



ARC Application Independent Access Control

White paper



Teamsoft Technologies
4677 Old Ironsides Drive, # 410
Santa Clara, CA 95054
Phone: (408) 970-4720
Fax: (408) 970-4719
www.teamsofttech.com

CONTENTS

SECURED DATA SHARING 4

<i>Secure Data Access during Client/Server era</i>	5
<i>WEB as De facto Platform Standard</i>	5
<i>TCP/IP protocol: the foundation of Internet</i> 5	
<i>Limitations of HTTP protocol</i> 6	
<i>Start of the security leak</i> 6	
<i>Present Chaos</i>	7

THE OPPORTUNITY 8

<i>The market pull</i>	8
<i>The right technology</i>	9

ARC TECHNOLOGY 11

<i>Data Retrieval in Typical IT Environment</i>	11
<i>Conventional implementation of access control</i>	13
<i>Why are current access control mechanisms inadequate</i>	14
<i>How ARC handles it</i>	15

ARC PRODUCT FAMILY 18

<i>ARC Wall</i>	19
<i>Zero administration appliance</i> 19	
<i>Application independent access rules</i> 19	
<i>Risk free</i> 20	
<i>ARC Logger</i>	20
<i>Zero administration appliance</i> 20	
<i>Easy configuration for HIPPA and Sarbanes Oxley compliance</i> 21	
<i>Zero overhead auditing</i> 21	
<i>ARC MIS Server</i>	22
<i>Safer replacement to report writers</i> 22	
<i>Choice to get back your decades of IT investments</i> 23	
<i>All in one functions</i> 23	
<i>ARC EAC Server</i>	23
<i>Secure aggregated access to multiple diverse data sources</i> 23	
<i>Application independent access rules</i> 24	
<i>HIPPA and SOX friendly</i> 24	
<i>ARC VDWH</i>	25
<i>Virtual aggregation rather than redundant physical copy</i> 25	
<i>Schema mapping, composite and qualified queries</i> 25	
<i>HIPPA and SOX friendly</i> 26	

ABSTRACT

The need of secure aggregated single point access to the distributed and diverse corporate databases has created a strong market pull for a product that can provide such access to the stake holders including employees, customers, business partners and vendors.

The conventional solutions by industry stalwarts are technology intensive, have heavy foot prints and long and involved implementation schedules. This results in high total cost of ownership in terms of implementing and maintaining the technology making these solutions cost prohibitive for many. Even then the dream of providing right information at the right time to the right person in the right format remains elusive.

ARC technology offers a product suite that is extremely thin, light weight, high performance, orders of magnitude cheaper and extremely scalable with a potential of quickly becoming the industry standard data platform. ARC access control satisfies the real life need of role based security to the extent necessary today that conventional tools fail to provide.

The urgent needs of the two biggest buyers in the industry, large corporations and large enterprise software vendors, are met too closely to believe making ARC a unique and must have technology especially for people looking to be HIPPA and SOX compliant.

This white paper by Teamsoft Technologies covers the data sharing challenges faced by corporations and their software vendors and the way ARC based solutions can help them meet those challenges at fractions of the cost of conventional solutions.



Secured data sharing

Exploding business need of data sharing, emerging diverse technology platforms and dire consequences of data theft has created new challenges for CIO.

Increasing demands for sharing the corporate data are compelling CIO's to grant access of data to various users such as employees, customers, vendors and public over the web. The problem of securing this data access is exacerbated by the fact that corporate data is geographically dispersed, resides on diverse platforms running different relational and non relational databases, is connected over diverse communication links and receives constant updates from different enterprise applications running round the clock.

Implementation of any scheme to grant access using conventional tools is associated with a compulsory risk of exposing the database to unauthorized and unintended access at all levels. Aggregation of this data by storing it at a single place is needlessly expensive, complex, cumbersome and unsafe because aggregated data stored at one location makes it a lucrative coffer that can be easily stolen. Access provided through third party reporting tools is fraught with risk of unintended exposure because the tools connect directly to the database thereby bypassing the application level security and access control mechanism.

Secure Data Access during Client/Server era

During the eighties, emergence of Client/Server as the platform of choice was a paradigm shift and added a new dimension of complexity to data security mechanisms. Information system components were distributed beyond the scope of individual machines and their operating systems.

Suddenly the operating system level access control was found to be inadequate and was replaced by parallel user/role definitions, role based access control and security logic at database as well as application level. Simultaneous use of more than one databases and enterprise applications made it a complex affair to implement and to maintain security rules because the same rules had to be defined and maintained at multiple places using individual tools mechanisms. This created unnecessary redundancy within an organization.

WEB as De facto Platform Standard

The next revolution saw the rise of the Internet as the de facto platform during the mid-nineties. Although WEB enabling means different things to different industry segments this document concerns WEB porting needs of the sectors using business application software as the essential equipment for their business. The popularity of the Internet has forced every business to not only WEB enable their legacy applications to make them accessible to direct and indirect users from anywhere but also to develop new WEB based applications to conduct business on Internet directly with the consumers (B2C applications) or with the other businesses (B2B exchanges).

TCP/IP protocol: the foundation of Internet

The foundation of Internet is the TCP/IP protocol and the HTTP server (popularly known as web server) over it. The HTTP protocol was designed for the simple purpose of serving static HTML pages in a request–response mode. The pages normally are woven in a simple directory structure and linked with one

another using hyperlinks. It was kept session less to be able to serve larger number of simultaneous requests.

Limitations of HTTP protocol

By the time overly enthusiastic businesses realized that the session less protocol and the hypertext markup language posed such severe limitations if used for handling business transactions and implementing business processes they had already spent and committed mega budgets on such project to stay ahead of the race of transforming their business to WEB. The protocol remains too deeply entrenched in existing use to be adequately amended. Most of such efforts like Banyan VINES, DCOM, etc have failed to become as popular as HTTP on TCP/IP.

Start of the security leak

CGI and application servers were introduced to enrich the functionality of web pages and improve the WEB enabled business processes. Instead of mitigating the security problem they worsened the situation by indirectly opening up a back door through which an application program can be executed on a server and uploaded from and to other servers too. The threat has been amplified by the ease with which boundless number of people across the globe can in principle gain access to the application server.

These limitations were initially overcome by simple programming extension languages like perl, Ihtml, Pythons etc. In due course more sophisticated extensions were devised at the back end of the web server in the form of application servers with session management, transaction handling, distributed computing capabilities and enterprise integration capabilities using popular middleware. Also sophisticated extensions were devised at the browser end in the form of plug-ins, Applets, Active X components, scripting languages like Java Script, VB script and DHTML. Additional web server extensions were designed to render more sophisticated and richer content than HTML pages viz. JSPs and Microsoft ASP. The fundamental problem of data access security remains the same.

Present Chaos

CEOs have spent millions and millions of dollars on IT infrastructures and enterprise applications that capture and input data into various systems but the delivery of the right information into meaningful report to the right person in right time is still a distant dream. Many of these CEOs look to expensive data warehousing solutions or custom applications for incorporating security rules to preserve the functionality of their expensive IT investments. Both the approaches have been found to have at least 40% risk of failure owing to the complexity and heuristic nature of real life access control rules and granularity to which the rules that can be implemented at using conventional data base queries.

Consider an enterprise with three different database types, ten different locations and 4 different applications. It currently has to implement and maintain security and access control logic at $3 \times 4 \times 10 = 120$ different places with overlapping functionality and diverse mechanisms.

A technology that simplifies the application centric approach towards data access security to more sensible data centric one eliminates this unnecessary complexity and redundancy in application of access control logic.

2

The Opportunity

"Disruption is an important characteristic of innovation... it causes losses in its path of making gains, creating the dynamism of healthy economies. In fact, the disruption caused by an innovation can bring down a whole industry, while simultaneously creating new opportunities for growth."--NSF Chief Operating Officer Joseph Bordogna.

CEOs in every industry today rely on accurate and pertinent information to make mission critical decisions about their corporations. Conventional wisdom in information system technology arena has lead to information systems that have wastefully started recording every minute event in the corporation into some database some where. Although the means of acquiring information are well established adequately secure tool to meaningfully present them to the right decision makers at the right place at the right time remain elusive. This problem exists in the same form in every industry from clothes manufacturing to car paint industry.

Opportunity exists for a technology that can inexpensively, reliably, securely and timely allow pertinent information to be presented to the decision makers in a palatable format.

The market pull

Opportunity exists for an innovative disruptive technology that can simplify data access security by virtually aggregating corporate data and allowing the application of access control logic at the data source. Large technology vendors like SUN, Oracle, Microsoft, IBM, Rational etc. will never attempt to bring

out such a simplified solution as it would be counter productive to their revenue which is generated by adding more layers of complex “solutions”.

Huge costs, increasingly long time and high failure rate in attaching layer upon layer of complex mechanisms to existing systems as part of conventional solutions has left a vacuum for a technology that can silently provide application independent access control without modifying existing systems. Such a technology is indispensable for effectively tracking and fixing security loopholes in existing systems without committing expensive changes to existing code.

Security leaks and loopholes are a product of the coarseness of the granularity to which security rules can be currently programmed in conventional tools that either exposes everything or nothing to an authenticated user. Specificity and performance requirements of real life access control logic have made a technology that allows intuitive and simple application of a consistent role-based access control policy to an arbitrary level of granularity absolutely necessary. Confidentiality protecting legislations like HIPPA and SOX have made this necessity even more urgent because such loopholes may now directly cost corporations business or expensive fines.

The right technology

Considering all the different requirements of different industries' information needs there is a strong market pull being felt for a product that can let CIOs implement the right security and data access mechanism across the corporation within following specifications.

1. It should be economical to implement and maintain.
2. It should be quick to implement and define new security rules.
3. It should permit to define real life heuristic security rules.
4. It should hide all the diversities of data sources for the information consumers making it extremely simple to gain access to right and secure information onto all popular front end tools such as MS Front page, MS Excel, MS Word, Crystal Report writer and so on.

Teamsoft has perceived this need in time and has developed the ARC technology to meet the information access security needs to every industry today. ARC technology is not only a suite of applications or appliances but a scalable technology platform upon which other security applications can be easily built.

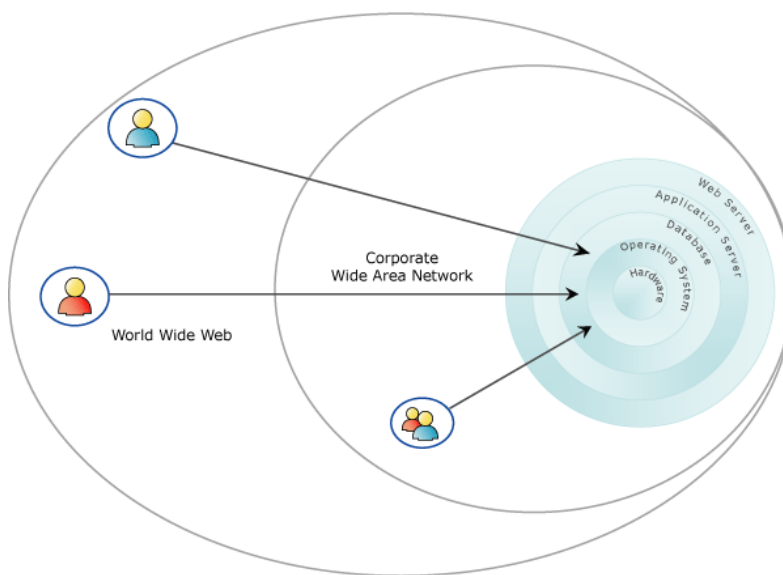
3

ARC TECHNOLOGY

“ARC (Access Right Control) is the right access control”

ARC is the only technology to provide universal data access with essential real life role-based access control without modifying existing code or infrastructure.

Data Retrieval in Typical IT Environment



Data retrieval by an enterprise application or other data consumer in a typical IT environment can be described using a layered model as shown in **Figure 1**.

Starting from the most fundamental hardware layer where the data is actually stored in the database to the World Wide Web layer where a public user is connected each layer represents another level of abstraction and software detail.

Figure 1 Layered Model of Data Retrieval in Typical IT Environments.

Corporate users like corporation employees are at the corporation WAN level and get access to the data through an application server which may be an enterprise application like PeopleSoft for example. In a typical data retrieval event a public user needs to access the corporate WAN, then the web server, then the application server which then accesses the database to retrieve the desired data from where it is stored.

Following actions should occur at the boundary of each of the layers shown in **Figure 1** as the user tries to access that particular layer in order to determine if the user should be allowed to cross that layer.

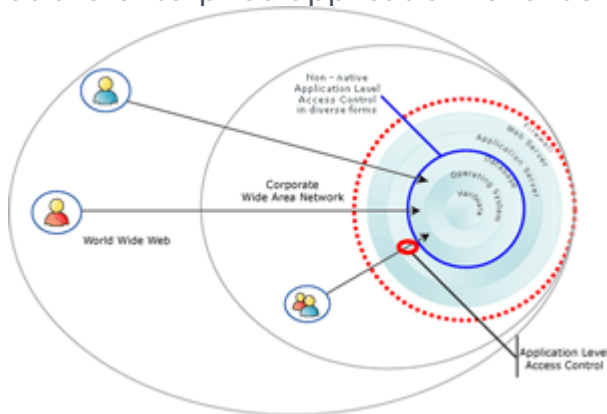
The first step involves the authentication to make sure that the users are who they claim to be usually by simple username-password verification. Next two steps involve determination of the scope of authorized access. The next step involves securing the smallest encapsulated unit of data which may be an IP packet for example through encryption. The last step involves recording the transcript of the type of access authorized during a particular event.

These steps are integral part of many classical security mechanisms. The responsibility for performing these steps and other due diligence is delegated to different components at different layer which may be an IP firewall for example as shown in **Figure 2**.

In practice the amount of detail with which these steps are performed is different at every different layer and in fact at some layers these actions are not performed at all or if performed are inadequately performed. In fact for many years the focus was limited to perimeter security at the IP and WAN level using IP firewalls solely. Access control at the database level was very much ignored or where implemented involved blanket denial or allowance of access.

Conventional implementation of access control

The conventional practice is to hard code the access control logic at the enterprise application level as shown in **Figure 2**

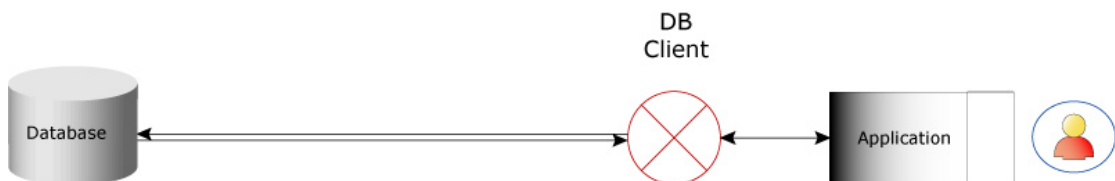


The native enterprise application has rich in-built application level access control logic which is restricted to the users that are registered in that application and connect through designated client programs of that particular enterprise application. All

other users that access data through third party tools, applications and utilities like MS Excel bypass the access control logic built into the native enterprise application.

Figure 2 Application Level Access Control

Implementation of consistent access control logic in every application is not only expensive and tedious because there are too many of these applications but also impossible because not every application allows access control with adequate or matching level of granularity. This is evident from the model shown in **Figure 3** which illustrates where a typical application connected to a database implements access control.



Typically an application authenticates the user to allow the user to send queries to the application. The application then sends these requests in SQL commands to the database and

retrieves the result. It further processes and presents the result to the end user.

Figure 3 Typical Databases –Application Communication

Notice in **Figure 3** that the access control logic is under the domain of the application and in context specific to that particular application. Also notice that no adequate security mechanism is implemented at the interface of the Db client and the database for the application user. This is even more egregious because the same Db client can connect to multiple applications simultaneously which may implement different access control logic.

Why are current access control mechanisms inadequate

Usually there are many more users that require the data and in many different format that a single or even a small number of applications can adequately serve. Application level access control logic decides who gets what so that many users whose number and diversity far exceeds the ones registered in each program are either granted false access or denied genuine access.

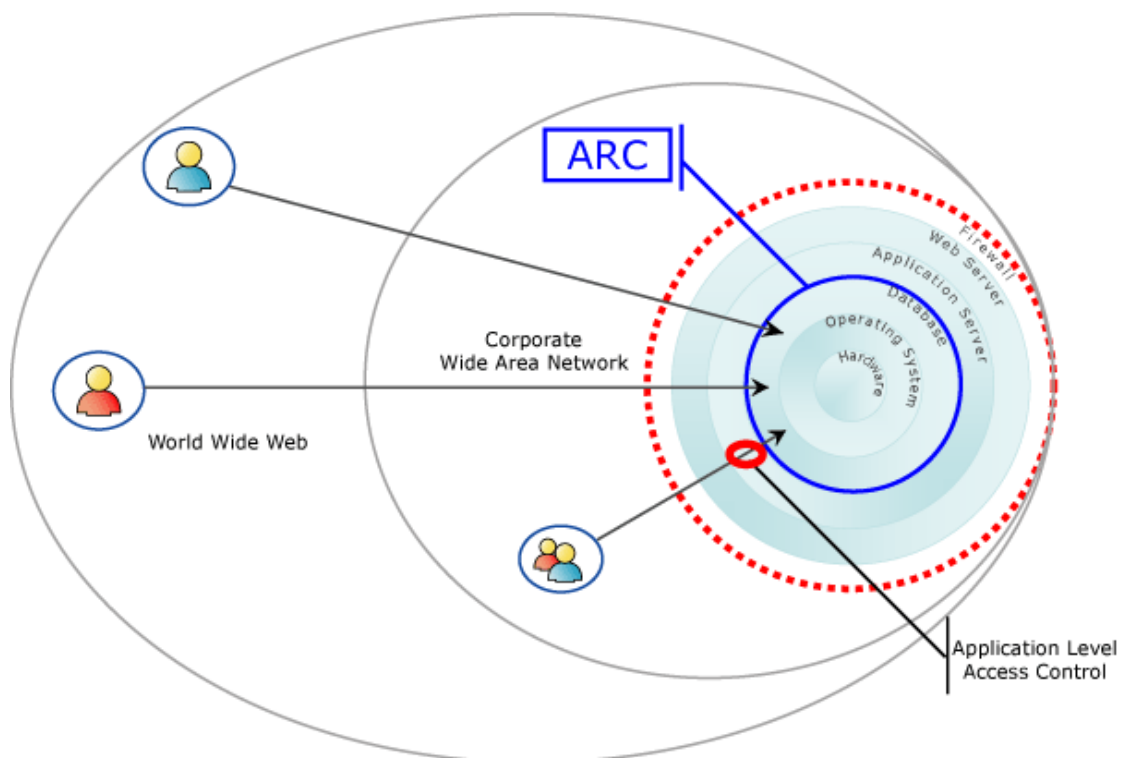
The complete access control mechanism however sophisticated is often distributed In the form of coded program logic at many layers and places and woven around user definition within the context of that specific application. An overly context specific access control mechanism prevents genuine users from gaining access while a general policy allows false users access. In the present scenario this context specificity is controlled by individual applications rather than the database and information within it that needs to be protected.

Since the same Db client serves many different applications there is no control over the SQL commands bombarding the database server from diverse sources in order to keep the data access as general as possible to serve as many users as possible. Using different Db clients would unnecessarily burden the database at the detriment of performance. DBAs resorting to role blind denial of access to all but a few applications defeat the

purpose for which IT investments were made in the first place; to provide the right type of information in the right format to the right person.

How ARC handles it

ARC technology allows implementation of a unified application independent access control policy at the interface of the database and the application layer without modifying the existing database or application as shown in **Figure 4**. The role-based access control that can be tailored to an arbitrary level of granularity is based on an asset centric approach to data security rather than perimeter centric.

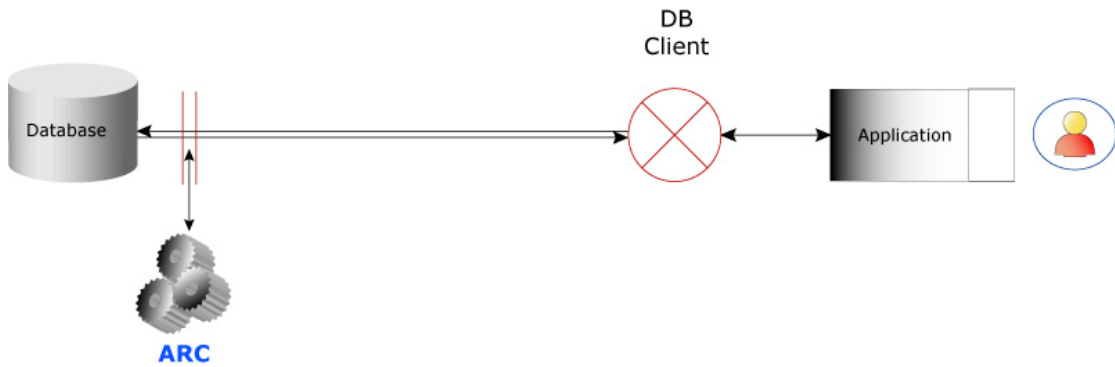


ARC acts as a universal data provider for information reporting applications such as MS Excel, Crystal Reports and Enterprise applications like PeopleSoft alike.

ARC implementation doesn't require expensive modifications in existing database or application code.

ARC access control logic can be changed in run-time without modifying the existing database or application code.

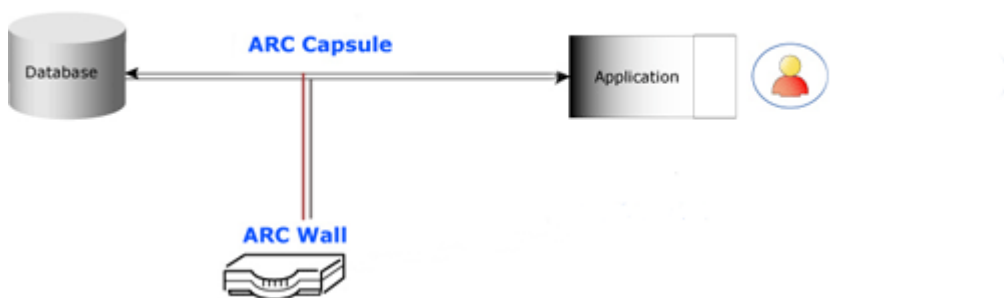
Figure 4 ARC in the Layered Model



ARC has sophisticated algorithms to enforce the access control policies without affecting the basic business logic programmed in the query.

ARC maintains the user database and schemas gathered from the information environment and let the administrator define access control policies that are used by the algorithms.

ARC technology is implemented at boundary of the database server layer using ARC server. When the same technology is deployed at the db Client level it can be contained in an appliance as shown in the following diagram.

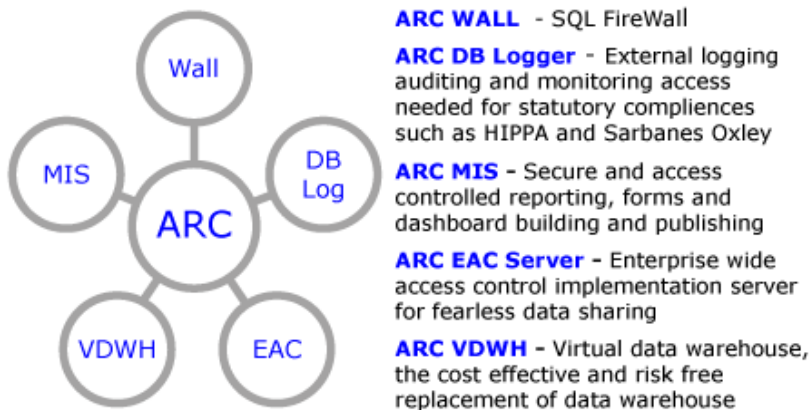


4

ARC PRODUCT FAMILY

"A new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die, and a new generation grows up that is familiar with it"--Max Planck

All ARC products are built on ARC technology for specific needs of secure aggregated single point access to the distributed and diverse corporate databases. Specific applications range from implementing HIPPA and SOX compliance to data virtualization.



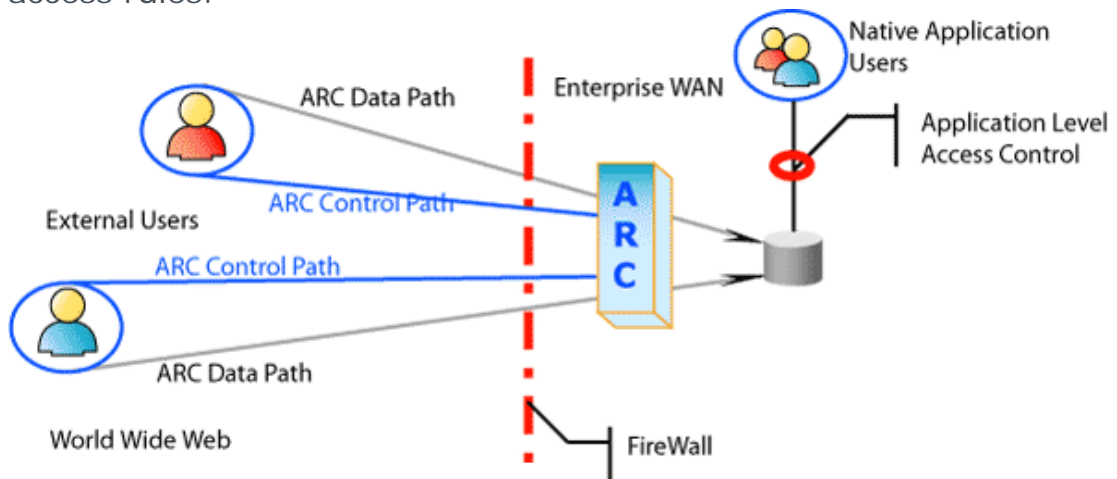
ARC Product Family

ARC Wall

ARC Wall is a SQL fire wall that protects the enterprise data when accessed by non-native data consumers such as crystal reports.

Zero administration appliance

Easy to setup ARC WALL shields the database once connected. There after it encapsulates the client libraries upon first access attempt. The protective layer, the ARC control path thus formed mandates the 'look ahead processing' of all SQL commands so as to enforce the user/role based access control as per configured access rules.



Application independent access rules

ARC Wall acquires the knowledge of the database needed by the administrator to establish the access policies on wide granularity level of tables, columns and fields using a GUI. Wild cards, group permits and access arithmetic greatly simplifies the task of emulating the real life heuristic situations.

Risk free

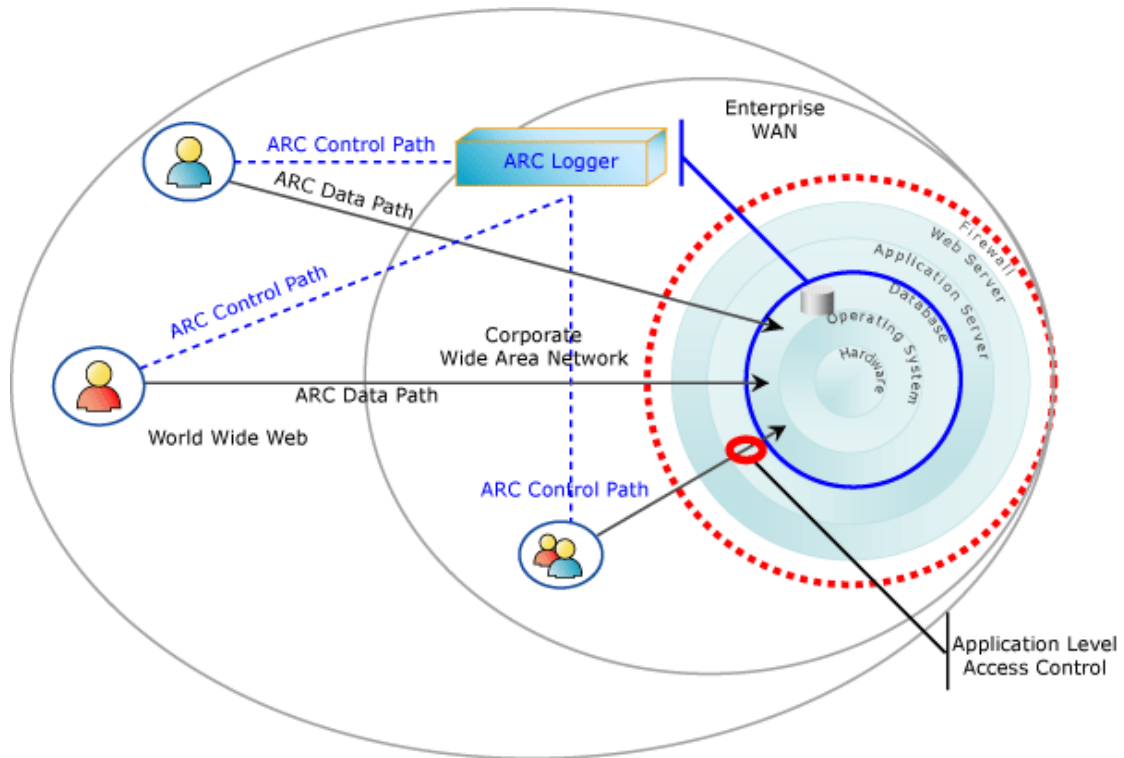
Being a thin server technology ARC WALL does not affect the application performance. ARC does not alter the basic SQL command logic nor does it poke itself between the data path.

ARC Logger

ARC Logger is a zero overhead appliance used to log useful data base parameters and activities for the purpose of alert, audit, compliance and performance optimization.

Zero administration appliance

Easy to setup ARC Logger shields the database once connected. There after it encapsulates the client libraries upon first access attempt. ARC control path thus formed intercepts the traffic and selectively logs the commands, resources and other parameters as per configuration.



Easy configuration for HIPPA and Sarbanes Oxley compliance

One can configure logging events, conditions and elements to be logged such as SQL traces, current resources, consumed resource and elapsed time. Conditions can be built around users, tables, columns and data contents.

Though the logging is distributed, structured logs are available at centralized place for useful reporting. ARC Logger's own reports offer valuable clues to performance improvements. These features are extremely useful for enforcing and auditing compliances such as HIPPA and Sarbanes Oxley without touching the existing systems.

Zero overhead auditing

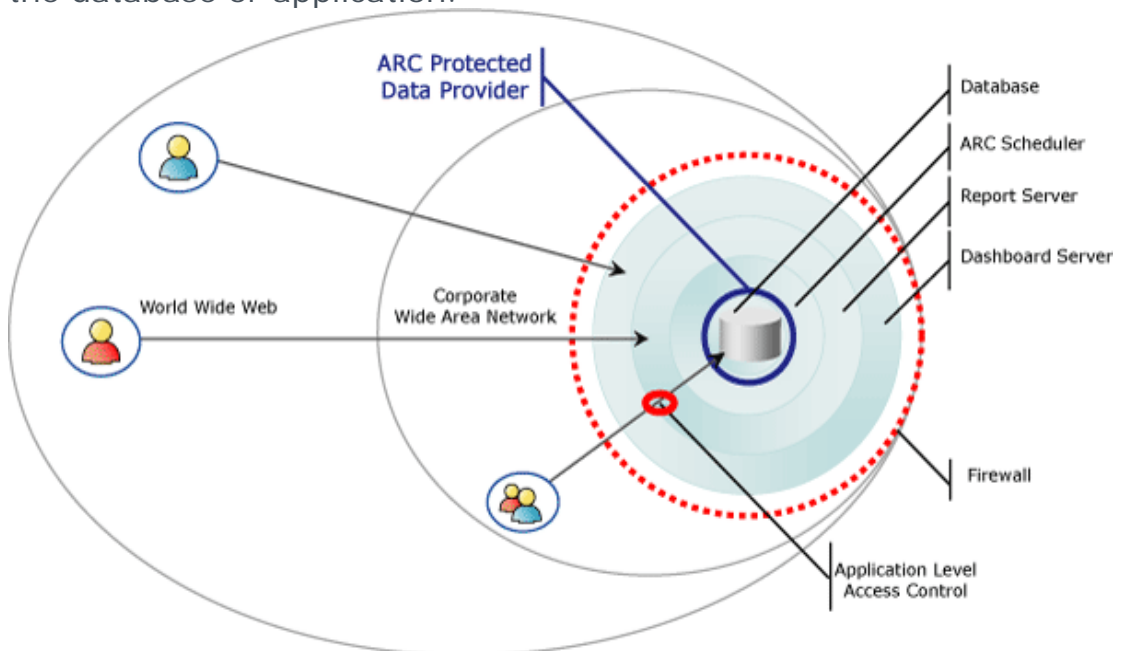
ARC Logger being a zero overhead logger is extremely useful for an overloaded database when its native features can not be enabled under given load conditions.

ARC MIS Server

ARC MIS Server is used to design and publish reports and dashboards over web with the contents modulated as per the access rights of the requesting user.

Safer replacement to report writers

ARC MIS is a suite of products that includes reports and dashboard designer, report server, dashboard server and scheduler tightly coupled to the database through ARC Protected Data Provider, the heart of the suite. Its built-in access control mechanism serves the result set only as per the access rights of the requesters. Moreover this applies to the users' non-native to the database or application.



These features are extremely useful for enforcing and reporting compliances such as HIPPA and Sarbanes Oxley without touching the existing systems.

Choice to get back your decades of IT investments

Strategic business need of data sharing has been grossly compromised due to the associated security threats keeping the decades IT investments bonded within the premise of native-application with restricted usage. ARC MIS gets them back.

All in one functions

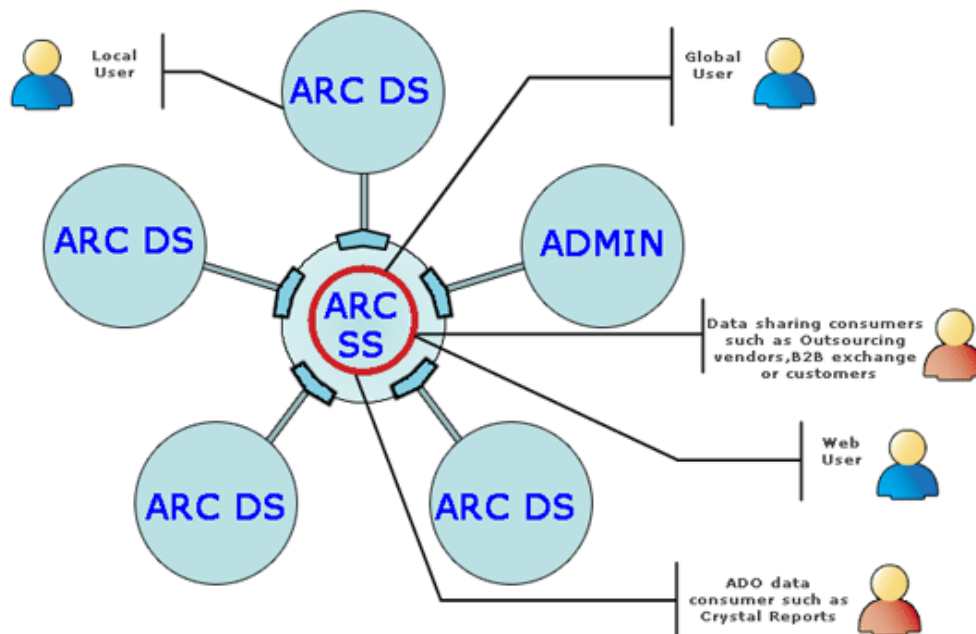
ARC MIS being the matched set of the components such as report writers, dash boards, business objects and scheduler saves the time and cost required to integrate if otherwise sourced from different vendors.

ARC EAC Server

ARC EAC Server is an Enterprise Access Control product that centrally manages secure data exchange between many diverse data sources and many diverse consumers.

Secure aggregated access to multiple diverse data sources

ARC EAC Server acts as a secure exchange between many diverse data sources to many diverse data consumers across enterprise. Though the data consumers can fire SQL queries to any of the data sources from one point, the result set served is governed by the access control policies defined for the user and the tables, columns and fields of the individual data source receiving the SQL query.



Application independent access rules

ARC EAC acquires the knowledge of all the databases connected to it. This information is needed by the administrator to establish the access policies on wide granularity level of tables, columns and fields using a GUI. Wild cards, group permits and access arithmetic greatly simplifies the task of emulating the real life heuristic situations. These policies extend to the users beyond one application and one data source.

HIPPA and SOX friendly

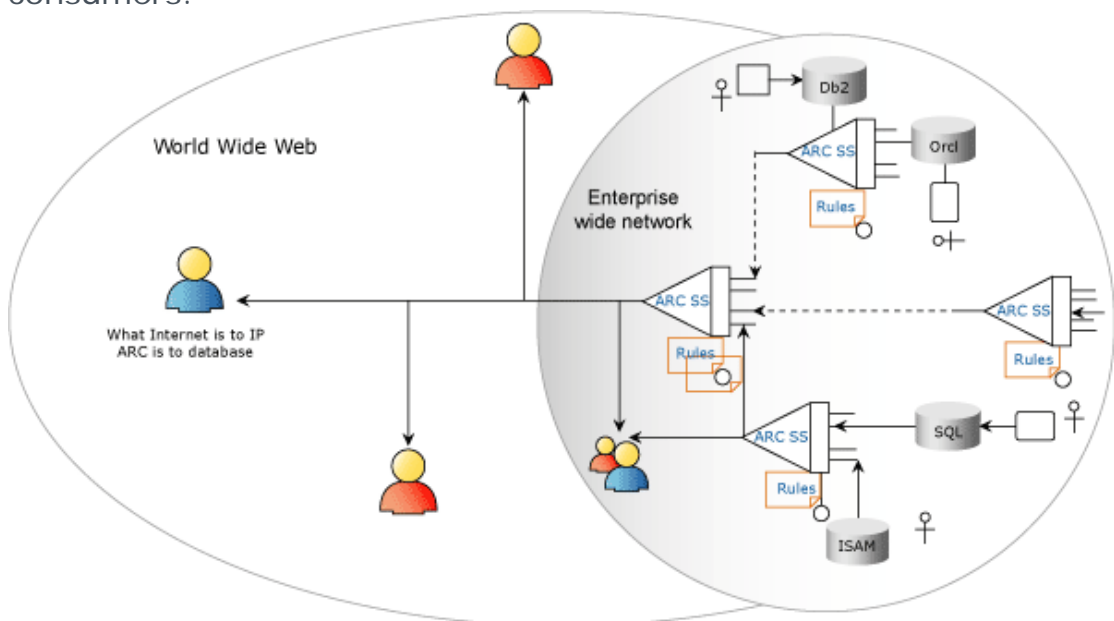
Centralized access control and reporting on access logs are extremely useful features for enforcing and reporting compliances such as HIPPA and Sarbanes Oxley without touching the existing systems and application.

ARC VDPWH

ARC VDPWH (Virtual Data Ware House) provides most needed functions of the data warehouse at fraction of the cost and time while scoring over conventional solutions by providing real-time data and low risk in implementation.

Virtual aggregation rather than redundant physical copy

ARC VDPWH is a hierarchical network of EAC servers managed by ARC Name Server that uniquely identifies the granular most data element. The node at the root of VDPWH provides connectivity to various data consumers. Those see the VDPWH as one big database containing the tables of all the member databases. The distributed processing of SQL queries is transparent to the data consumers.



Schema mapping, composite and qualified queries

Each of the ARC nodes exposes a part of schema scoped by an access control map to the next level. The composite schema at the highest level is formed by mapping the table and field names for the same data element into common user friendly names. This is used to resolve composite queries and route qualified queries.

HIPPA and SOX friendly

Centralized access control and reporting on access logs are extremely useful features for enforcing and reporting compliances such as HIPPA and Sarbanes Oxley without touching the existing systems and application.