Elo OS 360 for Android – FAQs

Elo Touch Solutions

Table of Contents

1. What is OS 360?

   OS 360 is a device support model for security on all Elo Android operating systems (OS) starting from Android 10. OS 360 provides Elo customers with the following features:

   - Monthly security updates
   - OS upgrades to maintain most current Google security patches
   - Extended availability of OS security updates/patches beyond what is offered by Google
   - Easy integration with EloView or 3rd party UEM

   OS 360 is intended for enterprise customers by providing coverage of known security risks and decreases costs for maintaining Android devices.

2. What is a CVE?

   All operating systems, whether it is Android or Windows, are susceptible to potential security risks and hacking. In Android, there is a list of common vulnerability exposures (CVE) that shows all potential known security vulnerabilities which range in severity level, and each CVE is tied to a unique number. You can find a list of all CVEs at https://cve.mitre.org/cve/.

3. What are Google security patches?

   Because Android operating systems are maintained by Google, each month Google publishes an Android Security Bulletin which contains a list of known CVEs for a corresponding month. You can find the Android Security Bulletin here: https://source.android.com/security/bulletin/. Along with each monthly bulletin, Google and the related hardware vendors will provide security patches for each CVE which then needs to be integrated into the OS to mitigate the known security risk.

4. How does OS 360 work?

   Elo Android devices on OS 360 will receive monthly updates to download and install. These updates can be applied on the device manually through an over-the-air (OTA) update or remotely using EloView or your preferred UEM through OEMConfig.

5. Are future operating systems supported by OS 360?

   OS 360 supports Elo Android devices starting with Android 10. OS upgrade availability depends upon hardware support from chip suppliers as well as other business factors

and may not always be available. OS upgrades are not guaranteed on all devices. OS upgrades are planned for Elo I-Series 4, Backpack and M50 devices through Android 12.

6. Do I need an EloView account to use OS 360?
    No. An EloView account is only needed for remote OS 360 updates. An OTA update can be applied manually from the device through the Android settings or using your preferred UEM through OEMConfig if the OS 360 status is active.

7. Will I get monthly updates if I use a 3rd party UEM provider?
    OS 360 updates will be available on the Elo Android device via manual OTA updates through the Android settings as long as the OS 360 status is active. Remote OTA updates are available with a 3rd party UEM provider through OEMConfig.

8. Will I get monthly updates throughout the lifetime of a device?
    OS 360 provides monthly updates if a device is on the latest available OS. Once a new OS is available for a device, security updates will be made on a quarterly basis for the previous OS. An OS upgrade is required to maintain monthly OS 360 updates.

9. How long does Google provide security support for Android releases?
    Google typically provides security support for a period of 36-42 months after an OS release has gone open source. For example, Android 12 was released in October 2021, so security updates for this version of Android will be provided monthly via Google through the beginning of 2025.

10. Are updates available for an OS that Google no longer supports?
    Any Elo Android OS version 10 or above that Google has ended support will continue to receive certain updates based on severity and technical capability at the discretion of Elo.

11. How can I purchase OS 360?
    OS 360 will be available as a 3-year, 4-year or 5-year OS support for all Elo devices with Android OS 10 and up. It can be ordered from the Elo Price List as E873133 (3-year OS 360) E565885 (4-year OS 360) or E873326 (5-year OS 360). Once the extension is

purchased, the corresponding device will show an active OS 360 status with the corresponding expiration date.

12. Why is OS 360 important now?

In 2016, Android and iOS accounted for almost 99 percent of the global mobile OS market. Though this widespread usage has numerous advantages, this also makes devices attractive targets for hackers. As a result, enterprise clients must be more prescriptive and rigorous than ever before when it comes to maintaining the security of their mobile operating system.

13. Can Elo guarantee that my device is safe if I keep it up to date?

No. It is repeatedly noted that Security is a never-ending journey. Security updates are one component in an "In-depth defense" security paradigm. Specifically, a paradigm with numerous degrees of security. For increased security, customers should install the most recent security updates and use normal Android and Elo features.

14. What kinds of attacks are we trying to prevent?

There are distinct kinds of attacks. Remote code execution, application privilege escalation (allowing an application access to resources it should not), information disclosure on the device, and denial of service assaults are all frequent threats. It is worth noting that many recent attacks have relied on social networking rather than exploiting OS flaws (e.g., phishing).

15. Does Elo recommend all updates to customers?

According to Elo, customers should apply all updates as soon as they are available. However, we recognize that all software updates come with some level of functional risk. Customers operating during peak season (and facing a code lockdown) may wish to look into the specific CVEs addressed in a release. Many of these CVEs may already be mitigated by customers (e.g., application whitelisting, enterprise home screen, lock task mode). Customers should make an informed decision even though updates will give an additional layer of defense (in-depth defense).

16. Are Elo updates ever pushed to devices covertly?

No. Unlike other platforms (e.g., iOS), Elo does not push updates to devices either explicitly (e.g., a message asking the user to accept the update) or secretly (e.g., a message asking the user to accept the update).

17. What happens for zero-day attacks?

At times, a crucial attack might appear out of nowhere. These attacks are unpredictable, and it will be challenging to forecast a response time. Even though, Elo keeps an eye out for such attacks and has already replied in real time.

18. How does Elo decide what to push after google support ends?

The Android security bulletins are the primary source of Elo updates. This is accurate both during and after Google's support for a particular OS release. As a result, after Google's help, Elo evaluates each vulnerability and decides how to backport applicable updates (if possible)

It should be noted that certain security vulnerabilities may be systemic during this time, necessitating considerable improvements that would have an impact on the platform's stability and interoperability in an earlier OS version. In such instances, Elo cannot promise that every vulnerability will be addressed directly. As a result, Elo will make remedial suggestions but may not be able to give a code patch or update.

19. Are there any GMS security updates provided by OS 360?

Google Mobile Services (GMS) devices are made up of two primary software components: the Android Open-Source Project (AOSP) and Google Mobile Services (GMS) (GMS). GMS libraries are closed binaries licensed and distributed by Google, whereas AOSP is open source. Google usually updates the GMS libraries through the Android Play Store (access to the play store is required). The sole exception is when Elo releases a full image upgrade, so in that point the GMS libraries will be included. It's worth noting that the GMS version offered by Elo might not be the most recent. Consumers who have GMS-enabled apps should enable a connection to the Play Store so that they can get GMS updates.

20. How large is a standard android security update?

The sizes of each update can differ significantly. The size of Security updates that include bug fixes and maintenance releases will be bigger.

21. How do I know if my device has been updated with security updates?
    The Patch Level shows the date of the most recent, critical only, monthly, and quarterly updates.

22. Is the security update always different from other maintenance releases?
    No, Security Updates can come alone or as part of a larger package of bug fixes and maintenance releases.

23. Are these security updates cumulative?
    Yes. If you chose not to install an earlier update, installing a recent update will install both the prior and current updates.

24. Are release notes a part of security updates?
    Yes. The security update comes with release notes and these notes can be found on the OS 360 security bulletin board https://www.elotouch.com/services/elocare-os-360/security-bulletins.

25. After a security bulletin, how long will it take Elo to release a security update?
    Elo's objective is to be within 2-3 days of the Android security advisory being released to the public. Many upgrades, however, vary in complexity and breadth, and others rely on third-party code that Elo must obtain. As a result, security updates may differ by location, product type, and third-party software providers. Furthermore, owing to additional testing and/or carrier certification, WAN (cellular) device releases may lag other releases. Carrier certifications can take anywhere from two to six weeks, depending on the carrier and the amount of testing necessary. It is also worth noting that an update might be a mix of a maintenance release and a security upgrade.

    Finally, because of the latency in carrier certification, a carrier approved update may include a security patch level that is earlier than a previous release. Customers should verify the patch level and, if required, load the appropriate patches before installing a new, significant, carrier-certified update.

26. **Can I purchase OS360 at a later stage after my device purchase date?**
    Yes, OS360 can be purchased later after the device purchase date. It is important to note that the OS360 start date will be the same as the device purchase date since the securities provided will be from the date of purchase of the hardware. For example, if you purchase a 4 Year OS360 in Dec 2023 for devices purchased in March 2022, the 4-

year S360 warranty period will start from March 2022. Elo recommends OS360 be purchased at the time of device purchase to ensure the devices are well protected from any severe vulnerabilities.

27. How am I notified that a security update is available?

Elo want these updates to be applied to the devices at the earliest so we will make every effort to make it available with minimal turnaround time. Notifications for the new updates will be made available through EloView portal and newsletters.

28. How can I see the status of my OS360 subscription?

Your OS360 subscription for any given device will be shown on the device as well as on the EloView cloud portal. The Elo Diagnostics tab within the Elo Home App and the Android settings will show this information for all Elo Android 10+ devices. This can also be viewed under the software tab on your EloView cloud portal account in which the device is registered. Active devices will show the active status and the OS360 expiration date. Devices without OS360 will show the status as expired. The update to show the status will be rolled out by end of March.