



# 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 multiple component risk analysis to approve or decline the transaction, ask for additional authentication, or alert a customer service representative.

Hybrid combination of a statistical model and rules, assess transaction risk to produce a Risk Score.

**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 instantaneously detect and block fraudulent activity before fraud losses 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:** Arcot RiskFort is your first line of defense against identity fraud. You can verify and detect suspicious activity in real-time for consumer and enterprise online services without inconveniencing legitimate users. RiskFort is a comprehensive, multi-channel risk assessment and fraud detection solution that transparently helps you detect and prevent fraud before losses occur. You can create an adaptive risk analysis process that assesses the fraud potential of every online login and transaction based on level of risk, user and device profiles, and organizational policies. As a result of the risk score users can be allowed to continue, be required to provide additional authentication credentials, or be denied access.

### Measures Risk in Every Transaction

RiskFort examines a wide range of data it collects automatically about each login or transaction. The self-regulating scoring engine produces a risk score derived from analytics and rules. The RiskFort scoring engine uses a hybrid combination of a statistical model and rules to decide what action to take on a given transaction. You can set the false positive rate tolerance or the fraud reduction rate tolerance to adjust the affect on legitimate users. 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. There is no change to their user experience and therefore no new calls to the help desk.

### Reduce Losses Due to Fraud

RiskFort prevents fraud losses by blocking high-risk transactions before they complete, or requiring additional authentication for unusual or suspicious transactions. In ePayment 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. RiskFort also works with third party fraud prevention solutions.

### Multi-Component Risk Assessment

RiskFort combines multiple components for unmatched fraud detection capabilities:

- Self-learning scoring engine based on an analytical model
- Customizable rules engine with field-programmable rules that take effect immediately
- Default rule sets that cover typical fraud patterns based on predefined use cases
- Multi-channel fraud management architecture combining Web, Call Center (IVR), ATM and Mobile channels
- DeviceDNA™ fingerprinting isolates devices with suspicious activity.
- Arcot Fraud Prevention Network shares fraud information with all of the network members
- Callouts to other internal or external fraud analysis tools

### Sophisticated Fraud Modeling Techniques

The RiskFort scoring engine is based on analytical modeling techniques. These models are built by conducting a statistical analysis of transactional and fraud data. These models use multivariate analysis and Bayesian techniques to return a score based on the relative values of multiple parameters. The scoring engine adjusts itself based on ongoing data – when new threats arise, the scoring engine can adapt itself. RiskFort periodically updates the formula based on recent fraud and transaction data. The rules engine can trap outliers that are not yet part of any trend.

## Server Platforms

### Operating Systems

- Microsoft Windows Server
- Sun Solaris
- Linux

### Application Server Interface Support

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

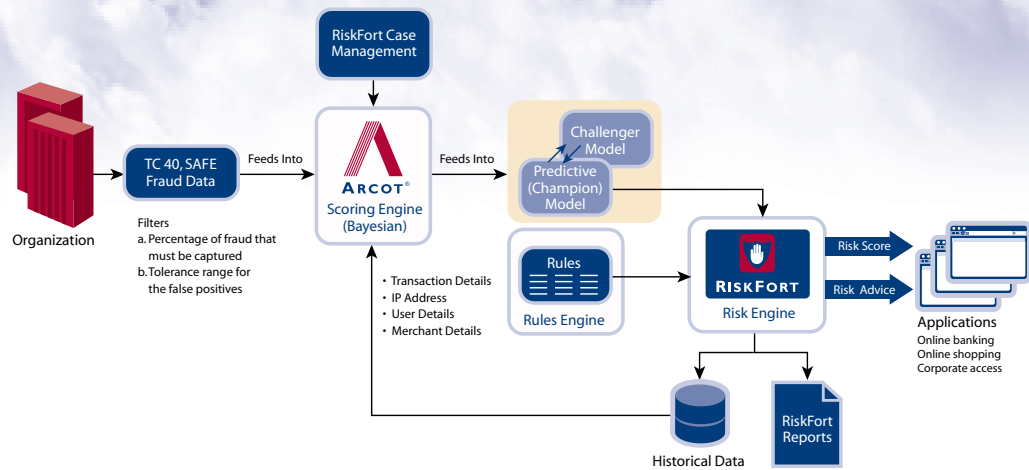
### User Identification Data Sources

- 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 FRAUD DETECTION AND ANALYSIS PROCESS



### Field-Programmable Rules Engine

You can build rules that are specific to your policies and environment and combine rules based on a wide range of transaction and session criteria. You can add or change rules on the fly when policies change. The rules engine consists of rules that can be combined into different rule sets for different transaction types and user groups. The risk evaluation leads to a result for each rule. The combined value of the rules analysis results in a risk score which can be used to override the score from the scoring engine. This allows you to immediately block known fraudulent actions that may not yet be known to the model in the scoring engine. It also allows organizations to make exceptions for users that may override an existing transaction pattern, such as a person traveling in a country that is not part of their established user profile. Administrators can add new rules or configure existing rules to work off revised parameter values.

### Protect Existing Infrastructure Investment

You can integrate RiskFort with any Internet-facing application via an API. It enables you to add real time fraud detection to existing business processes and applications. RiskFort integrates with your existing access management, VPN, online banking, and e-Commerce software and other security products, eliminating the need for you to upgrade other parts of your network to add Web fraud detection.

### Case Management and Reporting

Organizations can input "truth data" based on actual results, manage individual user profiles, and examine cases awaiting review. Using simple point-and-click screens, analysts can prioritize and take action on cases, query fraud data and manage

alerts. RiskFort provides an audit trail that annotates each recommended action.

RiskFort has a powerful reporting module and includes a set of built-in reports. These reports include statistical summaries and detailed case analyses. The reports can be viewed on the screen and exported for further analysis. The reporting module runs in an offline database in a data warehouse configuration minimizing impact on the risk assessment system. It also includes a built-in authorization model that provides fine-grained access control for each report.

### Collaborates With External Fraud Systems

RiskFort can callout to an external system to validate or augment its own risk assessment. You can also aggregate scores from multiple systems to generate one combined score. For example, a user normally resident in Los Angeles may be logging in from New York – a suspect transaction. But the callout to a credit card authorization system may show "card present" transactions in New York that will confirm that the user is in New York and therefore reduce the risk of the online access.

### Optional Anti-phishing and Keystroke Logging Protection

Arcot provides a personal assurance message or image to allow users to verify that they are logging into the legitimate site. With the Scrambled PIN Pad, organizations can provide a virtual key pad for users to enter their PIN. Because the number pattern can change every time the user logs in, keystroke and mouseclick logging can be thwarted.

For more information, please visit [www.Arcot.com](http://www.Arcot.com), email [sales@arcot.com](mailto: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](http://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.