Security 90-day plan

Pre 90-day plan:

March 20th:

- Published a blog post to help users address incidents of harassment (or so-called "Zoombombing") on our platform by **clarifying the protective features** that can help prevent this, such as waiting rooms, passwords, muting controls, and limiting screen sharing.

March 27th:

- **Removed the Facebook SDK** in our iOS client and have reconfigured it to prevent it from collecting unnecessary device information from our users.

March 29th:

- Updated our **privacy policy** to be more **clear and transparent** around what data we collect and how it is used – explicitly clarifying that we **do not sell our users' data**, we have never sold user data in the past, and have no intention of selling users' data going forward.

For education users we:

- Rolled out a **guide for administrators** on setting up a virtual classroom.
- Set up a guide on how to better **secure their virtual classrooms**.
- Set up a **dedicated K-12 privacy policy**.
- Changed the **settings for education users** enrolled in our K-12 program so **virtual waiting rooms are on by default**.
- Changed the settings for education users enrolled in our K-12 program so that **teachers by default are the only ones who can share content** in class.

April 1st:

- Published a blog to **clarify the facts around encryption** on our platform – acknowledging and apologizing for the confusion.
- Permanently removed the attendee attention tracker feature.
- **Released fixes for both Mac-related issues raised by Patrick Wardle**.
- Released a fix for the UNC link issue.
- Permanently removed the LinkedIn Sales Navigator app after identifying unnecessary data disclosure by the feature.
- Announced that **over the next 90 days, we are committed to dedicating the resources needed to better identify, address, and fix issues proactively. This includes**:
    - Enacting a **feature freeze**, effectively immediately, and shifting all our engineering resources to **focus on our biggest trust, safety, and privacy issues**.
    - Conducting a comprehensive review with third-party experts and representative users to understand and ensure the security of all of our new consumer use cases.
    - Preparing a transparency report that details information related to requests for data, records, or content.
    - Enhancing our current bug bounty program.
    - Launching a CISO council in partnership with leading CISOs from across the industry to facilitate an ongoing dialogue regarding security and privacy best practices.

- Engaging a series of simultaneous white box penetration tests to further identify and address issues.
- Starting next week, I will host a weekly webinar on Wednesdays to provide **privacy and security updates to our community**.

April 8th: Announcements

- **Eric's first weekly AMA webinar**
- Zoom formed **CISO Council and Advisory Board**, including security leaders from across industries
- **Alex Stamos has joined Zoom as an outside advisor** to assist with the comprehensive security review of our platform

New Releases:

- Addition of Zoom meeting control, '**Security**'
  - Lock the meeting
  - Enable waiting room
  - Remove participants
  - Restrict participants' ability to:
    - Share their screens
    - Chat in a meeting
    - Rename themselves
    - Annotate on the host's shared content
  - The Security icon replaces the Invite button in the meeting controls. The Invite button has been moved to the Participants panel, and hosts can add additional guests there.
- **Change defaults**:
  - Waiting Room by default for free Basic, single licensed Pro accounts, as well as education accounts enrolled in our K-12 program.
  - Password on by default for free Basic, single licensed Pro accounts, and for education accounts enrolled in our K-12 program. The default setting cannot be changed for those education accounts.
  - Alphanumeric characters in password (6 characters) for Basic Account users
- **Meeting ID**:
  - Removed from the title bar
  - One-time meeting IDs for newly scheduled meetings will be 11 digits (PMIs will remain the same)
- **Domain contacts**:
  - For free Basic and single licensed Pro accounts with unmanaged domains, contacts in the same domain will no longer be visible. We've also removed the option to auto-populate your Contacts list with users from the same domain. If you would like to keep those contacts, you can add them as External Contacts.

April 10th:

- **Cloud Recording**:
  - Passwords are now on by default
  - Require complex password (must be 8+ length, with at least 1 digit, 1 character & 1 special character)

April 12th:

- **Zoom Chat**:
  - Mask the content of the message in the notification
  - File sharing security enhancement
- Dashboard Enhancements: Performance tuning
- **Password Complexity**: Admins will have the ability to define meeting/webinar password guidelines

April 14th: New Releases

- Password requirements for meetings and webinars (account owners and admins can configure password requirements)
- **Random meeting IDs**: One-time randomly generated meetings IDs for newly scheduled meetings and webinars will be 11 digits instead of nine. Your Personal Meeting ID (PMI) will remain the same.
- **Cloud recordings**: Password protection for shared cloud recordings is now on by default for all accounts. We've also enhanced the complexity of passwords on your cloud recordings. Existing shared recordings are not affected.
- **Third-party file sharing**: You can once again use third-party platforms, such as Box, Dropbox, and OneDrive, to share across the Zoom platform. We temporarily disabled this feature and have restored it after a full security review of the process.
- **Zoom Chat message preview**: Zoom Chat users can hide the message preview for desktop chat notifications. If this is turned off, you'll simply be alerted that you have a new message without displaying any message content.
- Additionally, we've fixed issues related to missing data and delay on the Zoom Dashboard. We will continue to monitor and make improvements to dashboard and reporting performance.

April 15th:

Eric's second weekly AMA webinar: Main takeaways

- New Security icon in the meeting controls: The newly released Security icon in the toolbar provides Zoom Meetings hosts and co-hosts with one-click access to a number of existing Zoom security features, including Lock Meeting and Enable the Waiting Room.
- Changes to Zoom's default settings: Both meeting passwords and Waiting Rooms are **enabled by default** for our free Basic users and single Pro users, while those in our **K-12 education program need a password** to join a meeting. **Waiting Rooms** also are on by **default for those K-12 users**.
- Enhanced meeting password complexity
- **Changes to data center routing**: Starting April 18, account admins will have the ability to choose whether or not their data is routed through specific data center regions, giving users more control of their interactions with Zoom's global network.
- **Bug bounty program with Katie Moussouris of Luta Security**: Zoom will be working with Luta Security to reboot our bug bounty program. Luta Security was founded by Katie Moussouris, who created some of the most important vulnerability programs still running today. She started Microsoft Vulnerability Research and Symantec Vulnerability Research, and also started Microsoft's and the Pentagon's bug bounty programs. Luta Security will be assessing Zoom's program holistically with a 90-day "get well" plan, which will cover all internal vulnerability handling processes.

- **Introducing Alex Stamos**: Former CSO of Facebook and the director of Stanford's Internet Observatory, who will be joining Zoom as a consultant to help us identify and implement enhanced security measures.

April 18th: New Releases

- **Customizable Data Center Selection**: Accounts can choose to customize which data center regions their account will use for real-time traffic with an account/group/user setting

April 19th:

- **Zoom Phone**: Phone admins will have the ability to define cloud recording passwords guidelines
- **Cloud Recording password guidelines**: Admins can now define meeting and webinar cloud recording password guidelines to be a minimum length and include letters, numbers, special characters, or just be numeric passwords.
- **Dashboard Enhancements**: Provide additional visibility in the dashboard on how data is being routed
- **Linking accounts**: Admins can now securely share contacts across multiple accounts using a new self-serve web feature to link their accounts to one organization. This feature can be found in Account Management – IM Management – IM Settings.
- **Voicemail PIN**: Zoom Phone administrators can require a longer PIN to access voicemail.
- **Call recording access**: Zoom Phone account owners and admins can now enable or disable users' ability to access, download, or delete their automatic call recordings.

April 20th: New Releases

- **Control your Zoom data routing**: Customers on paid accounts can now customize their data center settings with respect to real-time meeting traffic for Zoom Meetings and Zoom Video Webinars.

April 22nd:

- **Eric's third weekly AMA webinar**: Main takeaways
  - **Zoom surpasses 300M daily meeting participants**
  - **Announces Zoom 5.0**
    - AES 256-Bit GCM Encryption: Zoom 5.0 supports AES 256-bit GCM encryption, which provides more protection for meeting data and greater resistance to tampering. Organizations will have access to GCM encryption with the release of Zoom 5.0, and a system-wide account enablement will occur May 30, when all Zoom customers will switch to the new cryptographic mode.
    - Report a User: Hosts and co-hosts can report users to Zoom's Trust & Safety team, who will review any potential misuse of the platform and take appropriate action. This feature will be found within the Security icon in the meeting controls.
  - **Introduces Lea Kissner, former Global Lead of Privacy Technology at Google and Chief Privacy Officer of Humu, who has joined Zoom as a security consultant**.
  - Data Routing Control: Zoom admins and owners of paid accounts can opt in or out of any data center region (apart from their home region) at the account, group, or user level.

April 27th: New Releases

- **Zoom 5.0 generally available**
- **'Report a User' to Zoom**:
  - Meeting hosts and co-hosts can report a user in their meeting who is misusing the Zoom platform. Found in the Security icon, the option sends a report to Zoom's Trust & Safety team for review. The report can include a specific offense, description, and optional screenshot. The Report a User function is on by default but can be turned off at the account, group, and user level in the Zoom web portal.
- **AES 256-Bit GCM Encryption**:
  - This release delivers one of our most advanced security enhancements to date with support for AES 256-bit GCM encryption, which provides added protection for meeting data and greater resistance to tampering.
  - Zoom 5.0 supports our current encryption and GCM encryption. A system-wide account enablement to GCM encryption will occur on May 30, 2020, and only Zoom clients on version 5.0 or later, including Zoom Rooms, will be able to join Zoom Meetings starting May 30.
- **New encryption icon**:
  - Meeting hosts and co-hosts can report a user in their meeting who is misusing the Zoom platform. Found in the Security icon, the option sends a report to Zoom's Trust & Safety team for review. The report can include a specific offense, description, and optional screenshot. The Report a User function is on by default but can be turned off at the account, group, and user level in the Zoom web portal.
- **Enhanced data center information**:
  - Meeting hosts can now select data center regions at the scheduling level for meetings and webinars. The Zoom client also shows which data center you're connected to in the Info icon in the upper left of your Zoom window. You can get additional details in-meeting by selecting Video Settings – Statistics in the meeting controls.
  - Additionally, if organizations outside of China did not opt in to the China data center before the April 25 deadline, those accounts will not be able to connect to mainland China for data transit.
- **Enhancements to ending/leaving meetings**:
  - We've refined the action of ending or leaving a Zoom Meeting to make it easier and also more secure. With a new UI update, hosts can clearly decide between ending or leaving a meeting. If the host leaves, they can now easily select a new host and have the confidence that the right person is left with host privileges.
- **Additional security enhancements**:
  - Profile picture control: Account admins and hosts can disable the ability for participants to show their profile picture and also prevent them from changing it in a meeting.
  - Minimum password length: The minimum default password length will be six characters for meetings, webinars, and cloud recordings.
  - Cloud recording security: Admins and meeting hosts can set expirations on their cloud recordings and can disable the sharing of their recordings.

Announcements and New Releases Pending:

May 7:

Launching a company wide security training for developers across the board. We are also building and strengthening security pipeline with multiple security tools including mobile security and dynamic analysis.

May 15 - June 15:

White Box Pen test - Completed China Network Route by Third party, we are working on a project to confirm that meetings are using AES 256. We have three major security researchers engaged with Zoom in one way or another: Majority of the work will be completed by mid June.

There's a lot more in the works that we are not ready to discuss at this point, but there more updates to come...