Zoom places security as the highest priority in the operations of its suite of products and services. Zoom strives to continually provide a robust set of security features and practices to meet the requirements of businesses for safe and secure collaboration.

while real-time conference media is processed in globally distributed tier-1 colocation and commercial cloud data centers with SSAE 16 SOC 2 Type 2 certifications.

Real-time media processing

A distributed network of low-latency multimedia software routers connects Zoom’s communications infrastructure. With these Multimedia Routers (MMR), all session data originating from the host’s device and arriving at the participants’ devices is dynamically routed between endpoints

Firewall compatibility During session setup, the Zoom client connects via HTTPS to Zoom servers to obtain information required for connecting to the applicable meeting or webinar, and to assess the current network environment such as the appropriate Multimedia Router to use, which ports are open and whether an SSL proxy is used. With this metadata, the Zoom client will determine the best method for real time communication, attempting to connect automatically using preferred UDP and TCP ports. For increased compatibility and support of enterprise SSL proxies, connection can also be made via HTTPS. An HTTPS connection is also established for users connecting to a meeting via the Zoom web browser client.

End-to-end encryption: End-to-end encryption, when enabled, ensures that communication between all meeting participants in a given meeting is encrypted using cryptographic keys known only to the devices of those participants. This ensures that no third party — including Zoom — has access to the meeting’s private keys. End-to-end encryption is available as a technical preview to all customers.

Authentication Authentication methods include password, or single sign-on (SSO) with SAML or OAuth. Users authenticating with username and password can also enable two-factor authentication (2FA) as an additional layer of security to sign in.

With SSO, a user logs in once and gains access to multiple applications without being prompted to log in again at each of them. Zoom supports SAML 2.0 which enables web-based authentication and authorization including SSO. SAML 2.0 is an XML-based protocol that uses security tokens containing assertions to pass information about a user between a SAML authority (an identity provider) and a web service (such as Zoom).

Communications are established using 256-bit TLS encryption and all shared content can be encrypted using AES-256 encryption, and optional end-to-end encryption.

Controlled data routing that allows paying customers to opt-in or opt-out of any of our data centers (excluding their home region) and, for enterprise clients, the ability to customize and manage geographic regions for specific meetings

We meet the following industry and security organization standards: ● SOC 2 (Type II) ● FedRAMP (Moderate) ● GDPR, CCPA, COPPA, FERPA, and HIPAA Compliant (with BAA)

Zoom enables secure meetings via multiple methods and technologies, including optional two-factor authentication; optional end-to-end AES-256 GCM meeting encryption; passcode authentication; the ability to deny, block, or remove attendees; and the ability to lock meeting/webinar access.

During the first few months of 2020, the Zoom team worked around the clock to support the tremendous influx of new and different types of users. The sudden and increased demand was unlike anything most companies have ever experienced. As March 2020 ended, Zoom quickly realized that it needed to expand its work on security and privacy—so it began making a number of enhancements to deepen security and privacy in Zoom’s DNA.

Despite this ongoing work, Zoom has been experiencing a “trust gap” with potential users across industries. This is not because of a lack of new security or privacy features; Zoom has continued to enhance and expand its security feature set. This is more due to a lack of understanding of/hesitancy to accept Zoom’s assertions of its commitment to security and privacy

Zoom’s security program includes numerous third-party certifications and attestations: to support customer needs across industries and verticals: • SOC 2 Type II • CSA STAR Level 2 Attestation • FedRAMP Moderate • HIPAA/HITECH Attestation

. By default, all data transmitted from a Zoom client to the Zoom cloud is encrypted in transit.

“End-to-end encryption” is an additional option for all Zoom users—free and paid—and is not enabled by default. Zoom’s optional end-to-end encryption, when enabled, ensures that communication between all meeting participants is encrypted using cryptographic keys known only to the devices of those participants. This ensures that third parties, including Zoom, do not have access to the meeting’s private keys.

Data Routing Control Customers on paid accounts can customize their data center settings with respect to data in transit for Zoom meetings and Zoom video webinars at the account, group, or user level. Organizations can opt in to, or out of, specific data center regions with respect to meeting and/or webinar data in transit (see Figure 4). If someone needs to join a meeting from an opted-out region, they can, but the meeting data will still not pass through the opted-out data center.

Hundreds of millions of participants join Zoom Meetings each day. They use Zoom to learn among classmates scattered by recent events, to connect with friends and family, to collaborate with colleagues and, in some cases, to discuss critical matters of state. Zoom users deserve excellent security, and Zoom is working to provide these protections in a transparent and peer-reviewed process.

In the meeting setting (as opposed to webinars), Zoom supports up to 1,000 simultaneous users. When a Zoom client gains entry to a Zoom meeting, it gets a 256-bit per-meeting key created by the Zoom server, which retains the key to distribute it to participants as they join. In the version of Zoom’s meeting encryption protocol released on May 30, 2020, this per-meeting key is used to derive a per-stream key by combining the per-meeting key with a non-secret stream ID using an HMAC function. Each stream key is used to encrypt audio/video (UDP) packets using AES in GCM mode, with each client emitting one or more uniquely-identified streams. Those packets are relayed and multiplexed via one or more Multimedia Routers (MMR) in Zoom’s infrastructure. The MMR servers do not decrypt these packets to route them. There is no mechanism to re-key a meeting.

sAll meeting data sent over UDP gets encrypted with AES in GCM mode [9]. Key derivation uses the HKDF algorithm [11]. For public key encryption and signing, we rely on DiffieHellman over Curve25519 [4] and EdDSA over Ed25519 [5]. We use the interface and implementation of the NaCl [6]-inspired libsodium library [8], as detailed below.

For signing, we use libsodium’s EdDSA implementation directly: • Sign.KeyGen generates a keypair (vk, sk) (via crypto sign keypair). • Sign.Sign takes as input a context string Context and a message M and outputs a “detached” signature Sig over SHA256(Context)||SHA256(M) (via crypto sign detached). • Sign.Verify takes as input a detached signature Sig, a context string Context, and a message M; it outputs true on verification success and false on failure (via crypto - sign verify detached)

We have proposed a roadmap for bringing end-to-end encryption technology to Zoom Meetings (as that term is best understood by security experts). At a high level, the approach is simple: use public key cryptography to distribute a session key to a meeting’s participants; and provide increasingly stronger bindings between public keys and user identities. However, the devil is in the details, as user identity across multiple devices is a challenging problem, and has user experience implications. We proposed a phased deployment of E2E security, with each successive stage giving stronger protections.

Zoom was hosting 10 million users before the COVID-19 pandemic, now the number has increased to 300 million meeting participants. This increase in usage has also placed Zoom under the microscope, revealing numerous security and privacy issues

Usability Flexibility Ease of Use Simplicity connectivity

The heightened security will also come with some tradeoffs – recording of calls in will be disabled for encrypted meetings, as will ‘phone bridging,’ the ability to dial into a Zoom meeting by telephone.

**Oblivious Servers**

In typical meetings, its cloud meeting servers generates encryption keys for every meeting and distributes them to meeting participants using Zoom clients as they join.

With Zoom's new E2EE, it continued, the meeting's host generates encryption keys and uses public key cryptography to distribute these keys to the other meeting participants, who will also see the meeting leader's security code that they can use to verify the secure connection. The host can read this code out loud, and all participants can check that their clients display the same code.

Headlines report on bans imposed by governments and private sector companies against the platform. In order to fix privacy and security issues, the company has instantly issued a number of patches, formed a security board consisting of known professionals from the security community, and announced a 90-day feature freeze.

Turning on end-to-end encryption comes with various inconveniences. When you have it enabled, all call participants need to call in from either the Zoom desktop or mobile apps—not a browser—or a Zoom Room. (That also means no telephone participants.) Features like cloud recording, live transcription, breakout rooms, polling, one-on-one chat, and meeting reactions aren’t compatible with end-to-end encryption, and no one can join the meeting before the host does.

### Some users are done with Zoom

In the meantime, several governments and prominent companies (Tesla, Google) have prohibited staff and employees from using Zoom for work.

According to Blind, who polled 4,392 professionals from various big US companies, 12% of professionals have completely stopped using Zoom due to security issues, and 9% are using Zoom less.