PRODUCT SHEET:
CA Arcot RiskFort

CA Arcot RiskFort

CA Arcot RiskFort™ provides real-time protection against identity theft and online fraud via risk–based, adaptive authentication. It evaluates the fraud potential of online access attempts (including everything from enterprise online services to consumer e-commerce transactions) and calculates the risk score based on a broad set of variables. All of this is done transparently without inconveniencing legitimate, low-risk users.

Overview

Identity theft and online fraud are both an organizational and individual problem. Attacks are becoming more sophisticated and organizations are trying to find a good balance between the strength of security necessary and the level of inconvenience for their employees, partners and customers. It is important to have the ability to use risk-based rules and parameters and analytical modeling techniques that can reduce your exposure to fraudulent activity without annoying end users or creating a high rate of false positives. CA Arcot RiskFort is a flexible tool that can help you block fraud in real-time.

Benefits

CA Arcot RiskFort lets you detect and block suspicious logins or transactions in real-time without affecting legitimate users. This helps reduce your fraud related expenses and protect your end user's identity. It also helps you reduce risk and meet both internal security requirements and external compliance regulations.

Challenge: identity theft

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 information from government organizations and sensitive enterprise data that is accessible online. Overbearing anti-fraud countermeasures that require repetitive user interaction can create a negative experience and affect customer loyalty. The challenge is to instantaneously detect and block fraudulent activity before fraud losses occur, without affecting or distracting legitimate users.

Solution: risk-based, adaptive authentication

CA Arcot RiskFort is your first line of defense against identity fraud. You can verify and detect suspicious activity for consumer and enterprise online services without burdening intended users. It is a robust, 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 real-time, calculated risk score users can be allowed to continue, be required to provide additional authentication credentials, or be denied access.

CA Arcot RiskFort can be used to reduce fraud and protect users from Internet attacks whether they are shopping online or accessing confidential or private information via a Web portal or application. It also provides organizations the ability to determine and enforce different levels of authentication based on the acceptable amount of risk for the given transaction. Based on a risk score and company policies, organizations can enforce other forms of strong authentication, including the use of CA Arcot WebFort®, depending on the user and the type of desired transaction. CA Arcot RiskFort can be deployed on the customer's premise or be consumed from the cloud as a cloud security service.

Measures risk in every transaction: CA Arcot 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 CA Arcot 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 the flexibility to determine the response to that score based on your policies and risk tolerance.

Multi-component risk assessment: CA Arcot RiskFort combines multiple components for a broad range of 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 network members
- Callouts to other internal or external fraud analysis tools

Sophisticated fraud modeling techniques: The CA Arcot 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. CA Arcot RiskFort periodically updates the formula based on recent fraud and transaction data. The rules engine can also trap outliers that are not yet part of any trend.

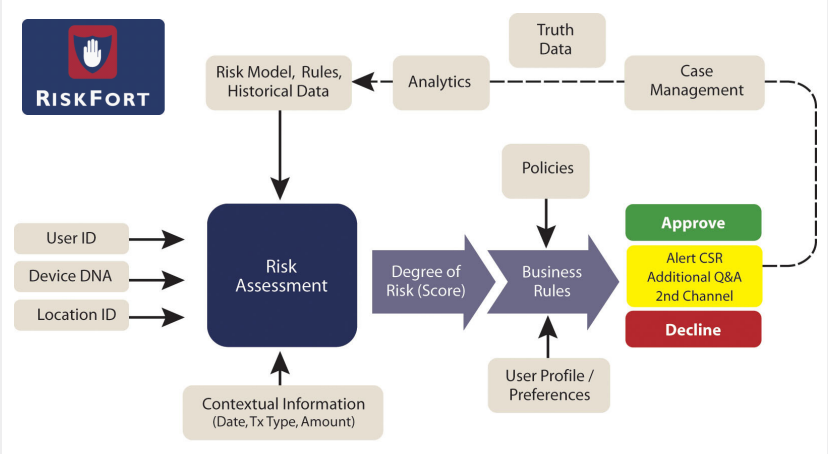
Field-programmable rules engine: You can build rules that are specific to your policies and environment and combine rules based on a wide range of transaction and session criteria. You can add or change rules on the fly when policies change. The rules engine consists of rules that can be combined into 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.

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. CA Arcot RiskFort provides an audit trail that annotates each recommended action and has a powerful reporting module that 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.

Collaboration with external fraud systems: CA Arcot RiskFort can call out 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.

Figure 1

CA Arcot RiskFort fraud detection and analysis process



Integration with CA SiteMinder®: Integration between CA Arcot RiskFort and CA SiteMinder simplifies the deployment of risk based, adaptive authentication in your environment. CA Arcot RiskFort capabilities or services are visible within the CA SiteMinder policy management interface and can be applied to a select set of applications and users or across the entire enterprise SiteMinder community. These powerful advanced authentication processes can be configured within the SiteMinder environment for the initial user authentication, step-up authentication for sensitive applications or specific SSO zones.

Easy integration with CA Arcot WebFort multi-factor authentication: CA Arcot RiskFort integrates with CA Arcot WebFort, Arcot's software-only multi-factor authentication solution. WebFort helps you to upgrade your users to strong authentication without expensive hardware, changes to your users' behavior, or changes to your critical business processes.

In the cloud or on-premise deployment options

CA Arcot RiskFort can be deployed as a cloud service or can be installed on-premise. When deployed in the cloud you can eliminate the headaches associated with installing hardware and

software on-site which can reduce cost and management overhead. Arcot has been offering cloud authentication services since 2000, and today, Arcot's cloud computing services serve over 70 million users, worldwide. Hosted in multiple SAS 70 Type II audited, PCI DSS-compliant data centers, Arcot services are highly scalable, configurable, and multi-tenant efficient.

Business benefits

Reduce losses due to fraud: CA Arcot RiskFort helps prevent fraud losses by blocking high-risk transactions before they complete, or requiring additional authentication for unusual or suspicious transactions. In ePayment environments, CA Arcot RiskFort interacts with the Arcot TransFort 3-D Secure compliant solution to help reduce the risk of fraudulent cardholder transactions. In consumer and enterprise Web and remote access situations, CA Arcot RiskFort interacts with CA Arcot WebFort Versatile Authentication Server to implement step-up authentication when encountering a suspicious transaction. CA Arcot RiskFort also works with third party fraud prevention solutions.

Address regulatory requirements: CA Arcot RiskFort helps you to meet a number of government and industry regulations for protecting access to data, including FFIEC, HIPAA, and SOX as well as your own internal security requirements.

Protect existing infrastructure investment: You can integrate CA Arcot RiskFort with any Internet-facing application via an API. It enables you to add real time fraud detection to existing business processes and applications. CA Arcot 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.

Match rules to your environment: The customizable rules engine enables you to configure CA Arcot RiskFort to match your business practices and risk tolerance, rather than forcing you to change your operations to fit your security tool. This allows you to reach the appropriate balance between the strength of your security and the impact on the end user.

Deploy and use multi-factor authentication invisibly: Your Web users never have to know that you upgraded them to multi-factor authentication, unless you want them to. They can keep the same username/password sign-on experience with which they have become so accustomed. CA Arcot 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 or additional support costs.

The CA Technologies and Arcot advantage

Arcot, a CA Technologies company, delivers additional identity protection for your Web applications and portals. Whether you want integrated multi-factor authentication, transparent risk-based authentication, or both, Arcot's authentication expertise adds additional protection to your critical data and applications. CA Arcot RiskFort can efficiently add adaptive, risk-based authentication to your CA SiteMinder protected Web applications and portals, without changing your users' familiar username/password sign-on process. Arcot's flexible, software-only approach gives you the right balance of cost, convenience, and strength for enhancing the protection of your Web resources and the identities of your Web users.

CS0070_1110