Panasonic ideas for life



Toughpad A1

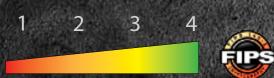
EMBEDDED HARDWARE SECURITY

Marvell [®] Processor	
Application	Security
Core	Core
Processors	Processor

The processor in the Toughpad A1 tablet has a unique and dedicated security core to handle encryption for the most sensitive data. Since the security core is separate from the application cores, encryption is more efficient, and the encrypted data is at less risk and more secured.

FIPS 140-2 ENCRYPTION*

The Toughpad A1 is the only Android tablet using a FIPS 140-2 Level 2/3 compliant processor. The Marvell[®] encryption module is compliant with NIST approved algorithms for hardware encryption in government use.



FIPS Secure Level

* Marvell® will submit to NIST for Level 2/3 compliance verification.

LOCK-SLOT SECURITY

A steel reinforced slot for a cable lock helps keep the tablet protected and prevents sensitive data from getting in the wrong hands.



Cable lock slot

WHAT MAKES THE PANASONIC TOUGHPAD A1 THE MOST SECURE ANDROID[™]-POWERED TABLET? The Panasonic Toughpad[™] A1 tablet is designed and constructed with

The Panasonic Toughpad ^m AT tablet is designed and constructed with the mission-critical mobile user in mind to offer secure connectivity that's ideal for highly mobile workers and the security conscious. That's why every Toughpad A1 user can rest assured that their company data remains safeguarded with enterprise-grade security that won't be found in any other AndroidTM-powered tablet.

1.800.662.3537 / panasonic.com/toughpad

TRUSTED BOOT

The Trusted Boot feature verifies the unique signature of digitally signed operating system load, prior to booting the system. If tampering is detected, the boot process halts, preventing any unauthorized access to data. For added protection, it keeps fraudulent OS versions from circumventing the data encryption and software security features of the tablet.

Virus Checker Data Encryption Trusted Boot (Prior to OS boot)

SOFTWARE SECURITY

The Toughpad A1 tablet supports all major software security vendor applications for data management, VPN end point security, messaging and web access. Also, the latest version of Android 4.0 supports RSA 2 factor authentication.

MOBILE DEVICE MANAGEMENT

MDM software allows for low-level device control over tablets, like the Toughpad A1, to manage and secure one or many devices in the field. MDM solution providers give IT administrators enterprise-class support of functions like:

Asset Tracking

Device Monitoring

Hundreds more

- Application Management
- Security Policies Management
- Remote Device Lock / Wipe
- THEFT DETERRENT DOCKING

The docking station from Havis Inc. protects the tablet with a convenient lock and key system to keep the tablet securely mounted and charged in a number of workplaces.

TOUGHPAD

Panasonic is constantly enhancing product specifications and accessories. Specifications subject to change without notice. Trademarks are property of their respective owners. ©2012 Panasonic Corporation of North America. All rights reserved. Android is a trademark of Google Inc. The Android robot is reproduced or modified from work created and shared by <u>Google and used according to terms described in the Creative Commons 3.0 Attribution License. S. Security_03/12</u>