apersona™
effortless application security℠

# Adaptive Security Manager™ v2.0

www.apersona.com Patent Pending v15

## Why should I care?, What is Adaptive Authentication? & Why is it necessary?

**Why should I care?** Simply put: 1) 81% of fraudulent account take-overs were the result of weak or stolen credentials. 2) 61% of all credentials are reused across multiple services because no one can remember hundreds of passwords. 3) Over 2 Billion credentials have been stolen. Combine these three stats and there is only one conclusion: The majority of your user credentials are likely already known to the hacking community and no reasonable security professional should use ID and Password alone ("Naked Security") to protect Personally Identifiable Information (PII) that is "Non-Public" data.

**What is Adaptive Authentication?** Authentication solutions use some combination of "What a user knows" (like an ID, PIN and/or Password), "What a user has" (like a key fob, or one-time-password-generator, or key card, etc.), and "What a user is" (usually a biometric like a fingerprint or iris print, etc) to verify a user. Adaptive Authentication intelligently evaluates and learns hundreds of user related factors and behaviors that are continuously reviewed and updated. These factors are remembered and utilized to "fill in the gaps" for "What a user has" and "What a user is", and are used to supplement the "What a user knows" part of the authentication process.

**Why is it necessary?** Adaptive solutions enable service providers to provide broad all-in login and transaction security without any change in login behavior. Zero changes in the login behavior is particularly important when the users are customers. Without adaptive technology, the best solution that can be offered is an opt-in type offering where the user is offered the opportunity to step-up their authentication. While this is an option, many service providers recognize that an opt-in login security solution is by default communicating this rather negative message to their users: "Our service is not secure, but if you, our customer, want to take these additional steps, you can make it secure." Bottom line, Opt-In Login Security is becoming less and less desirable, while the need to protect every user's non-public data is increasing.

## Zero-Touch/Invisible Strong Adaptive Authentication & Risk Management

The aPersona Adaptive Security Manager™ (ASM™) delivers strong and invisible authentication with a revolutionary, future proof, adaptive multi-factor technology that addresses the need to protect millions of currently unsecure logins and applications. aPersona accomplishes this thru patent-pending, adaptive, behavioral recognition technology providing the lowest total cost of ownership while invisibly and reliably protecting vulnerable credentials from fraud and misuse.

## Audit, Compliance & Regulatory Requirements

**Meet and exceed your Audit, Compliance & Regularity Authentication Requirements** – It is no secret that the security threats surrounding stolen credentials are creating an ever increasing set of regulations that highly recommend and/or require multi-factor authentication for access to non-public information. Organizations protecting non-public consumer data need a robust and cost effective way to meet and exceed their Audit, Compliance and/or Regulatory Authentication Requirements. aPersona's Adaptive Security Manager™ protects your organization's applications with an invisible and cost effective login security layer that actively protects transactions and logins, and at the same time provides rich Risk-Analytics for your Audit, Compliance or Regulatory Requirements. In addition, our reporting also provides Big-data information and analytics on: Invisible/transparent User Registrations, Forensic Learning, Monitoring, Risk Scoring, and Real-Time Risk Analysis Reports that address all transactions. Managed thru a single pane of glass management services portal for operational management, no other adaptive multi-factor authentication solution provides such a simple, seamless yet cost effective security authentication protection and reporting.

## Truly Adaptive Technology Powered by Real Intelligence

**Patent-Pending Patterns of Behavior Authentication** – Every user has his or her own unique Patterns of Behavior in cyberspace. aPersona's patent-pending adaptive multi-factor authentication platform learns these Patterns of Behavior (PoB) and gathers forensics for reliable and efficient authentication for any type of transaction. These individual PoBs provide strong assurance for invisible multi-factor authentication, and meet the standards for NIST FICAM Trust Criteria Level 3 and enable enterprises to meet and exceed FFIEC Guidelines and NIST's latest upcoming recommendations for risk-based multi-factor authentication. Continuous learning and adapting evaluations of user's behavior, devices, locations, one-time-use keys and other factors are constantly being evaluated and scrutinized against pre-set application specific security policies.

**Truly Adaptive for a Frictionless User Experience** – Adaptive Security Manager™ is always learning and evolving the digital behavior of each user as they change devices, networks, and the way they interact with online and mobile applications. Rather than rely on industry blacklists that are never up to date, ASM™ intelligently blacklists everything outside a user's normal patterns of behavior. This allows ASM™ to know when to allow a transaction and only when needed, when to step-up authentication for a user allowing for a seamless layered security architecture.

**No Static Factors** – The Adaptive Security Manager™ patent pending technology provides continuously evolving and ever changing digital forensic signatures. This means there are no seed "keys to the kingdom" or static authentication factors sitting around waiting to be discovered or stolen.

## Great End-User Experience

**Nothing to Install** – Users expect that their accounts are protected. For customer facing applications, if a security solution requires the user to "do anything", the best to you can do is make it an opt-In, which will get low to zero adoption. aPersona ASM requires NOTHING from the user. Users don't need to register, or download anything or carry anything.

**Nothing Extra to Carry** – Not only do users hate to keep up with hard tokens and USB key fobs, they are expensive to buy and administer. ASM™ does not require users to have anything other than the device from which they are accessing the application. In the event ASM™ needs to confirm a new behavior, a one-time password is sent via email, SMS, or voice call.

**Invisible Registration & Initial Learning** – As new user accounts are added and begin accessing ASM™ protected applications, a profile is automatically created and ASM™ begins learning the user's behavior.

Invisible Authentication – When users login or do any authenticated transaction within an application, ASM™ quickly and invisibly evaluates over 100 behavioral characteristics to authenticate the user's identity. This allows for layered security and a great user experience.

## Easy Configuration & Administration

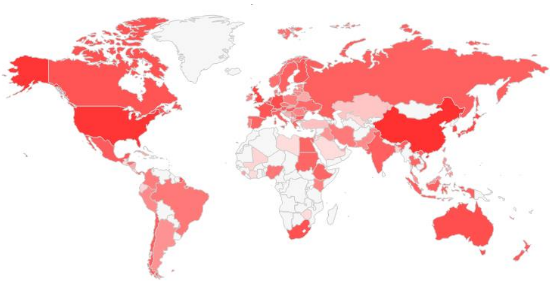
**Auto Learning & Auto Registration** – Once a security policy is chosen and transactions are sent to the ASM™ for authentication, the ASM™ will begin automatically registering users and learning their behavioral patterns. If administrators only want the ASM™ to learn without challenging users, they simply put the security policy in "Learning Mode." Each security policy can be in one of three modes: Learning, Predicting, or Protecting.

**Strong Authentication and Auto Whitelisting** – The aPersona ASM™ evaluates over 100 forensic and behavioral characteristics to create unique behavioral profiles for each user. Only transactions falling within normal user behaviors are whitelisted. This creates very strong identity authentication. Everything outside of that is automatically blacklisted at the individual user level unless the user specifically adds it to their whitelist by successfully completing the user challenge.

**Country Filtering** – ASM provides granular Country Filtering that can be configured by individual security policies. Approximately 80% to 90% of attacks for any service will originate from outside the service country location. While country filters can be deployed at the firewall level, this type of deployment is problematic where executives or employees travel outside of normal country service areas. ASM's Country Filtering is uniquely defined within each security policy with override options that can be configured to support one-off overrides for a period of time for a given user when required. ASM's Country Filter is updated from the current Global IP Country Block lists once per day.

aPersona™ effortless application security℠

# Adaptive Security Manager™ v2.0



**Active Threat Actor IP Filters** – ASM's Active Threat Actor IP Black List Filter can be turned on for any ASM Security Policy. The ASM Threat Actor Filter is comprised from hundreds of Threat Actor Databases across 8 different categories of threat data that include categories such as: Spam, Bad Reputation, Threat Organizations, Malware, Attacks, & Abuse. The ASM Active Threat Actor IP Block List contains over 600M Threat Actor IP addresses and is continuously updated every 15 minutes.

**Enterprise Management Portal** – In addition to a very robust API, everything an administrator needs to do can be accessed through a user-friendly, web management portal.

**Multi-tenant** – Create separate instances and security policy groups for specific applications, business units, or even clients. ASM™ is designed for service provider flexibility whether your clients are internal or external.

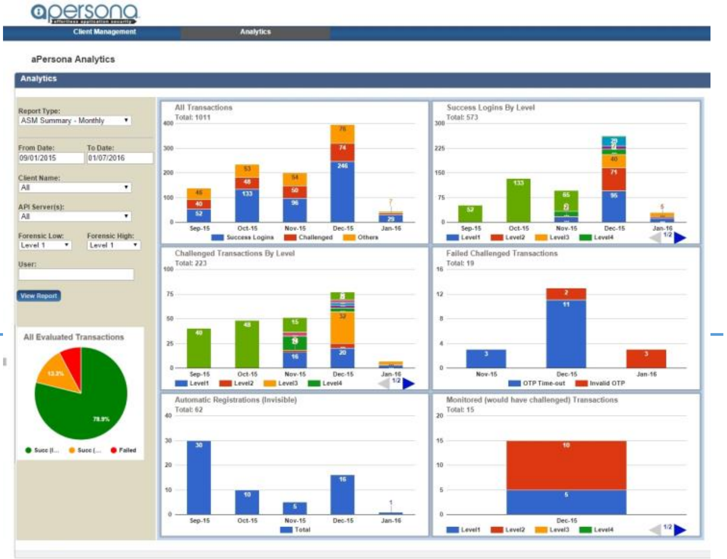
**Low TCO** – Zero-Invisible-registration, self-learning, and self-purging along with very thin resource requirements give ASM™ an extremely low Total Cost of Ownership. We don't require expensive database licenses or hardware, and our license and maintenance fees are designed to make sense to protect thousands or millions of users.

**Highly Scalable** – The ASM™ architecture is designed to allow for easy on-demand scaling for peak loads. Simply spin up additional application servers to meet peak demand and de-provision them once the peak load has passed.

**Run Anywhere** – ASM™ can be run as a service or installed locally on premise or in the cloud.

## aPersona Scalability, Flexibility & Big Data Risk Analytics

aPersona's Adaptive Security Manager™ scales across your organization and enables a customized set of factors that match the levels of risk or compliance needed by user, transaction, service, location, user group, and transaction values all governed and managed centrally over selectable periods of time. The Adaptive Security Manager™ uses a multi-tenant architecture that enables enterprises and IT service providers to isolate, support, and manage any combination of user groups, organizational groups, geographic groups, and/or customers easily from a single management portal. Further, aPersona's advanced reporting and analytics gives IT security personnel real-time forensic data for Big Data risk analysis and analytics.



aPersona Analytics

Analytics

Report Type: ASM Summary - Monthly

From Date: 09/01/2015

To Date: 01/07/2016

Client Name: All

API Server(s): All

Forensic Low: Level 1

Forensic High: Level 1

User:

Finding the balance between user convenience, commerce and security is challenging. The Adaptive Security Manager™ gives you the tools to take back control while giving users transparent access your services. "Naked Security" just doesn't cut it anymore; aPersona brings the intelligence and adaptability that's necessary to successfully deliver easy to use and secured services to users.

**For more information or to set up a free trial, go to www.apersona.com or call us at 1-866-229-0177.**