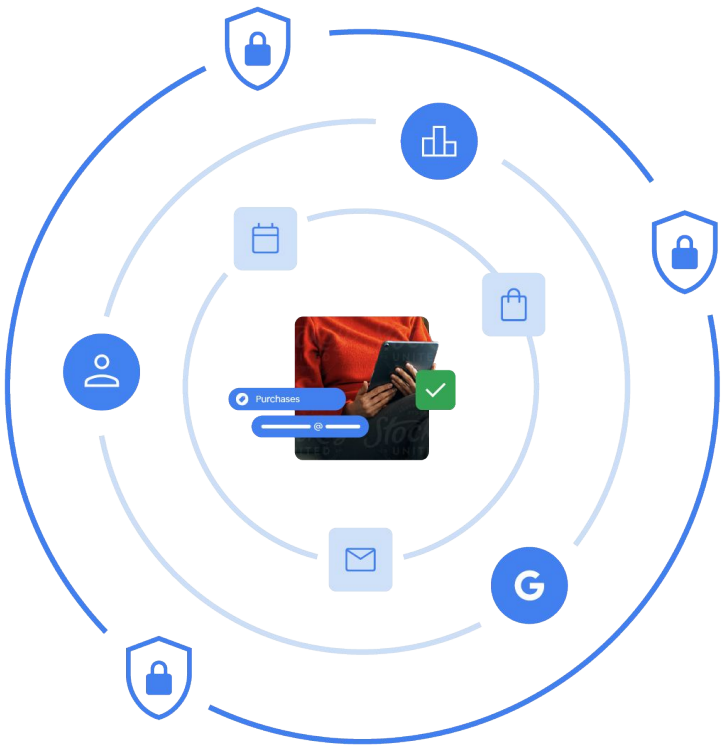
Supporting small businesses with privacy-centric tools

Small businesses count on digital ads to grow and sustain their businesses, and reach people who may benefit from products and services they offer.

Publishers rely on advertising revenue to allow them to sustain their businesses.

Now, confidential computing offers more privacy to the entire advertising ecosystem. We are making confidential computing available to businesses of all sizes, free of charge, paving the way for a truly privacy-centric digital advertising landscape that benefits everyone.

Privacy Enhancing Technologies support a safer ads ecosystem



Auditability and control:

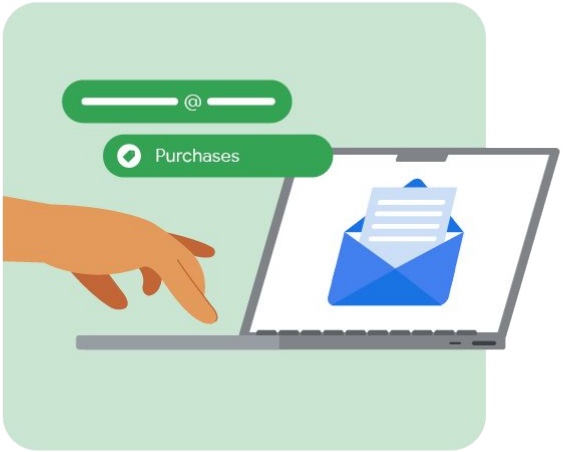
How confidential computing works

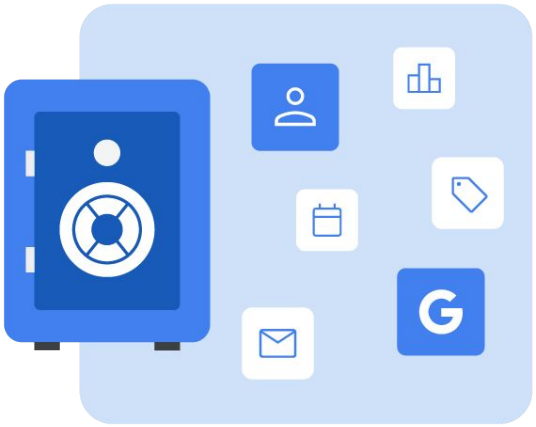
Google's solution delivers data security using:

Hardware Isolation:
A trusted execution environment (TEE) is a secure area within the main processor that Google uses to process data on its servers. This isolation protects it from threats in the broader system - it means that the data inside is protected from unauthorized access.

Operator and Insider Protection:
Even administrators (e.g. Google) cannot access the TEE's contents. This prevents external attacks or internal misuse.

Auditability:
The TEE generates records of device's software and hardware, to prove to auditors that the data has been protected and only used for specific purposes. This allows businesses to be confident that they can keep their promises to their customers.





TEEs are designed to help with:

Attestation - auditing how data is used:
When data is processed in a TEE, the customer restricts how the data is used. Data use and processing is provable, ensuring Google does not use customer information collected in one context for another. For these controls to work properly, the use cases must be clearly defined. The ability to verify a TEE's structure gives transparency to regulators or auditors that data is processed as intended. Put simply, it means that promises not to share data can be kept, and that promise is auditable and provable.

Cross platform interoperability: Not only will Google's TEE be available to all advertisers, we will also open-source code for many use cases of TEEs, because keeping the internet safe requires collaboration.

Scalable privacy: TEEs offer the privacy benefits without the cost and complexity barriers associated with many alternative technologies that provide similar data isolation.