



AuthenWare® Identity Authentication **Achieving Strong Security With Advanced Keystroke Dynamics**

Problem

All businesses depend on accurate identification and authentication of users in order to manage risk, protect private information and avoid losses due to fraud. Establishing a user's identity through username/password is not strong enough:

- Credentials can be shared – jeopardizing security and regulatory compliance
- Credentials can be stolen – leading to unauthorized access, disclosure of confidential/personal information, fraud and financial losses.

Secondary authentication mechanisms (challenge/response questions, hardware tokens, digital certificates) are costly to deploy and cumbersome for users resulting in significant user dissatisfaction and increased costs. While security professionals agree that effective security solutions must be easy to use and transparent to the user, today's secondary authentication typically causes user anxiety that significantly lowers effectiveness.

Solution

The AuthenWare® solution is a second-factor authentication technology based upon behavioral biometrics that is very accurate and completely transparent to the end user. AuthenWare uniquely identifies the rightful owner of the username/password credentials being supplied, by combining keystroke dynamics and heuristics to make user authentication and validation easy, cost-effective and reliable. With AuthenWare, you can be sure that:

- Only authorized users are granted access to applications or data
- Invalid access attempts are detected
- Stolen credentials are rendered useless
- Authentication is totally transparent to the user

How it Works

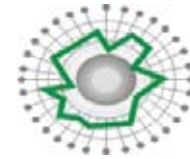
AuthenWare incorporates a breakthrough, multi-dimensional approach to validating identity. Using a series of security algorithms that record and measure a person's unique keyboard typing patterns, as well as other behavioral and environmental heuristics, the product creates a personal security pattern – the AuthenWare Singularity Pattern™ – that is as unique as the person's DNA. Based on a series of statistical singularities (aspects that distinguish one person from others), the pattern can even adapt to nuances in behavior such as those caused by medication, injury or fatigue.

With AuthenWare® you can be sure that:

- **Only authorized users are granted access to applications or data**
- **Invalid access attempts are detected**
- **Stolen credentials are rendered useless**

Each time a user signs in, their log-in characteristics are compared to the AuthenWare Singularity Pattern, and if it is mathematically similar, the authorized user is granted access. An imposter who has obtained username, password or other authentication information, however, will not be granted access since their pattern will not resemble that of the valid user. Rather than looking for an identical match, AuthenWare looks for a strong correlation to those aspects of the user's rhythm, including attributes like keyboard dwell time and flight time, that are highly individual.

The AuthenWare® Singularity Pattern™
is as unique as a person's DNA.



The product can be implemented in a way that matches the organization's needs, with configurable levels of authentication policy, False Acceptance Rates (FAR) and False Rejection Rates (FFR), and tight integration into existing applications and processes.

What it Does:

Improves Overall Security

AuthenWare uses multiple factors (keystroke dynamics as well as heuristics like IP address, screen resolution, browser version, time of use, and more) to authenticate the user. With multiple factors, a weakness in one factor is mitigated by the strength of other factors, providing the strongest possible security. The unique signature produced for a user is not directly tied to personally identifiable information (PII), ensuring compliance with numerous regulatory requirements including the Payment Card Industry Data Security Standard (PCI-DSS), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley Act (SOX), strengthening the organization's overall security posture. As an additional point of validation, AuthenWare has been certified by the International Biometric Group.

Minimizes Fraud

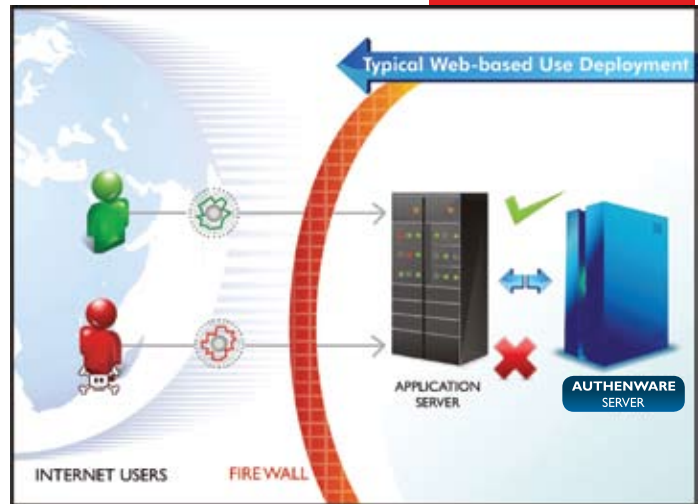
AuthenWare helps any organization to ensure that users are accurately authenticated, and that imposters are not able to access private or corporate information by masquerading as a valid user. It works in conjunction with the organization's existing authentication methods but goes beyond, to render stolen credentials useless. AuthenWare detects fraudulent authentication attempts and can enforce a variety of policies based on the user, transaction, application, specific application function or system, and can block man-in-the-middle and man-in-the-browser attacks as well as many other cyber threats.

Reduces Operational Costs

AuthenWare brings high confidence at a very low cost. Acquisition and implementation costs are just a fraction of other authentication or validation methods. The product works in concert with existing policies and practices, with seamless integration into web-based applications as well as standard corporate authentication methods. Help desk costs related to secondary authentication are reduced dramatically, and the cost of ensuring compliance with important regulations such as GLBA, HIPAA, PCI-DSS and others are minimized through strong user acceptance and ubiquitous adoption.

Deployment Scenario – Web-Based Applications

When used for strong authentication related to web-based applications, AuthenWare can either be located behind the perimeter firewall in the Demilitarized Zone (DMZ), or within the internal network infrastructure. AuthenWare is installed on a local server, deployed as an appliance or run as software-as-a-service (SaaS) that communicates with the web application using standard web services. For instance, in a typical deployment at a telecommunications company, the online customer self-service application is configured with business rules for each AuthenWare response type, including the determination of FAR and FRR relative to groups, users, transactions, etc. In production, it transparently monitors the web application login fields and compares user login characteristics to the AuthenWare Singularity Pattern, providing the appropriate response to the web application.

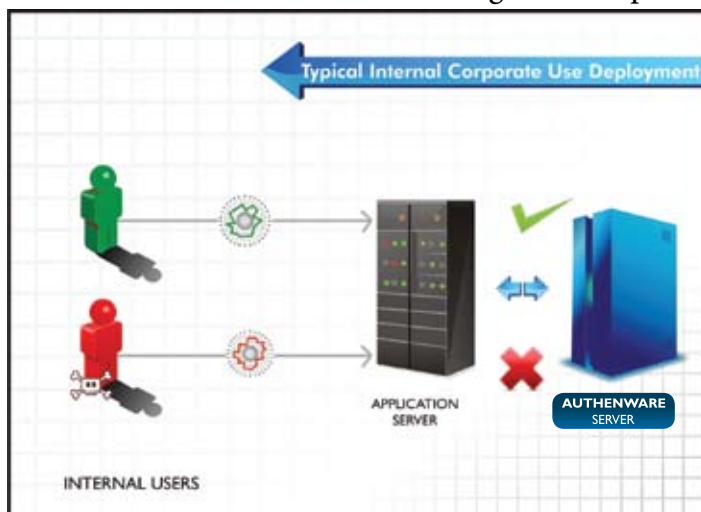


This not only provides security and identity protection, but it also assists companies with regulatory compliance. Since AuthenWare does not hold or transmit actual user credentials – only the AuthenWare Singularity Pattern – it ensures adherence to government and industry mandated regulations that protect personally identifiable information.

Deployment Scenario – Internal Applications

When AuthenWare is used for strong authentication, for example inside a government agency to prevent credential sharing, it is deployed behind the internal network firewall, and communicates with the application server(s) using standard protocols. The internal corporate application is configured with business rules for each AuthenWare response type, including the determination of FAR and FRR relative to groups, users and transactions. In production, AuthenWare transparently monitors the internal corporate application login fields, comparing the user login characteristics to the AuthenWare Singularity Pattern, passing the appropriate response to the application.

AuthenWare thus provides protection against sharing or theft of passwords and other authentication credentials, eliminating the most prevalent access control and data



vulnerabilities in today's corporate environments. Because Singularity Patterns are produced for each individual user, any attempts to login using another person's credentials will be caught. In addition to providing increased security, AuthenWare ensures that the organization will be well served when proving compliance with SOX, HIPAA and other industry-specific regulations that require auditability and individual accountability.

Why AuthenWare?

AuthenWare takes authentication and verification to a new level. Unlike other two-factor methods that can be bypassed, stolen, spoofed, phished or pharmed, with AuthenWare there is nothing to lose, nothing to forget, and no reason to call the help desk. This technology can be deployed instantly to massive numbers of customers, requires no additional hardware, and is totally unobtrusive. It is one of the most accurate and effective implementations of biometrics in the market today.

Features

- *Easy to implement* – dramatically increases security almost immediately
- *Easy for end users* – completely transparent; nothing to lose or forget
- *Safe* – biometric signatures are encrypted and kept separate from personal information and directory stores
- *Flexible* – customizable transaction-specific policies to respond to different regulations and requirements
- *Configurable security* – including False Acceptance Rate, False Rejection Rate, and five levels of authentication security at the user, group, transaction, application and system level.
- *Manageable* – administrative console that provides flexible and detailed reporting for auditing, setting rules, policies and alerts
- *Standards-based* – utilizes industry-standard Web service technologies
- *Convenient* – may be deployed to internal or web-based applications, as well as embedded within third-party applications and systems

Benefits

- Eliminates unauthorized access
- No additional end user hardware or software – completely transparent to the user
- Enhances user satisfaction and customer trust
- Bolsters regulatory compliance
- Complements existing security strategies
- Saves money through reduced help desk costs and low TCO
- 100 percent scalable
- Proven solution, certified by International Biometric Group (IBG) and Common Criteria
- Over 70 million current users

Platform Support

AuthenWare integrates with any 32-bit or 64-bit client application and supports the following environments:

Server Side: Operating System – Red Hat Enterprise Linux 5.2

Client Side: Web Browser – Microsoft Internet Explorer 6.0 and up, Mozilla Firefox 3.0 and up, Safari 4.0 and up

Minimum Server Hardware:

1.6 GHz dual-core processor (physical machine), 2GB RAM, 60 GB free disk space, and a connection to the internet



About AuthenWare®

AuthenWare® Corporation is a leading cybersecurity software provider focused on fighting identity theft. The Company's innovative tokenless authentication system delivers strong security through a combination of keystroke dynamics, behavioral and environmental characteristics to minimize identity theft, web fraud and other system vulnerabilities. The AuthenWare solution creates a unique personal security pattern that recognizes authorized users while keeping hackers out. AuthenWare is headquartered in Miami, FL, with offices around the world. Tens of millions of people use the company's products every day in a variety of industries, including financial services, government, healthcare, telecommunications and online retailers.

For more information, visit www.authenware.com.

AuthenWare Corporation

1221 Brickell Avenue, 9th Floor
Miami, Florida 33131
T: +1 305 377-8768
F: +1 305 374-6146
info@authenware.com
www.authenware.com