The Breach You Read About Tomorrow May Begin with a Stolen Password Today

Every week, another organization makes headlines after attackers gain access to systems, steal sensitive information, and expose millions of records.

What's most alarming is that many of these organizations already had firewalls, antivirus software, endpoint protection, security awareness training, and experienced IT teams in place.

So why do these breaches continue to happen?

Because despite billions spent on cybersecurity, most organizations still leave one critical point vulnerable: the moment data is entered into a device by their employees.

Every password, access credential, authentication code, customer record, financial transaction, healthcare record, and confidential document begins the same way:

Someone types it.

Traditional security solutions typically begin protecting data only **AFTER** it has been entered, processed, stored, or transmitted. This creates a security gap where keystrokes, and the sensitive information they contain, can be captured by keylogging spyware that steals everything the user types.

And with the rise of AI-powered cybercrime, attackers are not only creating more adaptive credential-stealing malware, they also now generate highly convincing phishing messages that are often indistinguishable from legitimate communications. As a result, malware has more opportunities to be downloaded, and sensitive information has more opportunities to be compromised before traditional security tools can detect and respond to the threat.

The Solution: EndpointLock Keystroke Encryption

This is where EndpointLock comes in. By encrypting keystrokes at the point of creation, EndpointLock helps organizations close a critical security gap that traditional defenses often leave exposed.

This approach aligns with NIST's (National Institute of Standards and Technology) requirement that sensitive government and healthcare data be protected at the point of creation. - *NIST SP 800-53 Rev. 5*

> *How many more breaches will it take before organizations start protecting data where NIST says protection should begin: at the point of creation?*

Organizations spend millions protecting data at rest and in transit, protecting data ***after*** it has been created. Yet true end-to-end protection should begin ***before*** data is stored, transmitted, or even visible to malware.

It should begin at the keyboard.

If protecting data at creation is important enough to be required on government systems, **isn't it time organizations adopted the same approach?**

It stands to reason that organizations protecting data at the point of creation can significantly reduce the risk of credential theft, account compromise, customer data exposure, and the costly financial, operational, and reputational consequences that often follow a breach.

The best news is that keystroke encryption doesn't require a massive security investment. For a fraction of what organizations spend on other cybersecurity tools, EndpointLock adds a critical layer of protection at the point where sensitive data is most vulnerable: the moment it is created.

Protect data before it leaves the keyboard and strengthen the security posture of your organization.

Hackers Can't Steal What They Can't See!
