



Arcot RiskFort™ Fraud Detection and Prevention

Block Fraud in Real-Time

DATA SHEET

Overview

First line of defense against online fraud. Measures and blocks fraud in real-time.

Assesses fraud potential of every online access attempt or transaction by examining a range of data collected automatically.

Uses a Risk Score and business rules to approve or decline the transaction, ask for additional authentication, or alert a customer service representative.

THE IDENTITY FRAUD CHALLENGE: The incidence of online identity fraud continues to grow. Criminals have expanded their reach far beyond traditional targets of consumer banking and credit cards, looking to harvest valuable data that is accessible online. The challenge you face is how to detect and block fraudulent activity while it is occurring, before losses can occur, without affecting legitimate users. Anti-fraud countermeasures that require user interaction can create a negative user experience and affect customer loyalty.

THE RISKFORT SOLUTION: RiskFort is a fraud detection and risk-based authentication solution that prevents fraud in both consumer and enterprise online services. It can be used to reduce fraud and protect users from internet attacks whether users are shopping online or accessing confidential or private information via a web portal. RiskFort is your first line of defense against identity fraud. It measures and blocks fraud in real-time, without any interaction with your users. You can quickly and easily add it to any consumer, enterprise, or e-Commerce Web portal. RiskFort provides organizations the ability to determine and enforce different levels of authentication based on the assumed amount of risk. Based on a Risk Score and company policies, you can enforce multiple other forms of strong authentication depending on the user and the type of transaction.

Measures Risk in Every Transaction

RiskFort examines a wide range of data it collects automatically about each login or transaction, and uses that data to calculate a Risk Score. You have complete flexibility to determine the response to that Score based on your policies and risk tolerance.

Invisible to Legitimate Users

RiskFort affects only those users whose behavior does not match their personal profile, historical data and your policies. Most of your users will never know it is there.

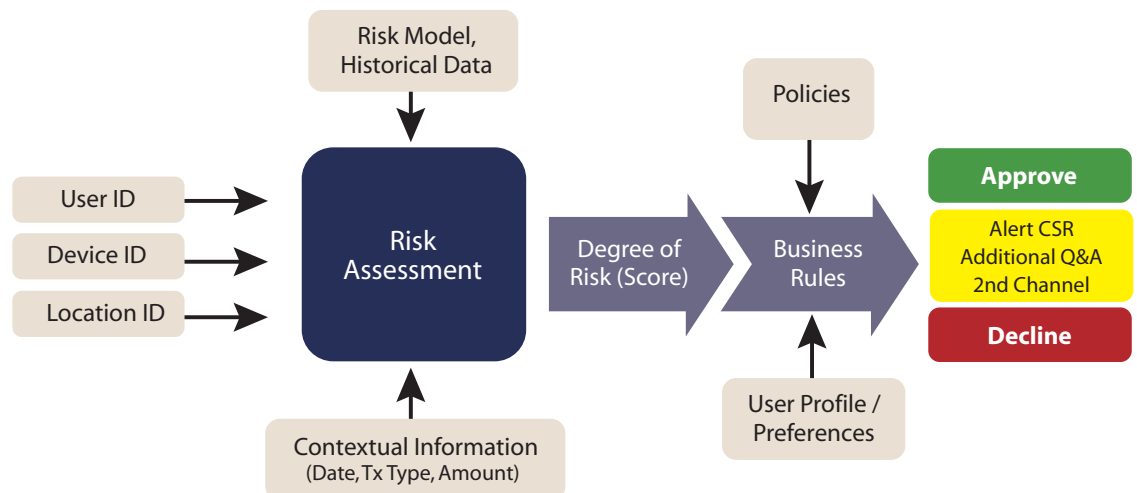
Real-time Blocking

You have the option of blocking high-risk transactions in real-time, before suffering any losses due to identity fraud. Block fraud as it occurs, rather than trying to investigate it afterwards.

Integrates with Any Application

You can integrate RiskFort with any Internet-facing application via an API. It enables you to add real-time fraud detection quickly and easily to existing business processes and applications.

RISKFORT PROCESS



Server platforms

Operating Systems

- Microsoft Windows Server
- Sun Solaris

Application Server Interface Support

- JAVA API for J2EE-compliant application servers (e.g., IBM WebSphere, BEA WebLogic, and Apache Tomcat)
- Web Services for Windows .NET platform-enabled and other application servers

User Identification Data Sources

- LDAP Directories
- SQL Databases

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.

RISKFORT FEATURES AND BENEFITS

Reduce Losses Due to Fraud

RiskFort prevents fraud losses by blocking high-risk transactions before they complete, or requiring additional authentication for unusual transactions. In ePayments environments, RiskFort interacts with the Arcot TransFort 3-D Secure compliant solution to reduce the risk of fraudulent cardholder transactions. In consumer and enterprise Web and remote access situations, RiskFort interacts with Arcot WebFort Versatile Authentication Server to implement step-up authentication when encountering a suspicious transaction.

Match Rules to Your Environment

The customizable rules engine enables you to configure RiskFort to match your business practices and risk tolerance, rather than forcing you to change your operations to fit your security tool.

Invisible Protection

Your users never have to know that you have RiskFort deployed to prevent fraud. There is no change to their user experience and therefore no new calls to the help desk.

Protect Existing Infrastructure Investment

RiskFort integrates with your existing access management and other security products, eliminating the need for you to upgrade other parts of your network to add strong authentication.

Meet Regulatory Requirements

Our customers use RiskFort to meet a number of government and industry regulations for protecting access to data, including FFIEC, HIPAA, and SOX.

Annotation

RiskFort provides an audit trail that annotates each recommended action.

Optional Personal Assurance Message and Scrambled Pin Pad

You can add site authentication for your users with the optional Personal Assurance Message. The optional Scrambled PIN Pad scrambles the pattern of numbers each time you users log in, to defeat spyware.

Easy Integration with Arcot Strong Authentication

RiskFort integrates with Arcot WebFort Versatile Authentication Server (VAS). WebFort VAS helps organizations achieve compliance by creating a central point for authentication policy and enforcement. WebFort VAS gives you the flexibility to choose the authentication method that best suits the security and convenience needs of different types of users. You can add standards-based hardware and software authentication methods, use the unique ArcotID Secure Software Credential, as well as employ callouts to proprietary authentication methods.

Reduce Fraud in e-Commerce Transactions

Arcot is the standard for ePayment authentication and fraud reduction for both card issuers and online merchants. Basic cardholder authentication and 3-D Secure compliance is provided by Arcot TransFort. RiskFort provides an additional layer of fraud prevention and works transparently with TransFort.

Multi-Component Risk Assessment

RiskFort combines four components for unmatched fraud detection capabilities:

- Customizable policy store
- Field-programmable rules that take effect immediately
- Optional fraud model
- Callouts to other internal or external tools

Policy Store, Field-Programmable Rules Engine

You can build rules that are specific to your policies and environment. You can create and combine rules based on a wide range of transaction and session criteria, and match those policies to different groups of users. You can add or change rules on the fly when policies change.

Fraud Model

Uses statistical techniques, such as Bayesian modeling, to compare each transaction against a scoring formula. RiskFort periodically updates the formula based on recent fraud and transaction data.

Callouts

RiskFort can call other internal or external fraud management applications, such as Falcon. You can also aggregate scores from multiple systems to generate one combined score.

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 © 2009 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.

09-243