KC DIGITAL SOLUTIONS
COPIERS · PRINTERS · DOCUMENT MANAGEMENT

DEVICE SECURITY BRIEF
KYOCERA MZ SERIES

A MANAGED PRINT PROPOSAL FOR

Security Built In, Not Bolted On.

Why your Kyocera MZ Series device is protected by design — no add-on antivirus required.

Some office devices depend on **signature-based antivirus** — software that scans for threats it already recognizes and must be constantly updated to stay current. Your Kyocera MZ Series takes a fundamentally different, more resilient approach: it is a purpose-built, locked-down device that **only ever runs verified Kyocera code**. Instead of detecting bad software after it arrives, the device prevents any unauthorized software from executing in the first place — closing the door on both known and never-before-seen threats.

Protection Engineered Into Every Device

Secure Boot & TPM
A Trusted Platform Module verifies firmware integrity at every startup. Tampered or unauthorized firmware simply won't run.

K-Level Security Standard
Kyocera's highest firmware security level, configured out of the box with user data encrypted by default — no manual setup to get wrong.

Authentication & Access Control
User login and role-based permissions ensure only authorized people operate the device and reach its data.

Digitally Signed Firmware
Only Kyocera-authenticated firmware loads, so malware cannot be injected through the update process.

Network Hardening
IP/port filtering, protocol control, SSL/TLS encryption and 802.1X — unused services can be switched off to shrink the attack surface.

Audit Logging
Device activity is tracked and traceable, supporting accountability and compliance reporting.

Independently validated. Kyocera TASKalfa devices have passed Keypoint Intelligence (BLI) Security Validation Testing — third-party assessment including automated attacks and white-hat penetration testing of the firmware and operating system. Security you can verify, not just take on faith.

Add the Data Security Kit — Protect the Data at Rest

The platform protects the device and the network. The Data Security Kit protects the information stored on the drive — where every scan, copy, print and fax job can briefly reside.

- ✓ **AES Encryption (128/256-bit)** — data is encrypted before it's written to the drive, so a pulled or stolen drive is unreadable.
- ✓ **Common Criteria Certified** — ISO/IEC 15408 & IEEE 2600.1 at Evaluation Assurance Level 3, recognized for compliance-driven environments.
- ✓ **DoD Overwrite & Sanitization** — latent image data is overwritten (3-pass method), critical at lease-end when the device leaves your building.
- ✓ **Remotely Deployable** — rolled out and managed via Kyocera Fleet Services, with no added burden on your IT team.

The bottom line: *a Kyocera MZ Series device isn't secured by chasing the latest virus — it's secured by an architecture that won't run anything it can't verify. That's prevention by design, backed by independent testing and, with the Data Security Kit, certified protection for your most sensitive data.*

Let's secure your fleet.

KC Digital Solutions • Fullerton & San Diego, CA • Serving LA, Orange County & San Diego

Corporate 800-448-0076
Web kcdigsol.com