Cyber Security Report

True End-to-End Encryption begins at the keystroke

Protecting Businesses and their Customers from Cyber Threats

February 2025

EndpointLock™
Desktop and Mobile Security

February 2025

True End-to-End Encryption Begins at the Keystroke

Protecting Businesses and Their Customers from Cyber Threats

In today's digital world, cybercriminals are constantly finding new ways to steal personal and financial information. Whether you're a business protecting customer data or an individual safeguarding your private information, **end-to-end encryption (E2EE) is essential.** But to be truly effective, encryption must begin at the keystroke level.

Why Traditional Security Measures Aren't Enough

Most cybersecurity solutions focus on securing data once it has been stored or while it's being transmitted. While these protections are necessary, they **leave a critical gap**—the moment data is typed. Hackers can exploit this vulnerability using **keylogging malware**, which records keystrokes before they're encrypted by traditional methods.

Keyloggers are one of the most dangerous cyber threats, responsible for identity theft, financial fraud, and helping to advance ransomware attacks and corporate data breaches. Studies show that **80% of keyloggers can bypass traditional antivirus software**, and they can sneak past even the most advanced security measures, including:

✓ Firewalls
✓ Multi-factor authentication (MFA)
✓ Virtual private networks (VPNs)
✓ Endpoint detection and response (EDR)

A **real-world example** of this occurred when LastPass, a leading password manager, suffered a breach after a hacker used a keylogger to steal (ironically) a senior engineer's **Master Password**—despite multiple layers of security. This proves that **encryption must start at the keystroke level** to truly protect sensitive data.

Keystroke Encryption: The Missing Piece in Cybersecurity

Keystroke encryption is a powerful solution that **locks down data at its source—the moment it is typed.** Even if a keylogger is installed on a device, the recorded keystrokes are completely unreadable.

How Keystroke Encryption Protects Businesses & Consumers

🔷 **Stops Keyloggers Cold** – Even if malware is present, stolen keystrokes are encrypted and useless to hackers.

🔷 **Protects Login Credentials & Payments** – Safeguards usernames, passwords, credit card numbers, and other sensitive information.

🔷 **Works Silently in the Background** – No complicated setup or maintenance; users simply install the app and stay protected.

🔷 **Enhances Consumer Confidence** – Businesses that offer keystroke encryption show customers they prioritize data security, leading to greater trust and loyalty.

Bringing Enterprise-Level Security to Everyday Users

At **Advanced Cyber Security**, we believe everyone deserves enterprise-grade protection. That's why we developed **EndpointLock™**, powered by our proprietary **Keystroke Transport Layer Security (KTLS™) Protocol**.

Why Businesses Choose EndpointLock™

✅ **Protects business endpoints and customers** from financial fraud, identity theft, and stolen login credentials.
✅ **Easy to implement**—ideal for banks, healthcare providers, e-commerce sites, and any company that values customer security.
✅ **Works across devices**, securing keystrokes on both desktop and mobile.
✅ **Defends against advanced cyber threats**, including zero-day, polymorphic, and AI-generated attacks.

Take the First Step in True End-to-End Encryption

By deploying **EndpointLock™ across employee devices**, businesses can ensure that their **own data remains protected**.

Consumers trust businesses that take cybersecurity seriously. By offering **EndpointLock™ keystroke encryption**, companies can give their customers **peace of mind** while strengthening their own security posture.

Want to protect your customers and your business? Contact Advanced Cyber Security today to learn more.

Visit www.advancedcybersecurity.com to discover how keystroke encryption can transform your security strategy.