TECHNOLOGY BRIEF

Integrating Arcot Multi-Factor Authentication & Fraud Prevention With CA Siteminder | November 2010

integrating Arcot multi-factor authentication and fraud prevention with CA SiteMinder

Matthew Gardiner
CA Security Management

table of contents

executive summary

Challenge

It is no secret that while the Web has literally transformed our business and social life, it has also opened up new avenues of attack for both malicious insiders and outsiders. As we have moved more of our life online, from financial transactions to social interactions, it is remarkable that the number and impact of data loss and identity theft hasn't been even greater. However as technology and automation advance it does so equally for both the good guys and the bad ones. Thus the security situation might get worse before it gets better. The challenge we face is how to provide strong security that is also cost effective and easy to use such that it can be deployed to the masses.

Opportunity

It is widely recognized in the security community that passwords have outlived their usefulness as sole factors of online user authentication. Excessive dependence on them is the root cause of many prevalent security weaknesses. This has been known for many years. They are simply too easy to guess, give away, write down, or lose. In addition, traditional forms of strong authentication that have reached a limited level of popularity are very costly and difficult to manage and use. Now there is a solution that combines high-security and user convenience at a reasonable cost.

Benefits

The benefits of using CA Arcot WebFort® (WebFort) and CA Arcot RiskFort™ (RiskFort) or the CA Arcot A-OK™ (A-OK) equivalent cloud security services with CA SiteMinder® are clear. The combination of these market leading security products makes the Web environment that is protected by them, more secure, less costly to manage, and easier to access. No longer does the use of strong authentication need to be limited to only small portions of an organization's users. With this integrated solution strong security can be provided to everyone.

Section 1:

The online need for advanced authentication and fraud detection

Web security and the futility of passwords

It is no secret that while the Web has literally transformed our business and social life, it has also opened up new avenues of attack for both malicious insiders and outsiders. As we have moved more of our life online, from financial transactions to social interactions, it is remarkable that the number and impact of data loss and identity theft hasn't been even greater. However as technology and automation advance it does so equally for both the good guys and the bad ones. Thus the security situation might get worse before it gets better. The answer is not clear. How many security breaches occur which are never found or reported? Are organizations staying ahead of the online risk curve?

All serious Web security experts agree that to make the future better than the past, more must be done to improve the security of online systems. If existing, proven security technologies were deployed more widely, the security posture of organizations on the Web overall would improve. This brings us to the username/password. Is there a more used yet more disdained means for authenticating a person online? Security professionals as a rule dislike passwords because they are too weak. Users dislike them because they are too cumbersome and they have far too many of them. As a profession, the security industry has been stuck with username/passwords for far too long. It is a key attack vector that marries the system's weakest link, the people, with an equally weak mitigation, a single factor shared secret that people must remember.

While important progress has been made over the past years with stronger forms of user authentication, perhaps most prominently leveraging "something you know" with improved knowledge-based authentication and "something you have" via various types of one-time-password (OTP) tokens and USB devices, nothing has hit the mark for cost, strength, and convenience that is necessary for mass-scale Internet communities, until now.

Arcot® Systems, recently acquired into the security business of CA Technologies, has been a key market and technology leader in the area of user authentication and online fraud prevention since its founding in 1997. Two mainstays of Arcot's user authentication portfolio are WebFort and RiskFort (when delivered via cloud services these products are labeled "A-OK"). Simultaneously over this same time period, from 1997 to the present, CA Technologies became a leader in Web security management, in particular with the CA SiteMinder® family of products.

CA SiteMinder not only largely defined the product category known as Web access management, but as a result of its capabilities, performance, and reliability has earned its position as protector of some of the largest consumer and enterprise Web sites in the world; many with more than 10 million users. Is it any surprise that the leaders in advanced user authentication and online fraud prevention and Web access management would join together to take on online fraud and identity privacy and cross-domain portability?

The remainder of this technology brief focuses on the "how" and "why" of using Arcot's solutions, in particular WebFort and RiskFort, to complement deployments of CA SiteMinder. This brief covers both the on-premise as well as the "from the cloud" deployments of the Arcot security systems.

Section 2:

Introduction to CA Arcot WebFort, CA Arcot RiskFort, CA SiteMinder and their complementary value

CA Arcot WebFort and CA Arcot RiskFort: Natural Complements to CA SiteMinder

Before getting into how the Arcot and CA SiteMinder solutions work together it is important to understand the basic capabilities of each individual product. The descriptions below are purposely in summarized form and are not intended to replace the product's individual collateral and documentation. If you want to learn more about the individual products themselves please see the product specific sources.

What is CA SiteMinder?

CA SiteMinder provides a centralized security management foundation that enables the secure use of the Web to deliver applications and cloud services to customers, partners, and employees.
CA SiteMinder is a Web access management system, and as such it enables Web single sign-on (SSO), centralized user authentication and authentication management, policy-based authorization, enterprise-level manageability, auditing, and reporting. CA SiteMinder is used to protect some of the largest Web sites and portals in the world. From the point of view of particular authentication technologies other than username/password, CA SiteMinder provides the point of integration and management through which specific authentication technologies can be used for login to some or all Web applications and user communities that CA SiteMinder is being used to protect. With the use of CA SiteMinder, integration of the individual authentication technology with the underlying application is not necessary. Through the use of SSO and policy-based authorization, a single user login enables the user to get access to all the applications for which they are entitled. For the purposes of this paper CA SiteMinder is presumed always to be deployed within the enterprise and on-premise.

What is CA Arcot WebFort?

CA Arcot WebFort is a software-only versatile authentication solution that protects and verifies Web users' identities. It protects customers, partners, and employees from identity theft, fraud, and man-in-the-middle attacks with a variety of authentication methods, including ones that are unique to the Arcot solution. WebFort provides and supports a number of authentication mechanisms; including the use of the ArcotID secure software credential and the ArcotOTP mobile application, which leverages the user's mobile phone as a factor of authentication through the generation of a one-time password (OTP). Both ArcotID and ArcotOTP make it simple for users to adopt strong authentication without the need to change their familiar username/password-based sign-on experience. ArcotOTP runs the iPhone,

Android, Blackberry and other mobile devices that support Java ME. WebFort can be deployed on the customer's premise or be consumed from the cloud as a cloud security service. When deployed "from the cloud" it is referred to as being part of the Arcot A-OK Cloud Service.

What is CA Arcot RiskFort?

CA Arcot RiskFort is a fraud detection and risk-based security system that prevents fraud in both consumer and enterprise online services. It 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. RiskFort measures and blocks fraud in real-time as part of the authentication process without requiring input from the users. It also provides organizations with the ability to determine and enforce different levels of authentication based on the acceptable amount of risk for a given transaction. Based on a risk score and organizational policies and by leveraging its integration with WebFort, organizations can enforce the use of stronger forms of authentication as desired. RiskFort can be deployed on the customer's premise or be consumed from the cloud as a cloud security service. When deployed "from the cloud" RiskFort is also referred to as being part of the Arcot A-OK Cloud Service.

Using Arcot WebFort and RiskFort together with CA SiteMinder

In addition to providing out-of-the-box support for the use of username/passwords and directories, CA SiteMinder has had long standing support for the use of whatever alternative authentication scheme the customer desires. Over the years nearly every available form of authentication technology has been used with CA SiteMinder, covering all the traditional areas of "what you know, what you have, what you are". With the latest generation of more cost effective strong authentication technologies, best represented by CA Arcot WebFort and CA Arcot RiskFort, and the rapid acceptance of cloud delivered security solutions, the time is now ripe to address the strong authentication needs of sensitive data and applications that are in use by mass CA SiteMinder user communities.

While most organizations using CA SiteMinder have used strong authentication for some users for many years, most have not applied these to their entire user communities. This is largely due to the high cost and inconvenience of traditional strong authentication technologies. The combination of CA SiteMinder and the Arcot security solutions overcome these barriers and deliver an integrated solution that can provide effective security for the masses.

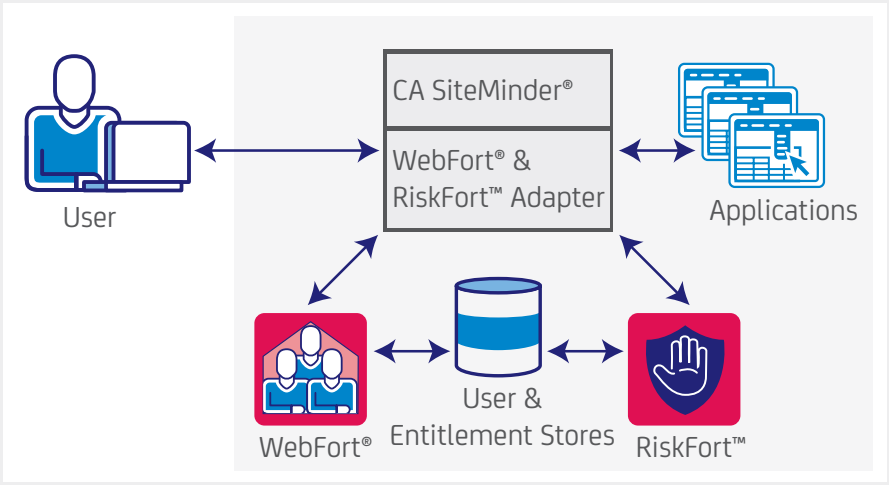
Arcot WebFort and RiskFort can be used separately or together to add fully software-based multi-factor authentication and risk analytics to a CA SiteMinder protected Web environment. As a result of their integration with CA SiteMinder, WebFort and RiskFort become authentication services visible within the CA SiteMinder security policy management interface. With this integration with CA SiteMinder the Arcot products can be used to enhance the security for a subset of users and applications or for the entire CA SiteMinder protected user community.

As a result of the integration with CA SiteMinder, WebFort and RiskFort are available for initial user authentication and step-up authentication, to be applied against specific SSO Zones, and to be used in conjunction with the authentication levels of CA SiteMinder. Also, as a result of ongoing integration work, RiskFort generated risk scores will be available for use within CA SiteMinder authorization policies. With the availability of WebFort and RiskFort with CA SiteMinder, the use of simple username/passwords can be a security approach of the past.

Figure 1 below shows a high-level diagram of the simultaneous use of both WebFort and RiskFort with CA Siteminder. In the remainder of the technology brief I will discuss in more detail how CA SiteMinder works with both WebFort and RiskFort in both on-premise and from the cloud (A-OK) deployments.

Figure 1.

High-level view of using CA SiteMinder with WebFort and RiskFort



Section 3:

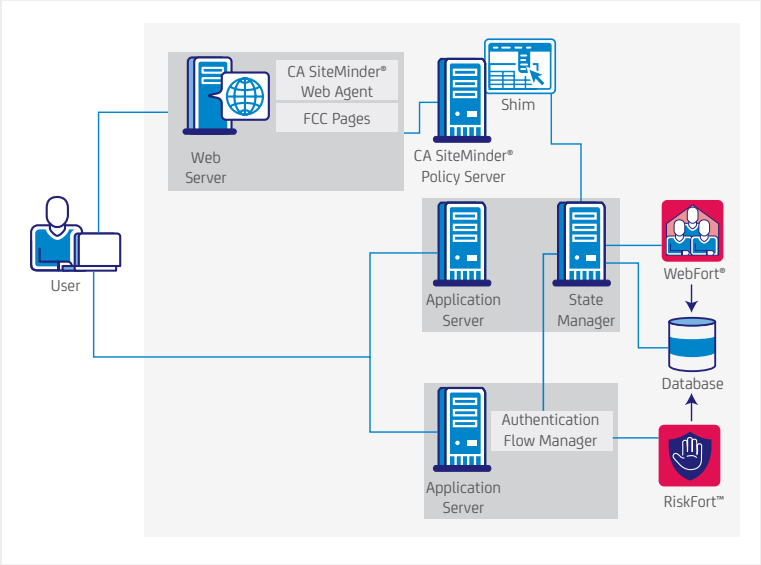
Integration of CA Arcot WebFort, CA Arcot RiskFort, and CA SiteMinder

How the integration works when deployed fully on-premise

In this section I will review the architecture and function of the Adapter which is the name of the software system which serves to integrate both WebFort and RiskFort with CA SiteMinder. To interoperate with CA SiteMinder the Adapter uses the Authentication API of the CA SiteMinder Policy Server and as a result becomes an available authentication scheme for use within the CA SiteMinder security domain. Please reference Figure 2 on the next page when reading the description of how the Adapter works.

Figure 2.

Architectural diagram of the integration of WebFort/RiskFort and CA SiteMinder



The main functional components of the Adapter are the:

- **State Manager.** The State Manager is responsible for creating, maintaining, and tracking the tokens and authentication information used to associate the logon session's authentication and risk status across the system. The tokens, which contain the information about the user and the session state, enable the other Adapter components to remain stateless. The State Manager also acts as a proxy to RiskFort by providing risk evaluation services to other system components. The State Manager receives the risk evaluation input parameters from the calling application and passes it to RiskFort for analysis. After the risk evaluation is complete, the State Manager inserts the result of the risk evaluation into the token for further examination or for processing by other components of the system.

  Based on the customer's particular requirements, risk evaluations can be performed before or after the initial user authentication. If the risk evaluation takes place after the initial user authentication, then the result of the authentication is persisted in the token before the risk evaluation is performed. The State Manager also provides a token validation mechanism to securely communicate the authentication and risk results to CA SiteMinder via the Shim (discussed below).

- **Shim.** The Shim integrates directly with CA SiteMinder's Policy Server via the Policy Server's Authentication API and acts as the interface between CA SiteMinder and the other Adapter components (State Manager and Authentication Flow Manager). Both WebFort and RiskFort, whether deployed individually or together, are integrated with CA SiteMinder through the use of the Shim. The Shim is an instance of a shared library and resides in the CA SiteMinder Policy Server instance.
- **Authentication Flow Manager.** The Authentication Flow Manager (Flow Manager) is the only component (along with FCC pages discussed below) of the Adapter that a user interacts with directly. It is a state machine that guides the end user through the authentication process, risk evaluation process, or both, by presenting Java Server Pages (JSPs) to collect the required information from the user. The Flow Manager also maintains the state data of the user flow, orchestrates WebFort authentication (the user ceremony), and reads or writes information (specifically the RiskFort DeviceDNA™) required by RiskFort. It should be remembered that not all security activities require user input. For example, risk assessments can be done without any user input. In addition to the four sample authentication flows with which the Flow Manager is shipped, it also provides the capability to customize an authentication flow to meet the organization's requirements.
- **Form Credential Collector (FCC) Pages.** FCC pages are the static HTML pages orchestrated by the Flow Manager to collect user inputs during basic or primary authentication and to display error messages, if any. These pages are deployed on the same Web servers where the CA SiteMinder Web Agents reside.

In this sub-section I will walk through a typical strong authentication flow.

Typical Workflow

The following steps describe the steps for user authentication and risk assessment of a Web transaction which uses CA Arcot WebFort, CA Arcot RiskFort and CA SiteMinder:

1. The user accesses a Web resource that is protected by CA SiteMinder.
2. Assuming that the user does not have a current CA SiteMinder session (as typically represented by a valid browser session cookie), CA SiteMinder performs user disambiguation by checking to see which user the userid belongs to in the set of CA SiteMinder connected user directories.
3. The CA SiteMinder policy determines that user authentication needs to be conducted by the Arcot solution and passes the authentication step to the Shim. The Shim redirects the user to the State Manager. The State Manager communicates with the Flow Manager, WebFort, and RiskFort. The Flow Manager guides the user through the authentication and risk evaluation process by conducting an authentication dialog with the user, for instance asking the user to answer security questions or enter a password. Flow Manager also collects information from the user's device to pass back to RiskFort for risk evaluation. The Flow Manager controls the flow of information between RiskFort and WebFort.
4. Depending on the authentication and the risk evaluation results, the State Manager saves the state of the user and securely communicates the authentication and risk results to the Shim.
5. The Shim forwards the results to the CA SiteMinder Policy Server.

6. If the user is authenticated successfully and the risk score is considered low by the organization's pre-configured risk policies, then the user is granted access to the protected resource. CA SiteMinder generates a session cookie which can then be used to enable SSO to all resources for which the user is entitled.

Section 4:

Integration between the A-OK Cloud Services and CA SiteMinder

How the integration works when delivered from the cloud

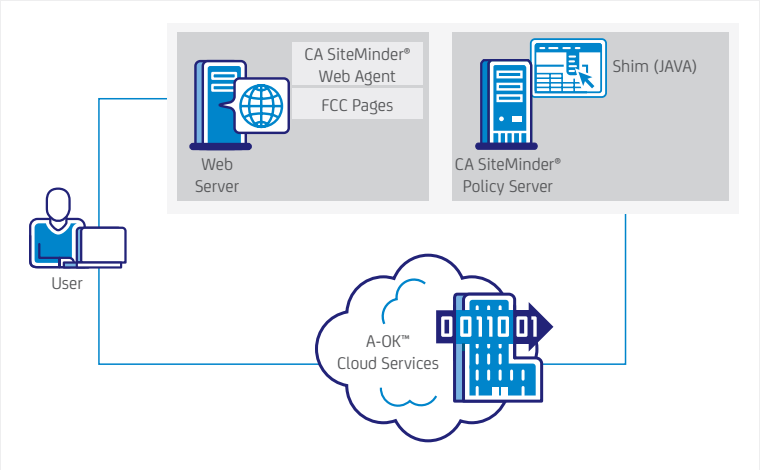
Whether deployed on-premise via locally installed software or as a security service from the Arcot A-OK Cloud Service, the core security functionality of WebFort and RiskFort remain the same. The cloud security service is made up of WebFort and RiskFort and is branded as A-OK Cloud Services. What is different is how these A-OK services integrate with an on-premise deployment of CA SiteMinder.

There are two options for integrating A-OK Cloud Services with an on-premise deployment of CA SiteMinder. The first mode is using a pure SAML-based federation between the two domains—one in the cloud (A-OK) and the other on-premise (CA SiteMinder). In federation parlance the CA SiteMinder domain in the enterprise acts as the federation service provider (SP) and the A-OK service acts as the Identity Provider (IdP). This approach presumes that CA SiteMinder has been enabled for federation using CA Federation Manager, which is the complementary identity federation product in the CA SiteMinder family of products. Using SAML-based federation with CA Federation Manager and CA SiteMinder is covered sufficiently in other documents and will not be addressed in this technical brief.

The second approach for integrating the A-OK Cloud Services into CA SiteMinder is through the use of the Arcot Shim. This approach is appropriate to use in the situation where the CA SiteMinder deployment has not yet been enabled with identity federation. In this case the function of the Shim with the CA SiteMinder Policy Server is the same as with the on-premise implementation. It is not important to CA SiteMinder whether the authentication scheme itself is operating locally or remotely in the cloud.

Figure 3.

Architectural diagram of the integration of the A-OK Cloud Services and CA SiteMinder

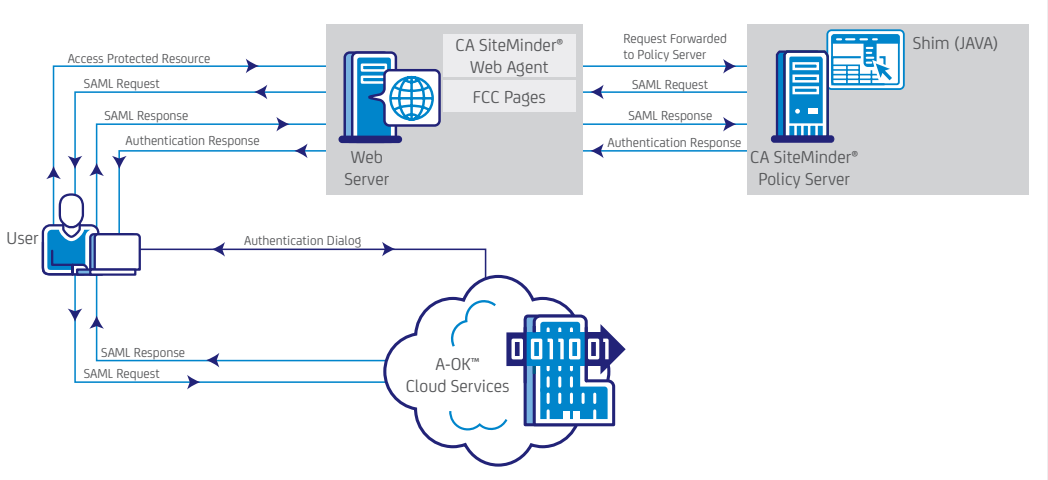


The main functional components of the integration between the Arcot A-OK Cloud Service and CA SiteMinder are:

- **Shim.** This Shim is the same one as used in the previously described fully on-premise deployment. In this case the Shim facilitates communication with WebFort and RiskFort that are operating as security services from the cloud. The Shim integrates directly with CA SiteMinder's Policy Server via the Policy Server's Authentication API and acts as the interface between CA SiteMinder and the A-OK services in the cloud. The Shim is an instance of a shared library and resides in the CA SiteMinder Policy Server instance.
- **Arcot A-OK Cloud Services.** Arcot A-OK Cloud Services are a cloud-based service delivery of the capabilities of WebFort and RiskFort.
- **Form Credential Collector (FCC) Pages.** FCC pages are the static HTML pages used by the Shim to collect user inputs during basic or primary authentication and to display error messages, if any. These pages are deployed on the same Web servers where the CA SiteMinder Web Agents reside.

Figure 4.

Functional flow of A-OK with CA SiteMinder



In this sub-section I will walk through a typical strong authentication flow that takes advantage of the A-OK security services.

1. The user accesses a Web resource that is protected by CA SiteMinder.
2. Assuming that the user does not have a current CA SiteMinder session (as typically represented by a CA SiteMinder browser session cookie), CA SiteMinder performs user disambiguation by checking to see which user the username belongs to in the set of CA SiteMinder connected user directories.
3. If the authentication is to be performed by the A-OK service as determined by the CA SiteMinder policy, the CA SiteMinder Policy Server redirects the user request to the Authentication Shim.
4. The Shim generates a SAML Request and redirects the user to the A-OK authentication URL with the SAML request in a query string.
5. The A-OK service guides the user through the authentication and risk evaluation process.
6. The A-OK service securely communicates the authentication result through a SAML Response to the Shim, which validates the SAML Response by using an appropriate certificate. After validation, it checks if the authentication was successful or not.
7. The Shim forwards the authentication result to CA SiteMinder.
8. If the user is authenticated successfully and the risk result is positive (sufficiently low risk), then the user is granted access to the protected resource. CA SiteMinder generates a session cookie which enables SSO to all resources for which he is entitled.

Section 5:

Conclusion and a peek into the future

It is widely recognized in the security community that passwords have outlived their usefulness as sole factors of online user authentication. Excessive dependence on them is the root cause of many prevalent security weaknesses. This has been known for many years. They are simply too easy to guess, give away, write down, or lose. In addition, traditional forms of strong authentication that have reached a limited level of popularity are very costly and difficult to manage and use. Now there is a solution that combines high-security, user convenience, at a reasonable cost. The benefits of using WebFort and RiskFort or the A-OK Cloud Services equivalent with CA SiteMinder are clear. The combination of these market leading security products makes the Web environment that is protected by them, more secure, less costly to manage, and easier to access. No longer does the use of strong authentication need to be limited to only small portions of an organization's users. With this integrated solution strong security can be provided to everyone.

Arcot Systems brings to CA Technologies more than just the WebFort, RiskFort, and A-OK products. Over the past 10+ years Arcot has innovated and patented many other security related technologies. These technologies (such as SignFort, SEND, ProxyFort, and RegFort) will be incorporated over the coming months into the product roadmaps of CA Technologies, both within and outside the security business. They will undoubtedly provide innovative value to our customers for many years into the future.

Finally, a key value of Arcot Systems to CA Technologies is Arcot's many years of experience building and deploying what today are called cloud delivered security services. Arcot has been providing security services from the cloud in their own managed datacenter (most notably the Verified by Visa and equivalent services for the other card networks) for many years before the term "cloud" became popular. As CA Technologies continues to expand its delivery of security services from the cloud, specifically identity, access, and governance services, both the experience and management systems developed by Arcot over the past 10+ years will be leveraged to the maximum.

Section 6:

About the author

Matthew Gardiner is a Director working in the Security business unit at CA Technologies. He is a recognized industry leader in the security & Identity and Access Management (IAM) markets worldwide. He is published, blogs, and is interviewed regularly in leading industry media on a wide range of IAM, cloud security, and other security-related topics. He is a member of and current president of the Kantara Initiative Board of Trustees. Matthew has a BSEE from the University of Pennsylvania and an SM in Management from MIT's Sloan School of Management.

CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and distributed, to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 rely on CA Technologies to manage their evolving IT ecosystems. For additional information, visit CA Technologies at ca.com.

CS0171_1110