GreatHorn

GreatHorn Account Takeover Protection

Reduce the Risk of Compromised Accounts

The risk of account takeover has increased exponentially. Yet identifying compromised email accounts can be tricky – often showing up only after there's been financial and reputational damage. Implementing multi-factor authentication won't protect users from cell-jacking, when a device has been left unlocked, or phone-based social engineering.

GreatHorn Account Takeover Protection provides a low-friction, secondary layer of authentication that's easy to implement, difficult to bypass, and minimally disruptive for employees.

Identify compromised accounts and block account takeover attempts using biometric authentication

Difficult to Bypass

Authentication is trustworthy and difficult to replicate as it's based on biometric data.

Minimally Disruptive

Initial setup and ongoing verification is as simple as typing an email address.

Simple Implementation

Administrator roll-out via Outlook plugin – no additional apps or devices.

Configurable Actions

Failure actions can be adjusted based on risk tolerance or group – from a simple alert to send prevention.

Mobile-Friendly

Supports mobile, desktop, and web interfaces to ensure protection regardless of access method.

Compatible with Other Solutions

Use in conjunction with multifactor authentication or identity access management solutions.

Eliminate risk by verifying a sender's identity using biometric authentication

GreatHorn's Account Takeover Protection uses machine learning to capture an employee's unique typing pattern on both desktop and mobile devices – analyzing the dynamics of a user's keystrokes, e.g. speed, pressure, and timing between keystrokes, but not the keystrokes themselves.

Deploy across mobile, desktop, and web interfaces with no additional applications or complicated set-up

Employees use their email address for authentication, with separate typing patterns for mobile and computer use. No additional software, hardware, or passwords required.

Gain greater visibility and control with automated policy-based actions

Configure actions based on authorization failures – such as inserting a warning banner to the recipient, removing the message upon send, alerting the security team, or simply logging the event for later analysis. Failed attempts populate into the GreatHorn dashboard providing context for faster incident response.

Get the Facts Sooner with a Free Trial. Learn more at www.greathorn.com.