BLINDHASH
RESTORING TRUST IN PASSWORDS

INTRODUCING BLINDHASH

Protecting password databases and users' privacy is one of today's most significant business challenges. Monthly, a new string of a corporate security breaches are in the headlines. In 2016, thousands of organizations experienced a data breach, each costing an average of $4 million or $158 per record of information.[1] In addition to the direct cost, companies suffer significant damage to their reputation and experience higher than normal customer turnover following a data breach.

For the last 45 years, best practice has been to protect passwords by making each guess at the password expensive. However, once a password database is stolen, current encryption methods are easily defeated by cybercriminals. Therefore despite spending billions of dollars annually on security, 63% of network intrusions exploited weak or stolen credentials.[2]

BlindHash completely secures your passwords against offline attack, even if your password database is stolen. Our technology transforms a password hash into a lookup function over a massive pool of completely random data. The result of the lookup is used to decrypt the hash and allow the authentication process to complete. The BlindHash data pool acts as a "data anchor" since the entire data pool would need to be downloaded before an attacker could even begin the process of cracking a single password. The data pool is large enough that attempting to transfer the entire pool over the network would take years at full line rate.

1. User Submits Credentials to Your Server

Blind Hashing Data Pool

2. Blind Hash API Request

3. Blind Hash API Response

Random Lookups Generate a Key

4. Your Server Unlocks the Hash and Authenticates the User
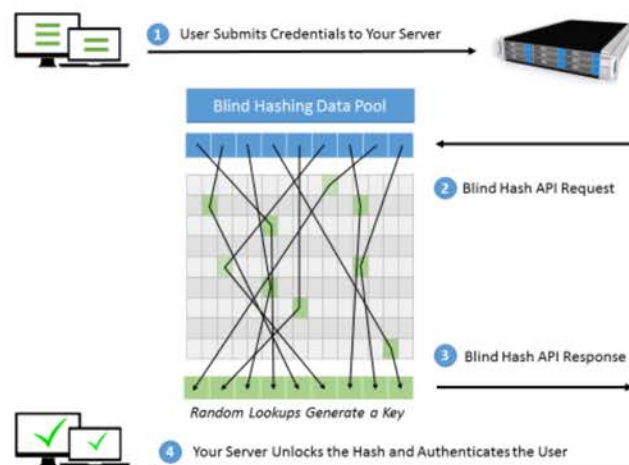
Our patented cloud-based solution provides an additive layer of security that works in conjunction with your existing password defenses, systems and processes. You maintain complete control over your data, your users, and your authentication process, but have the peace of mind that comes from knowing your password database is virtually impossible to steal.

Today your company can join the BlindHash Password Defense League where your users' passwords are immediately secured by the total combined resources of sites all across the internet. Every company that uses the data pool gains the full security benefit of the data pool, while just paying for a small share of the cost.

[1] *Ponemon Institute. Cost of Data Breach Study, 2016*
[2] *2016 Verizon Data Breach Investigations Report*

BLINDHASH
RESTORING TRUST IN PASSWORDS

FEATURES

Eliminates the possibility of a costly breach

Password theft puts our entire digital identity in the hands of cybercriminals, who use stolen credentials to cause billions of dollars in damages every year. BlindHash protects your systems, operations, brand, and most importantly, your customers from the most prevalent attack vector online today.

Unobtrusive

The BlindHash solution is completely transparent to your users. It provides an additive layer of security with no change to the login experience.

Simple & Secure

BlindHash is a single click install on all major platforms, and an open source library for your favorite language. Our solution is easy to add or remove on a per-user basis. The BlindHash API is designed so that your organization keeps complete control over your own user data. BlindHash knows nothing about your users; not their username, nor their password, not even if a login attempt was successful.

In the Cloud or In Your Datacenter

A massive shared data pool acts as Common Defense Fund for passwords on the internet. Every site gains the full security benefit, while paying just a small share of the cost. If your requirements warrant, a self-hosted private data pool is also available.

Scalable

BlindHash can protect any number of passwords and no site is too large or too small. Our system supports up to hundreds of thousands of logins per second, and provides responses in under 30 milliseconds.

BENEFITS

A small investment protects against a major loss

A small investment in the security provided by our BlindHash technology protects your business from major loss if your password database is compromised. It also protects your company against from the PR damage of having to report a data breach because even if someone hacks your system, they can never unlock the code to a password.

Seamless User Experience

BlindHash is completely transparent to the end-user, allowing companies to completely protect stored passwords without pushing complexity to the end-user.

Fully Additive Layer of Security

BlindHash works with your existing authentication infrastructure to measurably increase security with very low impact on back-end systems, and limited time requirements on IT staff.

Guaranteed Availability

We provide high availability through multiple levels of redundancy and fault tolerance, combined with a "shared nothing architecture" which allows the service to operate independently across multiple data centers, and avoid any single point of failure. BlindHash guaranties 100% uptime through multiple redundant data centers.

No lock-in

If for whatever reason you decide you want to stop using BlindHash, you can just turn it off. You don't need to reset your user's passwords, you can apply and remove the blind hash completely transparent to your users.