TeamTablet™ 55 / Flex

Device security

Overview

TeamTablet™ 55/Flex is based on the Android OS operating system that has been customized to prioritize security. Your data and privacy is safeguarded, providing you with peace of mind, through **regular security updates**, **kiosk mode** to restrict access control, and **prevention of unauthorized third-party applications**. We employ multiple layers of **encryption**, both on device and through the cloud. The TeamTablet™ 55/Flex are not typical Android devices but are **purpose-built appliances** optimized for collaboration and their respective use cases. We employ a multi-layered security approach, incorporating cutting-edge technologies and best practices to shield your device from emerging threats.

Android OS

Security updates and upgrade path

Our product seamlessly integrates a **custom Android 11 operating system**, ensuring your device remains secure and up to date with the latest security patches and features.
To maintain the device's security and compatibility, we will continue to provide regular **security updates for** Android 11 for as long as the revision is supported by Google.
We also have a planned upgrade path to **Android 13**, which is due 2024. The upgrade will be provided as an **OTA (Over-the-Air) update**, allowing you to seamlessly transition to the latest Android version without any disruptions or hassle. Updates can be applied automatically or initiated manually by an administrator.

Device lockdown

To ensure the security and controlled usage of our devices, a security measure known as **Android Kiosk mode** is employed. This mode restricts the device to running only authorized applications, effectively preventing unauthorized access or modifications. Kiosk mode blocks access to the device's default launcher, the graphical interface that facilitates app launching and general device navigation. This restriction serves to safeguard the device and ensure that only the specified approved applications can be used. By confining the device's functionality to pre-approved FlatFrog applications, control can be maintained over the device's usage and protect sensitive data.

Additionally, **Android Debug Bridge (ADB)** is intentionally disabled on all FlatFrog devices running release software to prevent unauthorized access and alterations to the device's configuration or data. This security measure helps safeguard devices from potential security threats and ensures that only approved applications can be installed or executed.

Android's built-in security features, particularly **SELinux** (Security-Enhanced Linux) and **Permissive Mode**, offer a robust defense against malicious attacks and data breaches. Permissive Mode's logging capabilities provide valuable insights into potential security flaws, while SELinux's strict access controls prevent unauthorized actions from exploiting those flaws.
By effectively leveraging Permissive Mode and SELinux, the device can be safeguarded from a wide range of threats, including malware, phishing attempts, and unauthorized access to sensitive data.

Third Party Applications

By design, FlatFrog devices do **not** come pre-installed with the *Google Play Store, Amazon App Store, or Google Play Services*. This deliberate exclusion prevents the installation of third-party applications from these platforms, thereby enhancing device security and preventing unauthorized software from being introduced.

App Security

To guarantee the authenticity and integrity of the software running on our devices, all applications developed by FlatFrog are **cryptographically signed** using Google's built-in, industry standard tools. This process involves embedding digital signatures into the software's code, allowing the device's operating system to verify the software's origin and ensure its integrity. By validating the digital signatures, the device can confirm that the software is genuinely from FlatFrog, preventing the execution of unauthorized or malicious code. This approach helps safeguard devices from malware attacks and ensures that only trusted applications are allowed to run.

Device Encryption

We **encrypt** all data on the device's storage, rendering it unreadable without the correct decryption key. This encryption provides an extra layer of protection in the event of device loss or theft, safeguarding your personal information even if your device falls into the wrong hands. However, note that board and user-generated data stored on the cloud service is not stored locally on the device.

Network Security

Wireless screensharing

Our screensharing solutions work on a direct connection between devices, following the Miracast and AirPlay protocols, without the need of external networking. This means that **screensharing works even with an air-gapped device.** Additionally, an **infrastructure mode** for connecting through an access point or switch is available for Miracast. The infrastructure behind it is based on 802.1X with standard network protocols.

Guest access is available and configurable to fit your safety requirements.

Cloud connectivity

Our cloud services require connection to the Internet for access to remote board content and device updates. The wireless interface of our devices is inherently safeguarded by **WPA2-PSK**, an authentication protocol that secures Wi-Fi networks using a Pre-Shared Key (PSK). WPA2-PSK encryption safeguards the privacy and integrity of all data transmitted across the wireless channel. This can be configured on the device or through an **administrator interface.** Wired Ethernet connection is also available on the TeamTablet™ Flex to ensure optimum performance.

FlatFrog devices utilize **encrypted communications** and endpoint authentication for secure internet connectivity for all data sent to our GCP (Google Cloud Platform) services. TLS 1.2+ is the preferred encryption protocol.

Physical anti-theft lock

An industry-standard on-device **anti-theft lock** provides a layer of security for your device, acting as a physical barrier to deter theft. By securing your device, these locks help prevent unauthorized access to sensitive data stored on the device, contributing to a safer and more secure work environment.

Commitment to User Trust

We prioritize user trust by being transparent about our security practices, clearly communicating our security policies and procedures. We also actively engage with our users to gather feedback and address any security concerns promptly.