apersona™
effortless application security℠

Adaptive Security Manager™
v3.x

Overview

aPersona Adaptive Security Manager™ (ASM™) utilizes machine learning, artificial intelligence (learning, problem solving and pattern recognition) and cognitive behavioral analytics to invisibly protect on-line accounts, web service portals & transactions from credential theft & fraud. Specifically engineered for both internal employee facing services and customer/client facing services, ASM™ arms organizations with a single solution with centrally controlled security policies for any type of transaction at any risk level.

Zero-Touch/Invisible Strong Adaptive Authentication & Risk Management

ASM™ delivers 'User Centric/Device Anywhere' 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. 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.

Truly Adaptive Technology Powered by Real Intelligence

Patterns of Behavior Authentication – Every user has his or her own unique Patterns of Behavior in cyberspace. aPersona's adaptive multi-factor authentication platform learns these Patterns of Behavior (PoB) and gathers forensics for reliable and efficient authentication for any type of transaction.

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 enabling ASM™ to know when to allow a transaction and when to step-up authentication users.

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.

Identity Provider Agnostic – aPersona ASM is agnostic to the backend Identity provider being used to perform the initial ID & Password / SSO Token Authentication. ASM easily integrates with all your current Identity Providers.

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 expensive key fobs to receive state of the art adaptive authentication protection.

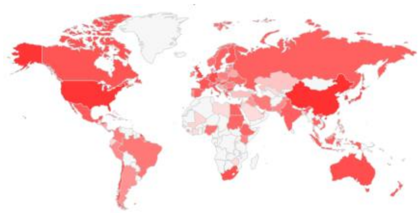
Invisible Registration & Initial Learning – As new user accounts are added and begin accessing ASM™ protected applications, a profile is automatically created and ASM™ begins learning the user's behavior.

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. 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.

GEO Country Fencing/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. 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.



Active Threat Actor Fencing/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 continuously updated every 15 minutes.

Real Time Threat Management – ASM continuously evaluates transactions for threats based on four different threat activity velocities (country threats, threat actors, transaction failures and all three combined) and automatically increases user protections when velocity thresholds are exceeded.

Flexible Centralized Security Policy Management – All available Adaptive MFA forensics are setup, managed and controlled with centralized security policies. Security policies can be setup by application and user security groups or for any other requirement.

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.

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.

Flexible Integrations – ASM™ can easily be integrated into any existing web service application using our three API's and ASM™ is fully integrated with popular services and SSO platforms like Microsoft Enterprise Active Directory Federation Services (ADFS) providing layered adaptive multi-factor authentication to enterprise SSO deployments.

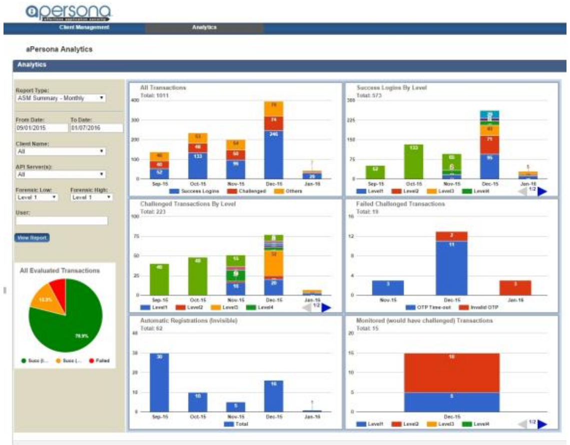
Response Methods - ASM™ supports a number of response options for end user verifications including Email, SMS, Voice and Mobile Push.

Extensible Use Cases - ASM™ Adaptive Multi-Factor capabilities enable it to be deployed for internal employee based services as well as customer/client/consumer use cases. Organizations can be confident that ASM™ will extend and support their use cases and MFA needs.

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.

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.



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:

For more information or to set up a free trial, go to https://www.apersona.com/contact-us.

Features list: https://www.apersona.com/features