

CVMetrics™ in Summary

Passwords Aren't Enough

In the economy of the 21st century, information is among our most precious commodities. Strategies on security and privacy, which are just ways of describing how to protect your information, are top priorities for both corporations and individuals. These can be difficult issues to conquer, as the principal enemy is often the security system itself, which may be so cumbersome that users are inclined to circumvent procedures for convenience and usability. How do you strike a balance between the need to meet regulatory and policy requirements for security, and the demands of users who want simplicity?

Current efforts include a jumble of solutions that require the user do something new: either that they keep track of a physical device, such as a USB token or PIV smartcard, or they submit a body part for scanning, such as fingerprints or faces. Sure, these approaches provide a better answer to the security question than just the simple challenge-response method of a username and password combination, but they utterly fail the test of simplicity. They require the user to do something different, they require additional hardware, support, training and cost, and further, they typically only protect access (aka, endpoints), and not ongoing activity. *Once you're in, you're in.*



Any sufficiently advanced technology is indistinguishable from magic.
- Arthur C. Clarke, "Profiles of the Future"

So, the magic is to not just reduce the footprint of the security system as apparent to the end user, but to make it virtually *transparent* in normal use, while at the same time meeting the needs of better security. By leveraging proprietary research, CVMetrics is able to validate users by the cadence and habit of how they use the keyboard itself. So, they are not required to do anything new. They can continue to use the traditional username and password approach, but now the system can capture this additional data about *how* they typed their credentials. Plus, once the user is authenticated, CVMetrics can validate *continuously*, in the background. Again, to the user, there is no change; *somehow, the system just knows.*

A Better Biometric

Using biometrics for security isn't a new idea, but they generally have a flaw by design: limited reference points. In the case of fingerprints, you have a fixed number of "swirls and whorls" on each fingertip, and only ten fingers. Using retinal scanners, you have a fixed pattern, and just two eyes. With facial recognition, you have but a single face. So, most biometric systems have an inherent problem: either set threshold low to make sure valid users aren't falsely rejected, or risk the false rejections by setting the threshold very high to protect against false positives, and letting the bad guys through. CVMetrics has several distinct advantages as a biometric: 1) it can dynamically ask for more typing (infinite reference points), allowing for a high threshold, with less chance of false rejection; 2) requires no new hardware, reducing training, support and cost; and 3) without specialized hardware input device, can be hidden from would-be attackers.

Combined With TickStream®

CVMetrics is a complimentary technology to TickStream. While both products have independent applications and use-cases, they are even more powerful when combined. TickStream provides a mechanism to understand what is happening on the computer. This includes what the user is doing, as well as all of the background processes and machine activities. With CVMetrics, you add corresponding data about who the user is at the time these things happen. This can be important because in *continuous* validation, you may find users will type differently depending on the applications they use, such as instant messaging versus a spreadsheet program. Only the full suite from Intensity Analytics provides complete analysis for security, telework, spend management, governance, risk and compliance, and more. Visit intensityanalytics.com for more information.