



Arcot Fraud Prevention Network

360° Fraud Protection

Solution Guide

SOLUTION GUIDE

Overview

Benefit from the largest destination for SaaS authentication transactions

Stop fraud faster with privacy-protected fraud data sharing

Uniquely identify individual machines with DeviceDNA and DeviceID technology

Automatically notify members when devices are marked as suspicious

Aggregate fraud data automatically to enhance risk management and fraud reduction programs

The Online Fraud Prevention Challenge

Online identity fraud is growing faster than ever. Cyber crime networks around the world are collaborating to enhance their capabilities to steal valuable online credentials and information. While individual organizations implement anti-fraud solutions and thwart some attacks, the fraudsters repeat the same attacks across other organizations and channels, taking advantage of the lack of data sharing between organizations. Criminals are also expanding their reach beyond the traditional targets of consumer banking and credit cards to online account access and web portal access in other industries. Current fraud detection and stronger authentication solutions fail to take full advantage of the collective experience of other organizations to get ahead of the cyber criminals.

The Arcot Fraud Prevention Network (AFPN) Solution

The Arcot Fraud Prevention Network enables you to incorporate secure, privacy-protected data sharing into your environment to help stop online fraud before it happens. With a network of millions of transactions and thousands of financial institutions and other enterprises, we have a vast collection of online fraud data with which to monitor emerging threats in the network, extrapolate fraud trends and immediately share that information with the network members. The AFPN can detect and prevent fraud at the individual machine, IP address, and payment card levels. When questionable activity occurs on a particular device, IP address or payment card, it is added to the AFPN suspicious activity list known as the gray list. The gray list is instantaneously shared with all of the AFPN members. Each member can then take action based on their individual fraud policies and risk tolerance. The AFPN is open to all Arcot RiskFort risk-based authentication customers whether they are using our A-OK Service or they have RiskFort installed on-premise.

Arcot DeviceDNA™ and DeviceID Technology Identify Individual Devices

The AFPN makes use of both tagless and tagged identifiers which allow it to track suspicious behavior to the device level. Other solutions are limited to detecting and reporting on an IP address that is committing fraud. Using a wide range of parameters, Arcot DeviceDNA technology creates a tagless fingerprint to uniquely identify individual machines.

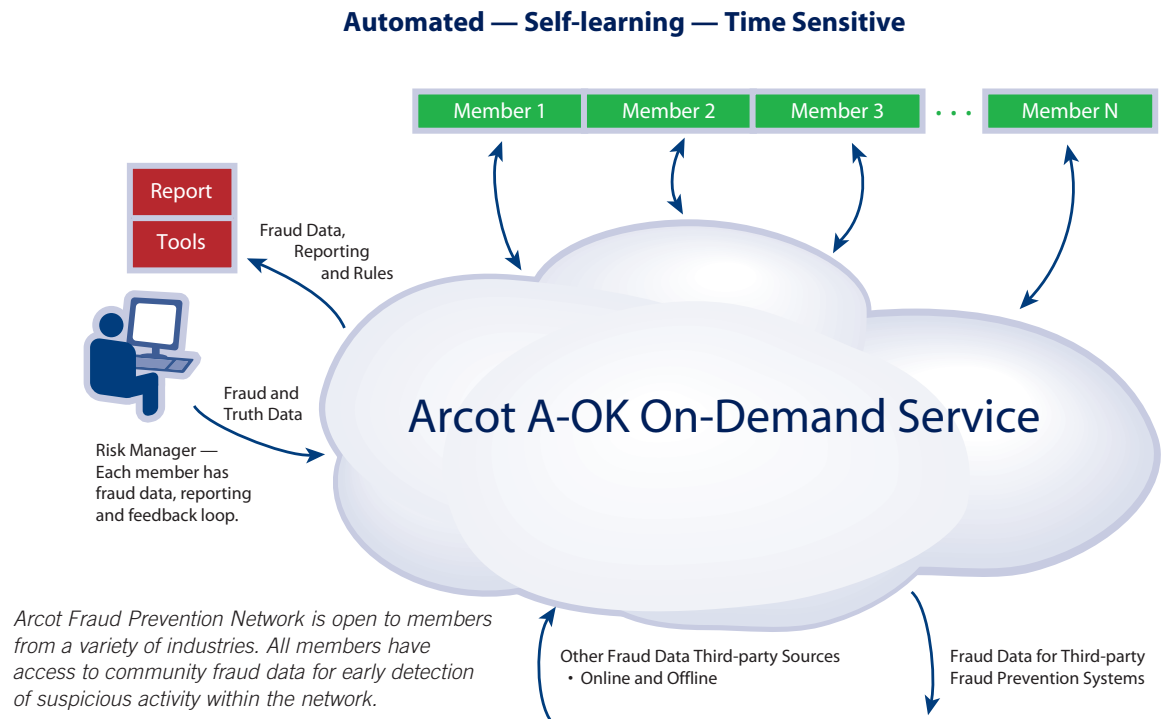
By combining security attributes, vertical-specific attributes and authentication methods, computers, mobile phones, and PDAs can be fingerprinted and suspicious behavior tracked to the individual device level. DeviceDNA is tagless and can identify the machine without putting a marker on the device. Arcot also provides a DeviceID tag for every device. Both DeviceDNA and DeviceID can identify devices and when used in combination, can uniquely identify a device with very high confidence.

The AFPN can also take advantage of existing tagged device identifiers such as browser cookies. Typically, these cookies are not visible to other organizations. The AFPN, however, can see these cookies, flag the device as suspicious, and instantly broadcast the information to the entire network by adding it to the gray list.

AFPN Monitors Suspicious Devices in Gray List

The AFPN monitors device activity using a combination of DeviceDNA, DeviceID and existing machine identifiers. When a device is suspected of fraudulent activity, it is flagged as suspicious and added to the gray list. The AFPN community is automatically notified of the addition to the list. Each member can then take appropriate action to quarantine the device and prevent it from accessing accounts or executing fraudulent transactions. Arcot uses fraud aging algorithms to ensure the integrity and currency of the data on the gray list. Suspicious devices receive a score and that score is used to update the list on a regular basis.

FIGURE 1: ARCOT FRAUD PREVENTION NETWORK



Shared Fraud Data Stops Fraud Faster

Arcot Fraud Prevention Network members can take full advantage of the shared experience of other AFPN members and no longer have to go it alone. The AFPN aggregates fraud data across the community automatically to enhance its members' risk management and fraud reduction programs. Arcot uses a consolidated view of the entire network to detect suspicious behavior using existing rules applied across all of the members. Therefore, the entire community benefits when suspicious activity is detected at an individual site. In addition, an individual member's risk policies are automatically enhanced. As an example, if an organization has a risk policy that takes effect after ten attempts/failures, this policy is now enforced once ten attempts of that type occur at any organization within the fraud prevention network. This means that suspicious activity is identified faster and preventive measures can be automatically activated. The AFPN uses a variety of real-time methods to identify, act upon, and log suspicious activity. As a result, AFPN members immediately benefit from the collective intelligence of the community with extra protection that is transparent to end-users.

360° Continuous Feedback Loop

The AFPN monitors online transactions and online access and provides continual fraud feedback to all of its members. The AFPN uses self-learning algorithms and ages the fraud data over time to keep the fraud data relevant. AFPN scans for suspicious behavior by analyzing various data across all participating organizations to identify criminal activity. For instance, if suspicious transactions arise with one account from one device, that device is flagged for all other organizations on the network. Therefore, a fraud attempt at one organization can put other organizations on alert even before they are hit with the same fraud. Case management tools allow the risk manager or fraud analyst at an individual organization to identify suspicious activity, update risk policies, incorporate fraud data into other applications and provide truth data back into the network.

Population Diversity Enhances Fraud Data

The AFPN sees data and information across a wide range of industries and businesses. Banks, Financial Institutions, Online Merchants, Pharmaceuticals, Health Care, Insurance, Telecom and other enterprises will help ensure that AFPN captures the widest range of online fraud data.

Arcot Fraud Prevention Network—360° Fraud Protection

AFPN uses multiple sources of information including trend analysis, risk assessment and fraud detection, truth data, and observed customer actions from over 60 million cardholders, issuers, merchants, online businesses and consumer users worldwide. It can also accept input from independent offline fraud prevention products and return feedback, data, and advisories to offline fraud prevention products. All input is aggregated into one data center providing a single collection point for all fraud information. From there, it is automatically shared with the members.

AFPN Maintains Privacy of Users and Organizations

Fraud data is stored in a secure manner in the AFPN, thus ensuring privacy of the each member's data. Privacy is preserved while sharing information. The AFPN doesn't post any information about a transaction that would identify the consumer or the institution. Instead, the network provides summary information on transactions that occurred at other organizations including transaction amounts, the IP address where the transaction originates, the location where that IP address is registered, the deviceID, and the DeviceDNA.

Flexible Case Management and Reporting Tools

As part of the 360° continuous feedback loop, the AFPN provides reports to its members on suspicious activity. It categorizes the information at the IP and device level and type of activity. The customer can then use this data to help determine whether fraud occurred and use the tool to send this information

back to the network. The AFPN also provides new suggested RiskFort rules and policies that can be quickly activated by the organization's risk manager. Optionally, members can choose to allow the new rules to be activated automatically. The tool can also be used to supply truth data to the network. Truth data from the case management tool has a self-regulatory impact on the AFPN. Regularly updated information maintains an accurate set of fraud data within the AFPN community.

Transparent to Consumers

AFPN continuously monitors, detects and prevents fraudulent activity from taking place while minimizing the impact to legitimate users. Online users are transparently protected with no additional burden placed on consumers for the bulk of their transactions. When suspicious behavior is detected, users may be asked to provide secondary authentication protecting them from fraudulent activity.

Program Participation

The AFPN is open to all Arcot RiskFort risk-based authentication customers whether hosted in the Arcot A-OK Service or installed on-premise. By joining, the member agrees to

- Permit Arcot to collect and share transaction data anonymously
- Report truth data monthly
- Provide feeds on suspicious and/or fraudulent activity.

There is a fee for member participation.

Contact your Arcot Sales Representative for more information.

About Arcot

Arcot is the cloud authentication leader. Our fraud prevention, strong authentication, and e-Document security solutions make Web transactions and online access safe for millions of consumer, enterprise, and e-Commerce users.

Organizations can transparently deploy stronger authentication and allow users to conveniently authenticate from any computer or mobile device. Arcot solutions deliver the right balance of cost, convenience and strength.

For more information, please visit www.Arcot.com, email sales@arcot.com, or contact your nearest sales office:

Corporate Headquarters, U.S.
Arcot Systems, Inc.
Ph: +1 408 969 6100

United Kingdom
Arcot International
Ph: +44 118 965 7998

Germany
Arcot Deutschland GmbH
Ph: +49 8157 997793

India
Arcot R&D Software Private Ltd
Ph: +91 80 6660 2745



www.arcot.com

Copyright © 2010 Arcot Systems, Inc. All rights reserved. Arcot, Arcot WebFort and ArcotID are registered trademarks of Arcot Systems, Inc. All other trademarks are the property of Arcot Systems, Inc. or their respective owners.

10-49