typingdna
ActiveLock

Prevent unauthorized use of company computers with typing biometrics-based continuous authentication

ActiveLock - A new breed of endpoint protection

ActiveLock provides continuous authentication built on proprietary typing biometrics technology to prevent device sharing, ensuring each person in front of the computer is always the true authorized user.

ActiveLock is an on-device continuous authentication solution that protects against unauthorized users accessing sensitive or privileged information on company computers on Windows and macOS devices.

ActiveLock represents the next generation of the zero-trust security model — preventing device sharing and securing sensitive data with typing biometrics technology.

Key features

- Prevents device sharing, ensuring each person in front of the computer is the true authorized user.
- Leverages the power of typing biometrics-based proprietary technology to analyze users' typing behavior in real-time.
- Protects from intruder risks without impacting the employee experience, working silently in the background.
- Real-time mitigation actions at the endpoint such as system lock or silent alerts.
- Works with third-party endpoint security providers or can be used as a standalone solution.

Real-time protection against fraudulent device sharing

As the employees' environment continues to shift to a remote setting, insider threats and account takeover pose a new challenge for organizations as fraud, monetary gains, and IP theft are the three most underlying reasons behind it. Insider threats, malicious and negligent, have seen a year-over-year increase of more than 50%, costing businesses an average of **$13.3 million dollars** per incident in 2021. TypingDNA's patent-pending solution provides real-time protection against malicious actors while offering a seamless user experience based on non-intrusive typing behavior analysis.

ActiveLock offers a new breed of endpoint protection for organizations operating in BPO, financial services, government, and customer services where sensitive customer data and company IP must be protected with the latest security standards.

Use Cases

Fraud deriving from shared devices

Specific industries such as government, BPO, or customer service fall under strict regulatory compliance standards. Companies must ensure that only authorized users have access to confidential data. If contractors or employees try to share company devices with unauthorized users, ActiveLock will keep client and company data safe, blocking access to sensitive information.

Protecting unattended or unlocked computers

Special precautions should be taken when leaving devices unattended in work-from-anywhere environments. If a user steps away from their workstation without logging out or an unauthorized person tries to use it, ActiveLock continuous authentication will automatically lock the device.

Unintentional security breaches

When working from home, the lines between personal and professional activities can get blurry. Sharing a work device with family members may seem innocent. But simple ignorance can cause real harm, especially if the company's security policies are unknown to the user with whom the device is being shared.

To protect against human error, which is the main cause of **95% of cyber security breaches**, ActiveLock prevents unauthorized use of company computers, even when there is no malicious intent.

Benefits

Continuous authentication that's always on

Seamless, unobtrusive continuous authentication for employees working from anywhere.

No additional hardware equipment required

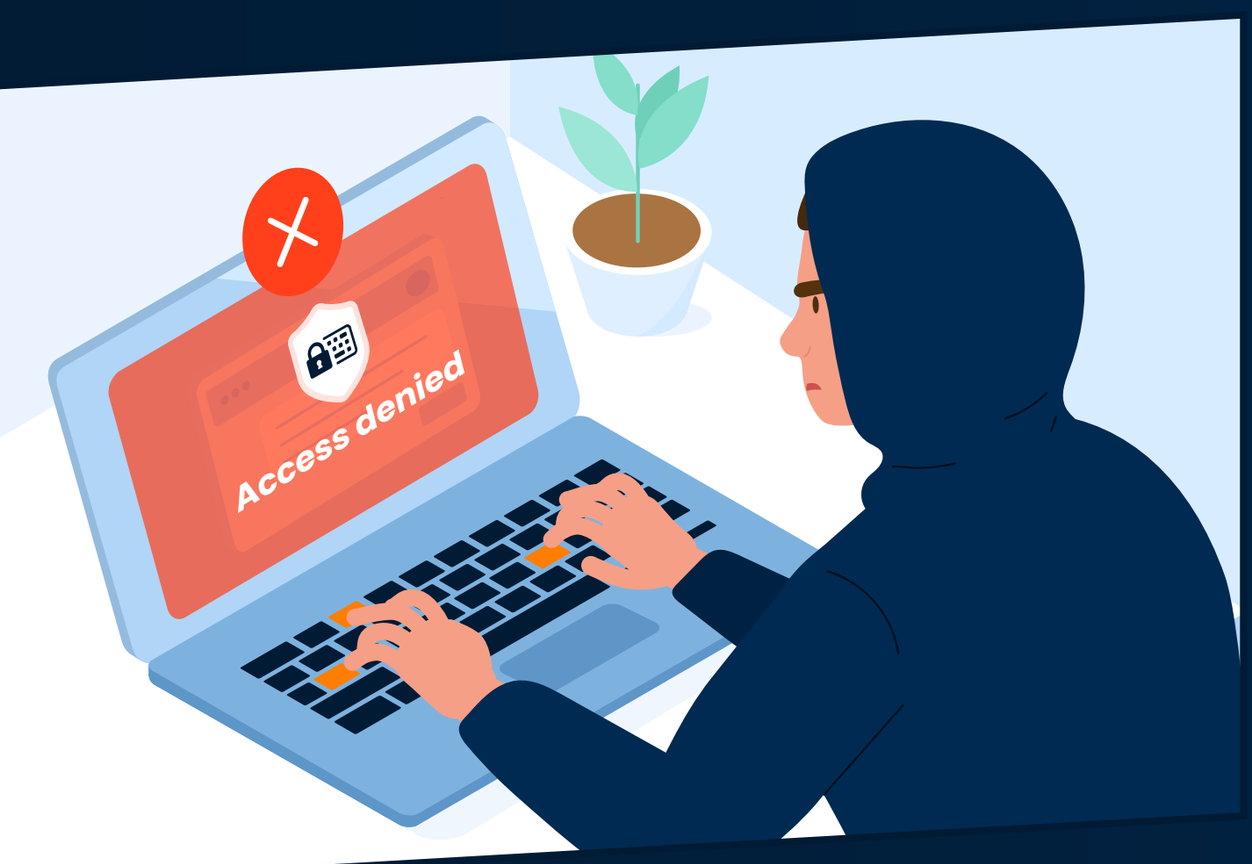
Plug and play solution that works on the device and protects both Windows and macOS devices while requiring no additional hardware.

Helps maintain high industry-specific compliance standards

Make sure only authorized users have access to company equipment so your company can respond to industry-specific compliance requirements such as ISO's or SOC.

Reduce risk without impacting the employee experience

The typing biometrics-based authentication solution works silently in the background for improved employee productivity.



How it Works

ActiveLock continuous authentication ensures that each person in front of the computer is the authorized user and is designed to prevent threats that arise with remote work, such as fraud, device sharing, and unattended devices. ActiveLock constantly verifies user identities by the way they type on their keyboard. If an unauthorized typing pattern is detected, the solution will send a silent alert or instantly lock the company desktop or laptop to protect your sensitive data.

The AI-based technology runs in the background and analyzes typing patterns right on the device, so your employee's typing data is kept private and never leaves the computers or gets stored in the cloud.

A privacy-first solution

ActiveLock is privacy-focused and only analyzes HOW users type, not WHAT they type, providing strong authentication security while protecting individuals' privacy.

Learn more ›

or schedule a demo

About TypingDNA

TypingDNA is a new kind of biometrics that recognizes users by their unique typing patterns, powering more affordable, user-friendly authentication and behavioral analysis solutions. Use TypingDNA for employee, user and student authentication, as a 2FA solution that protects against identity fraud and as a non-intrusive method of continuous authentication.

Typing biometrics technology is approved by the European Banking Authority as a compliant element under PSD2 and by the Department of Motor Vehicles as an identity validation method for Online Prelicensing Courses.

TÜV AUSTRIA HELLAS — EN ISO 27001:2013, EN ISO 27017:2015, EN ISO 27018:2014

EBA European Banking Authority