WHITE PAPER

CypherEye™
TRUSTED TRANSACTIONS

Credential-Free Authentication

Big Breaches from Password Insecurity

Anthem Inc.	80 million accounts (2015)
U.S. Office of Personnel Mgmt	22 million accounts (2015)
Sony Pictures Entertainment Inc.	100 terabytes of data stolen, $100 million in damages (2014)
JPMorgan Chase & Co.	83 million accounts (2014)
The Home Depot, Inc.	56 million accounts (2014)

Introduction

Passwords are a universal source of insecurity for financial services providers, enterprises and SaaS providers. Security phrases are the usual key for end users to unlock access, but the dozens or even hundreds of passwords juggled by each end user have become the Achilles heel of insecurity. As a result, prominent and costly breaches have occurred that could have been prevented. Organizations cannot expect their users and customers to solve the password problem on their own so recent institutional efforts to take control have helped alleviate the issue. However, they do not provide a lasting solution. CypherEye has created new optical and cryptographic capabilities that, when used with mobile devices, eliminate passwords and dramatically simplify integration and management of user logins. As a result, organizations can easily increase security of completing online transactions to an ultra-strong level and dramatically improve the user experience.

Passwords are a BIG Problem

Weak password security is a major risk for organizations of all sizes. Based on forensic investigations of prominent breaches, many occurred because attackers were able to guess simple passwords or steal credentials for system access.

Targeted phishing attacks are especially damaging when the unauthorized use of administrative passwords allow hackers access, enabling them to escalate their system privileges to reach sensitive systems, exfiltrate massive amounts of account data, and hide illegal activity. This type of attack allows damages to occur long before victims learn what happened.

For example, weak, unchanged default or stolen passwords were part of 63% of confirmed data breaches, according to the *Verizon 2016 Data Breach Investigations Report** (p. 20). Verizon's forensic analysts note: "The capture and/or reuse of credentials is used in numerous incident classification patterns. It is used in highly targeted attacks as well as in opportunistic malware infections. It is in the standard toolkit of organized criminal groups and state-affiliated attackers alike."

Weak passwords are like holes in a retaining wall, weakening security in random, unseen places – relentlessly placing your organization at higher risk of a breach. And this problem is getting worse. According to one study, the average number of passwords per user in the US is 130, and is forecasted to grow to 207 by 2020. Users often forget their passwords, typically 37 times a year. Another study notes that 61% of users re-use the same password on multiple sites.

The fallout from breaches triggered by password insecurity can be immense. Potential risks include financial loss, reputational loss, and compliance penalties. For

What is Multi-Factor Authentication?

A password is a security “factor.” Requiring a user to present two or more factors for system access raises security. Factors include:

- Something you have: a hardware token such as a key fob, USB stick or a pre-authenticated mobile device.
- Something you know: a password or pass phrase. A password issued for “one-time use” only is transmitted via a hardware device.
- Something you are: everyone has unique biometrics such as a fingerprint, voice pattern, or retina eye scan.

consumers, stolen account data and personally identifiable information can lead to months or even years of individual effort to fight the damage of identity theft.

Typical Options for Solving Password Insecurity

The password compromise problem is not new. To address this prolem, some organizations have implemented partial solutions such as single sign on (SSO) and password management. Both are helping to alleviate the issue, but both carry the same intrinsic flaw because they still rely on passwords for system access.

Single sign on systems allow users to log in once and automatically grant access to multiple sites requiring different credentials. SSO can be useful for an enterprise but is unhelpful for SaaS or consumer scenarios where millions of users are accessing systems not controlled by the SSO provider.

Password management system is a database of all the passwords for each user. Managing and updating these passwords can be cumbersome and this point solution is seldom used by enterprises. For consumers, a password management system creates a single point of vulnerability. This point solution may also prevent users from accessing services with mobile devices or via computers in internet cafes.

As noted, the primary vulnerability for every point solution relying on passwords is that security of the stored pass phrases is susceptible to threats such as brute force, man in the middle attacks, and keylogger and wireless intercepts.

Another approach is requiring more than one factor for access. Multi-factor authentication is often the preferred way to strengthen access security – but beware of a false sense of security in some scenarios. For example, some two-factor authentication solutions entail sending a one-time password to a phone via an SMS text. The U.S. National Institute of Standards and Technology has issued guidance calling for the phasing out of SMS-based two-factor authentication due to the inherent security risk that the one-time code could be intercepted or redirected.

The least attractive option for solving password insecurity is for your company to do nothing, which leaves users to continue actively causing risks mentioned above.

CypherEye’s Approach is Simpler and Stronger

CypherEye’s approach eliminates the password problem by doing away with the need for passwords. Our multi-factor authentication solution, called CypherEye, is simpler and stronger because it relieves the end user from the need to carry dedicated devices and remember complicated passwords.

The CypherEye authentication solution provides organizations with three major benefits.

1. Enables multi-factor authentication with a mobile device
2. Provides centrally managed administration with Microsoft Active Directory
3. Eases compliance with a unified audit trail of all authentications across devices, native applications and SaaS services.

For deployment, CypherEye easily integrates with enterprises and SaaS providers – typically requiring just a few hours to setup.

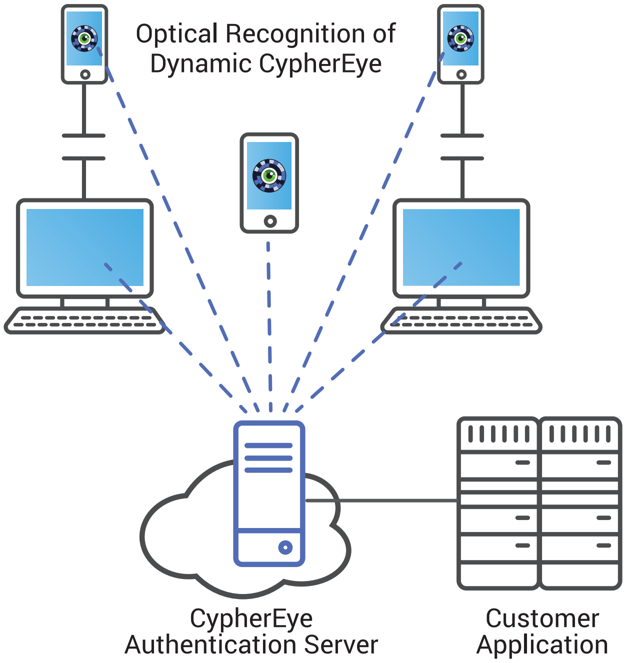
How it Works

CypherEye uses a unique patented optical code technology — CypherEye — to establish an out-of-band communication channel for secure authentication. This channel, along with state-of-the-art cryptography and key management creates a mutually authenticated four-way link between any device in need of authentication, the application or applications that need authenticated access, CypherEye Server and the end-users' phone CypherEye mobile application.

Effectively, the solution creates an identity vault under the control of the end user, complete with multiple online profiles, which can be securely unlocked from the mobile phone. With the CypherEye™ mobile app, authentication includes "something you know," "something you have," and "something you are" factors. The result is very strong protection from hacking, phishing and password re-use, while taking advantage of the bring-your-own-device trend to minimize solution cost and maintenance.

CypherEye provides faster recognition, better visual integration, and fewer errors. CypherEye ties authentication to a specific transaction, including those initiated on different devices to eliminate the cost and hassle of managing dedicated security tokens.

How CypherEye Works



Why CypherEye is Better

CypherEye's solution is better for any mid-to-large organization that needs strong multi-factor authentication for mobile devices.

> *"EIS integration with WInkk multifactor authentication and identity management allows our insurance customers to improve the security of access to sensitive information and furnish compliance with ISO 27000 family of standards."*
>
> Slava Kritov
> SVP Security & Operations, EIS Group

Features you need. CypherEye enables encrypted communications between the identity vault and the authenticating service with extra security of a shared secret. It uses optical code recognition with the mobile device's built-in camera to establish pairing between the phone and authenticating website. The solution enables a "mobile first" strategy with transparent public key identity-based cryptography for user authentication with a mobile phone. Strong authentication uses biometrics as an optional third factor. CypherEye provides endpoint protection with unique transaction reconciliation and endpoint compromise protection via second optical code recognition. The solution supports OAUTH2, SAML and ADFS for easy integration with existing applications, CAS and entitlement systems.

Flexible technology. CypherEye™ technology is flexible and works in a variety of scenarios. It provides fast response — up to one trillion unique patterns in every frame — even with challenging lighting, camera rotation, angles, and curvature of the surface with the animated optical codes.

More choices. CypherEye offers three choices for deployment: CypherEye Cloud, On Premise or Hybrid. Users get an easy-to-use, multi-device experience while on the back end, a solution that easily integrates with existing systems, protection from exploits and access removal if a device is compromised. Additionally it provides a complete audit log of registrations and sign-in.

Better for users. CypherEye is attractive to end users because it's easy to use, secure, encrypted and protected, and able to manage multiple identities with a single app.

Better for web providers. CypherEye is compelling for web providers because it increases registration, reduces support costs for password resets, provides built-in two- or three-factor authentication, and it is simple to integrate.

Better for enterprise. Our solution is essential to enterprise because it's easy to integrate (and is pre-integrated with Microsoft Active Directory), air-gaps corporate user identity information, supports multiple identities for different corporate roles, and enables hybrid cloud environments.

Invitation to try CypherEye

CypherEye invites your company to our free Trial Program for early adopters. By experiencing CypherEye, you will quickly discover how Winkk integration takes just a few hours. By establishing strong authentication with Winkk, your company can (1) increase your revenue while decreasing maintenance, (2) streamline and improve your customer experience, and (3) strengthen your brand by improving security.

To learn more about our Trial Program, please visit **cyphereye.com/trial** or send email to info@cyphereye.com.