Cybersecurity News

There is no Zero-Trust if keystrokes are not protected

Expanding your cybersecurity perimeter to fortify a zero-trust environment.

EndpointLock™
Desktop and Mobile Security

September 2023

There is no zero-trust if keystrokes are not protected

In the ever-evolving landscape of cybersecurity, the Zero Trust model has emerged as a beacon of hope in the battle against digital threats. This paradigm shift recognizes that trust should never be assumed, even within an organization's own walls.

While Zero Trust principles encompass various layers of security, from behavioral analysis to network segmentation, one crucial aspect often gets overlooked: keystroke protection. A core tenet of the Zero Trust Architecture is identity verification, which EndpointLock has been designed to protect. Your identity is a key component required to successfully compromise a Zero Trust environment.

The seemingly innocuous action of keystrokes can pose a significant security risk if not adequately protected even within a Zero Trust environment. If malicious actors gain access to these keystrokes, they can potentially compromise our personal and professional lives. EndpointLock's Keystroke Encryption stands as the answer to fortifying your Zero Trust environment.

Understanding Keystroke Encryption

Keystroke Encryption is a security measure that shields your keyboard input. It ensures that the characters you type are transformed into an indecipherable format before they reach the software or website you're interacting with. Everything you type remains encrypted and inaccessible during its entire journey from the keyboard to the active text box you are typing into.

Here's why keystroke encryption should be an integral part of a robust Zero Trust strategy:

- ✓ **Protection from Keyloggers:** Keyloggers are malicious software designed to record your keystrokes without your knowledge. Keystroke encryption foils keyloggers from capturing data, preventing any attempts at unauthorized access.

- ✓ **Securing Passwords:** Passwords are the keys to our digital kingdom. Encrypting keystrokes during password entry ensures that these critical pieces of information remain secure, even if a cybercriminal attempts to intercept them using a keylogger.

- ✓ **Credential Theft Prevention:** Many cyberattacks involve stealing user credentials through methods like keyloggers, which record keystrokes without the user's knowledge. A Zero Trust model must start by protecting keystrokes and mitigate the risk of credential theft at the point of data entry.

- ✓ **Protecting Sensitive Data Entry:** Whether you're typing credit card information during an online purchase or entering confidential business data, keystroke encryption ensures that your keystrokes remain confidential, guarding against potential data leaks.

- ✓ **Strengthen Multi-Factor Authentication (MFA):** Multi-factor authentication (MFA) adds crucial security layers beyond usernames and passwords, but keyloggers can still compromise it. Keyloggers capture keystrokes during username and password entry, potentially stealing credentials even before the second authentication factor. They can also record MFA codes as they are inserted, allowing attackers to bypass MFA.

In Conclusion

Each keystroke we type reveals a piece of our identity. It's crucial to recognize that Zero Trust extends beyond access controls and network segmentation. To achieve true Zero Trust, organizations must also prioritize the protection of keystrokes. Without this essential layer of security, your identity, a key component needed when attempting to compromise even the most robust Zero Trust environments is vulnerable. In the digital age, where data is a prized asset, protecting keystrokes is not just a recommendation; it's a necessity for comprehensive zero-trust cybersecurity plan.

Utilizing EndpointLock™ Keystroke Encryption software, all keystrokes are encrypted making them invisible to keyloggers. EndpointLock's Keystroke Transport Layer Security (KTLS™) Protocol provides strong cryptography from the moment you start typing. This protects the initial transmission of usernames and passwords and subsequent keystrokes entered into any desktop or mobile device.

ILLUSTRATION BELOW DEPICTS KEYSTROKE ENCRYPTION