



TOUGHBOOK GUARD: SECURITY WHERE IT MATTERS MOST

Built-In Protection That Starts Below the OS

When device integrity is mission-critical, TOUGHBOOK Guard delivers protection no one else can. It's a unique solution with embedded firmware security specifically designed to detect hardware tampering after deployment—before threats can take hold. Operating below the OS, TOUGHBOOK Guard protects TOUGHBOOK® devices against supply chain attacks, rogue hardware, and tampering attempts that traditional endpoint solutions miss.

Whether you're in federal, state, or local government, public safety, or critical infrastructure, your devices are only as secure as the hardware inside them. TOUGHBOOK Guard ensures they stay trusted from day one to end-of-life.

Built for Mission-Critical Environments

TOUGHBOOK Guard is embedded directly into the BIOS firmware of TOUGHBOOK devices. It continuously monitors key hardware interfaces (such as USB ports, SSD, RAM, cameras, wireless cards, and configuration options) for unauthorized changes, ensuring your configuration stays locked and secure.

Key Security Functions:

- **Pre-Boot Validation:** Detects hardware changes before startup
- **Offline Operation:** Works in air-gapped and disconnected environments
- **No OS Dependency:** Immune to OS-level attacks
- **Custom Hardware Profiles:** Lock in your agency-approved configurations
- **Real-Time Alerts:** Notifies end user of any tampering or rogue components

Once enabled, TOUGHBOOK Guard operates silently in the background with no impact on performance or end-user experience, keeping your systems protected and productivity uninterrupted.

Trusted Hardware, From Factory to Field

Government-issued technology must remain secure throughout its entire lifecycle—including manufacturing, transit, deployment, and service. TOUGHBOOK Guard protects against threats at every step.

- ✓ Ensures supply chain integrity
- ✓ Detects unauthorized component swaps
- ✓ Confirms firmware remains untampered
- ✓ Simplifies compliance with government mandates

Purpose-Built for Government Compliance

TOUGHBOOK Guard is engineered to align with major cybersecurity mandates, facilitating your agency to stay ahead of evolving requirements. Here are some of the government mandates:

| Mandate | How TOUGHBOOK Guard Helps |
|---------------------------|--|
| CJIS Security Policy v6.0 | Detects and reports firmware and hardware tampering; locks down the device |
| FISMA & EO 14028 | Verifies hardware trust anchors for zero-trust architectures |
| NDAA §889 & FASCSA | Blocks unauthorized or unapproved hardware |
| NIST SP 800-161 | Supports supply chain risk management protocols |

Available on new TOUGHBOOK models starting Fall 2025.



CJIS Deadline: September 30, 2027

Agencies must validate firmware integrity and monitor hardware changes. TOUGHBOOK Guard is ready now to meet those expectations.

Why Choose TOUGHBOOK Guard?

First-of-Its-Kind Firmware Protection

First rugged solution with embedded firmware security to detect post-deployment hardware tampering.

Zero-Trust Ready

Supports zero-trust architectures by verifying hardware before it ever touches your network.

No Recurring Fees

One lifetime license per device. Activate at the factory or in the field.

Secure Your Devices from the Inside Out

Don't leave your hardware exposed. TOUGHBOOK Guard delivers embedded protection that detects threats others miss, locks down your devices, and helps you meet today's toughest compliance standards—before the deadline hits.

Cyber Threats & Risks

1. RAM MEMORY

Prevent data theft or malware introduction via unapproved RAM modules.

2. STORAGE DRIVE

Block unauthorized external storage devices that could enable data exfiltration.

3. WIRELESS NETWORK ADAPTERS

Stop rogue Wi-Fi adapters from establishing unauthorized network connections.

4. BLUETOOTH

Prevent unauthorized Bluetooth connections that may pose security risks.

5. USB PORTS

Detect and alert on unauthorized USB device access.

6. LCD SCREEN

Prevent counterfeit LCD from capturing on-screen data.

7. WEBCAMS

Disable unauthorized webcams that may compromise privacy and security.

8. EXPANSION PACK MODULE (XPAK)

Prevent unapproved or counterfeit xPAK modules from introducing vulnerabilities.

9. SMART CARD READERS

Prevent unauthorized readers & TPM modules from gaining access.

10. OTHER DEVICES

Block unapproved accessories such as USBs, barcode scanners, LAN ports, GPS units, or fingerprint readers.

To learn more, visit www.mruggedmobile.com or call 877-870-3806