DATALOGIC SHIELD FAQ

September 19, 2024

This FAQ provides essential information about Datalogic Shield, including update processes, device support timelines, and security measures. It's designed to help you understand how we maintain the security and longevity of your devices.

General Information

Question 1:
Q: What products are currently covered by Shield?

A: Shield is available on the following Datalogic Products:

- Memor 11 Family
- Memor 10
- Skorpio X5
- Memor 30/35 Family
- Joya Touch A6
- Joya Touch 22
- Memor 20

Question 2:
Q: How do I buy Datalogic Shield?

A: Datalogic Shield is included as part of our mobile device maintenance plans (Ease of Care) or by purchasing a separate software-only Datalogic Shield contract.

Question 3:
Q: When should Shield be purchased?

A: Shield should be purchased together with the mobile computer hardware from the beginning. Datalogic may consider a late purchase of Shield depending on the specific case. However, customers should not wait to buy Shield only when they need a Shield update, as there may be an added cost.

Question 4:
Q: Why should a customer buy Datalogic Shield?

A: The following three points summarize the main reasons why a customer should buy shield.

Proactive Cybersecurity: In today's digital landscape, cybersecurity threats are constantly evolving. Datalogic Shield ensures your devices are always protected with the updated security patches, addressing vulnerabilities identified by Google.

DATALOGIC SHIELD FAQ

Continuous Innovation: Shield is more than just security; it's about keeping your devices at the forefront of technology. Firmware updates include performance enhancements, new features, and upgrades to Datalogic Mobility Suite tools, ensuring your devices are always operating at peak efficiency.

Futureproofing with Major Upgrades: Shield includes major Android upgrades that bring significant new features and improvements. This keeps your devices compatible with the latest applications and services, ensuring they remain valuable assets to your operations.

Question 5:
Q: Are there reasons why a customer might choose not to buy Shield?

A: If a customer's use case involves devices that do not require regular updates, major Android version upgrades, or the latest features, they may choose not to purchase Shield. However, this comes with the risk of leaving devices vulnerable to cybersecurity threats and missing out on the continuous improvements that enhance device performance and longevity.

Question 6:
Q: What if a customer doesn't have Shield and wants to upgrade to a new Android major version when made available by Datalogic ("Dessert Upgrade")?

A: Android major upgrades are part of the Shield offering. If a customer doesn't have Shield, they are not entitled to dessert upgrades (e.g. Android 11 to 13).

Datalogic Zero Latency

Question 7:
Q: What is Datalogic Zero Latency?

A: Datalogic Zero Latency represents the pinnacle of security support in the Android market. It's an enhanced level of service of the Shield program that guarantees the immediate integration of Google's monthly security patches with zero delay in terms of months. This means that as soon as Google releases a security patch, Datalogic ensures it is integrated into your devices before that Google provides the security update for the next month. Most of the times this means Datalogic can provide last security patches within 1 Month from the Google Date of publication.

This potentially guarantee Monthly FW Updates available, up to 12 per year.

Question 8:
Q: How does Datalogic Zero Latency work?

A: Upon the release of a new security patch in the Android Security Bulletin by Google, Datalogic immediately integrates this patch into the firmware of supported devices. This seamless process ensures that security updates reach your devices as quickly as possible, minimizing any potential

exposure to cybersecurity threats. With Datalogic Zero Latency, you receive the latest security patches with zero months of delay from the date of publication from Google.

Question 9:
Q: When is Datalogic Zero Latency available?

A: Datalogic Zero Latency is available on the latest OS update provided by Datalogic for your device during the period while the operating system is still supported by Google and by the chipset vendors consistently with the version of all specific SW Components running on the device.

Once Google and chipset vendors end support for that OS version or for the specific SW Components used in the Datalogic devices, the availability of high-frequency updates such as those provided by Zero Latency ceases.

This is because applying new security patches to older systems can be less reliable, and the benefits of backported patches are often outweighed by the risk of unexpected behavior from unsupported SW Components. However, we will continue to monitor for relevant vulnerabilities and apply backported patches when they provide clear benefits without compromising device stability, and compatible with software architecture of the target Operative System version.

Question 10
Q: What are the benefits of Datalogic Zero Latency?

A: The following benefits are identified.
Instant Security Protection: Zero Latency ensures your devices receive the latest security patches immediately, eliminating delays and reducing the risk of exposure to vulnerabilities. This immediate protection keeps your devices secure against emerging threats.

Minimized Disruption: By applying security updates as soon as they are available, Zero Latency reduces the potential for security-related downtime. This helps maintain continuous operations, allowing your business to run smoothly without unexpected interruptions.

Peace of Mind: With Zero Latency, you can trust that your devices are always up-to-date with the latest security measures. This provides confidence that your systems are protected, allowing you to focus on your core business activities without worrying about security gaps.

Question 11
Q: Can you provide an example of how Datalogic Zero Latency benefits organizations?

A: Imagine a critical vulnerability is identified that could potentially compromise millions of devices worldwide. While other solutions may take weeks or months to deliver a patch, Datalogic Zero Latency ensures that your devices are patched immediately within the same month the

vulnerability is identified. This rapid response prevents exploitation and protects your organization from risks such as data breaches, financial loss, and reputational damage.

Question 12
Q: Which devices support Datalogic Zero Latency?

A: Datalogic Zero Latency is available on the Datalogic device:

- Memor 11 Family
- Skorpio X5 – all SKUs
- Memor 30/35 Family.

Datalogic Zero Latency is automatically included in all current and new Shield contracts, ensuring that your devices are always at the forefront of security.

Support Statuses

Question 13
Q: What are the different support statuses under Datalogic Shield?

A: The description of the different support status can be full found here, and are following reported:

Active: Regular software updates, including security patches and bug fixes, are made available to ensure devices remain secure, up-to-date, and fully functional.

Active – Variable Frequency: Software updates continue, but the frequency may vary due to changes in support from Datalogic's partners. Datalogic carefully assesses each identified vulnerability to determine if it can be patched, prioritizing security and system stability.

Transition: When a newer OS version is released, the previous version moves to "Transition" status. Updates are still provided, but upgrading to the latest OS version is strongly recommended to continue receiving full support and protection.

Transition – Variable Frequency: Similar to "Transition," but with variable update frequency due to limited support.

Expired: Devices in this status no longer receive new updates, but existing software and security patches remain available for download.

Question 14:
Q: Where is possible to check the current support status of my Device?

A: On the download page of your device you can find a table on top reporting for each operative system released what is the current support status.

Question 15
Q: How does Datalogic decide on the frequency of updates for devices under "Active – Variable Frequency" or "Transition – Variable Frequency"?

A: Datalogic prioritizes your security by maintaining updates as long as possible. When support from partners diminishes such as Google or the chipset platform vendor, we adjust the frequency but continue to assess and address critical vulnerabilities on a case-by-case basis.

Question 16
Q: What happens during the "Transition" period for an OS version?

A: During the "Transition" period, Datalogic continues to provide updates for the previous OS version while recommending an upgrade to the newer version. This ensures your devices remain secure and compatible with the latest software, offering you a clear path forward in your technological journey. The duration of the Transition period is of 1 Year.

Question 17
Q: What does "Expired" support status mean?

A: “Expired" status means no new updates will be provided, but existing updates remain available for download. This status signifies the end of active support, and customers should consider upgrading to maintain security and performance.

Backporting

Question 18
Q: What is backporting, and how does it work?

A: Backporting is a process where Datalogic adapts security patches or updates originally developed for newer versions of the Android OS to work with older versions not supported anymore by Google or the chipset vendor. This ensures that even older devices continue to receive relevant security updates, reflecting Datalogic’s commitment to extending the life and security of your investments.

Question 19
Q: How does Datalogic decide whether to backport a security patch?

A: Datalogic assesses each vulnerability reported in the Android Security Bulletin. If a vulnerability is critical and backporting is feasible, Datalogic ensures that the patch is adapted for older OS versions, maintaining a high standard of security and quality across all supported devices.

Question 20
Q: Are all security patches eligible for backporting?

A: Not all patches can be backported due to technical limitations or the potential risks they may introduce to system stability.

CVEs and Security Patch Verification

Question 21
Q: What is a CVE, and how does it work?

A: A CVE (Common Vulnerabilities and Exposures) is a standardized identifier assigned to known security vulnerabilities. Once a CVE is identified, it's published in the Android Security Bulletin (ASB), detailing the vulnerability, its severity, and the necessary patch to resolve it. Datalogic uses the ASB in two stages: first, as a guide to apply the latest security patches on supported and active operating systems, and second, to assess which CVEs can be backported when official support ends.

Question 22
Q: How does Google handle CVEs, and how are they fixed?

A: Google identifies vulnerabilities and assigns them CVEs, which are then detailed in the Android Security Bulletin. Google develops patches to address these vulnerabilities and provides them to manufacturers like Datalogic. With Datalogic Zero Latency, these patches are immediately integrated into your devices, ensuring that your organization is always protected with the latest security measures.

Question 23
Q: How does Datalogic verify security patches before deployment?

A: Every firmware update made available to customers undergoes rigorous testing to ensure compatibility, performance, and security integrity. This comprehensive verification process includes leveraging third-party laboratories approved by Google to validate the security and functionality of the updates.

Incremental OTA Updates

Question 24
Q: What are Incremental OTA Updates, and how do they work?

A: Incremental Over-the-Air (OTA) updates are designed to deliver targeted fixes and improvements more efficiently. Instead of requiring a full system update, incremental OTA updates only include the most recent changes since the last update, resulting in faster downloads and installations. This method ensures a faster deployment and distribution of the FW Updates.

Question 25
Q: What are the benefits of Incremental OTA Updates for customers?

A: Incremental OTA updates are smaller, allowing for quicker download and installation, minimizing downtime and keeping your operations running smoothly.
These updates are less resource-intensive, making them ideal for environments where bandwidth and processing power are limited.

Question 26
Q:How are Incremental OTA Updates verified before deployment?

A: Just like full firmware updates, Incremental OTA updates undergo a thorough testing process at Datalogic. We ensure each update is compatible, effective, and secure, maintaining the highest standards of performance and reliability. Our rigorous verification process guarantees that these updates enhance your devices without compromising their stability.

Question 27.
Q: Can customers choose between Incremental OTA Updates and full firmware updates?

A: Yes, customers can choose between Incremental OTA updates and full firmware updates. Incremental OTA updates are available for customers who have kept their devices up-to-date with each OS release. However, full OTA updates are required when performing a major OS upgrade (e.g., from Android 11 to Android 13) or when updating between non-consecutive firmware versions.

Longevity

Question 28
Q: How long are Datalogic devices supported?

A: Datalogic devices are supported throughout the entire lifecycle of the product, and for at least two years after the product reaches its End of Life (EoL).
Depending on the platform's longevity, the support period can be even longer. During this time, Datalogic continues to provide OS updates, security patches, and performance enhancements.

Question 29:
Q: How many Android major versions are planned for Datalogic devices?

A: Typically, Datalogic plans to support two major Android versions for each device. However, this can vary depending on the specific platform, and in some cases, it could be extended to three or more major versions. The exact number of supported versions depends on the hardware capabilities and the longevity of the platform.

Question 30:
Q: How are Android major versions planned for Datalogic devices?

A: Datalogic plans Android major version updates with the goal of providing continuous and extended security support. We align these updates with Google's security support timeline to ensure that your devices remain secure and up-to-date for as long as possible. By carefully planning these updates, we aim to maximize the longevity and security of your devices.