

USE CASE: KSI-2100 HRPB-23

A Zero Trust Endpoint Strategy for Ransomware Protection

Stopping Credential Theft Before It Becomes Ransomware

Ransomware is no longer a malware problem — it's an identity problem. Modern attackers do not hack in; they log in using compromised credentials harvested through phishing, keylogging, or session hijacking.

To stop the progression from a single stolen password to a network-wide ransomware encryption event, organizations must move beyond the traditional login. The KSI-2100 Series keyboard serves as the critical hardware anchor for this transition, consolidating phishing-resistant MFA, biometric verification, and automated session security into a single desktop footprint.

The Challenge: The "First Mile" Vulnerability

Standard enterprise security often ignores the physical point of entry: the keyboard. In most environments, the "First Mile" of access is plagued by:

- **Shared and Weak Passwords:** High-pressure environments (such as healthcare and finance) often lead to password sharing or simple, guessable credentials.
- **The Walk-Away Gap:** Even with strong MFA at login, a workstation left authenticated but unattended is a prime target for insider attacks or lateral movement by remote actors.
- **Credential Harvesting:** Software-based keyloggers and sophisticated AITM (Adversary-in-the-Middle) phishing sites easily intercept typed credentials and even standard 6-digit TOTP codes.
- **The "MFA Fatigue" Factor:** Users frustrated by fumbling for dongles or phones often find ways to bypass security controls, creating risk that may result in a ransomware attack.

The Risk: From Compromise to Catastrophe

When an attacker gains legitimate access through a typed credential, they bypass the majority of the security stack. This leads to:

- **Stealthy Persistence:** Attackers can dwell for weeks, mapping the network while appearing as a "productive employee."
- **Lateral Movement:** Using valid (but stolen) identities to move from a standard workstation to high-value servers.
- **Privilege Escalation:** Exploiting the lack of continuous authentication to gain administrative rights.
- **Ransomware Execution:** By the time a malware payload is deployed, identity-based defenses have long since failed.



The Solution: The KSI-2100 Series Keyboard

The KSI-2100 Series keyboard disrupts the ransomware "kill chain" by replacing vulnerable, software-only workflows with hardware-backed, phishing-resistant identity controls.

Integrated Security Key Ports

The KSI-2100 Series keyboard features dedicated USB-A and USB-C ports located directly on the keyboard face that support protection against phishing.

- **No-Fumble MFA:** Users no longer need to reach behind a CPU or use unstable hubs. The keyboard is the hub. This convenience encourages the consistent use of FIDO2/WebAuthn security keys.
- **Hardware-Bound Identity:** By utilizing the keyboard as the hub for security keys, the credential is bound to a physical token that cannot be duplicated or intercepted by remote attackers.



Contactless NFC Reader

Integrated NFC technology allows for easy “tap-and-go” authentication.

- **Workflow Efficiency:** Ideal for clinical or high-traffic environments where users must authenticate multiple times a day.
- **Multi-Factor Flexibility:** Supports HID® Prox, iCLASS®, and other industry-standard badges, allowing organizations to leverage existing physical access cards for logical computer access.

KSI PresenceLock™

Patent-pending PresenceLock™ is an active session guardian — an integrated keyboard sensor that monitors human presence at the workstation.

- **Automated Walk-Away Security:** When a user leaves their desk, the sensor detects the absence within seconds and triggers a workstation lock.
- **Continuous Validation:** PresenceLock solves the “unattended terminal” problem without software. Security is enforced by the hardware itself, ensuring that a valid session is only active when a valid user is present.

Biometric Smart Card Integration

For organizations requiring an even higher level of assurance, the KSI-2100 series supports biometric smart cards through its integrated NFC and security key interfaces. This enables robust 3FA workflows without the privacy risks of a centralized biometric database:

- **Something You Have:** The physical biometric smart card or security key.
- **Something You Are:** The fingerprint scan performed locally on the card to unlock the credential.
- **Something You Know:** A PIN to authorize the final secure handshake with the workstation.



Outcome

By deploying the KSI-2100 series, organizations realize a hardened defense posture and four immediate security outcomes:

- **Eradication of Phishing:** Even if a user is tricked into revealing a PIN, the attacker cannot access the system without the physical hardware key or badge tap on the KSI keyboard.
- **Closed Walk-Away Vulnerabilities:** PresenceLock™ ensures that the "open door" of an unattended PC is eliminated, enhancing adherence to compliance requirements (HIPAA, CJIS, GDPR).
- **Reduced IT Friction:** By making the "secure way" the "easy way" (via integrated ports and NFC), user compliance increases, and the likelihood of security bypasses decreases.
- **Disrupted Ransomware Kill-Chain:** Without the ability to harvest credentials or exploit abandoned sessions, attackers lose their primary vectors for lateral movement.

Ultimately, the KSI-2100 Series transforms the desktop into a Zero Trust endpoint, one that is continually verified through hardware-backed identity.

FEATURE	BENEFIT
Integrated Security Key Ports	Top-facing USB-A and USB-C ports for accommodation of FIDO®-compliant security keys, including YubiKey®, HID Crescendo®, FEITIAN, Hirsch, Thales, Swissbit®, Idemia
NFC Reader	Secure logon with integrated dual frequency HID OMNIKEY 5127CK Mini reader module
PresenceLock™	Human presence detection sensor facilitates walk-away logoff without manual tap-out
Biometric Support	Facilitates 3FA via NFC or USB, using Match-on-Card biometrics to maximize privacy
Mobile Access	Works with mobile credentials in Apple Wallet and Google Wallet
OS Support	Compatible with Windows, macOS, Linux, ChromeOS, IGEL, Window Hello

Summary

The KSI-2100 series is not just a peripheral — it's a ***security endpoint hub*** that can help stop credential theft before it becomes ransomware. It moves the perimeter from the network edge to the fingertips of the user, ensuring that every session is authenticated, every credential is phishing-resistant, and every workstation is safeguarded, even when the user walks away.

ksikeyboards.com
info@ksikeyboards.com
14494 Wicks Blvd.
San Leandro, CA 94577
510.562.5000