IQware

Smart & Secure Enterprise Software

Product & Business Overview

V2.1
June 2010

TABLE OF CONTENTS

Products

IQware makes patented content delivery, presentation and management systems for multiple verticals. Content management includes medical records, pharmaceutical & demographic data, business data, command & control center data, etc. Content management also includes POS (point-of-sale) advertising, ad tracking, effectiveness monitoring. Our current verticals are Pharmacy Medication Therapy Management (MTM), health information kiosks, pharmacy fulfillment, DoD command and control centers and critical infrastructure systems. IQware sells to the regulated industries, which have the following requirements, needs and characteristics:

- Tailored, secure content management, analysis, delivery and presentation
- Interoperability and compatibility with new, emerging technologies
- Very high security with complete, tamper-proof audit trail and comprehensive reports
- Inadequate information integration due to multiple disparate IT systems and legacy IT systems
- Inadequate tracking, auditing, reporting capability
- Cannot meet compliance with existing IT systems

IQware's patented (US #7,322,028) software has three unique, differentiating and critical attributes:

- It is hacker-resistant and immune to desktop viruses
- It is rule-based so it can be changed on-the-fly and without programming
- It is interoperable so it works with all platforms, including emerging, hand-held wireless devices

Market Analysis, Description and Approach

The US market for IQware's software is $19 Billion, with a 10% growth rate (compiled from The Gartner Group, International Data Corporation and the US Department of Commerce). IQware targets the following (regulated) industry segments:

- Pharmacies (retail MTM implementation and regulatory compliance)
- Pharmaceutical production (regulatory compliance, manufacturing)
- Health care (regulatory compliance, information integration, reporting auditing)
- Federal government (communications, auditing, tracking, analysis)
- Military (DoD, information integration, analysis, reporting, C^3I)
- State/Local government (infrastructure monitoring, control and auditing)

This market need is now met by package vendors and System Integrators (SIs) writing costly, non-secure, error-prone and high-risk custom code. Competing products would have to be redesigned to effectively compete with IQware. This redesign would likely infringe IQware's patented (US #7,322,028) architecture (both US and international), a significant roadblock. IQware's "go-to-market" strategy is to cultivate relationships with key system integrators ("SIs). Here's why:

- The SI wins with IQware because it is a differentiator that can win contracts with customer base
- The SI wins with IQware because it can beat offshore competition while maintaining profit margins
- The SI wins with IQware because it strengthens relationships with customers and attracts new ones
- IQware wins because we leverages the SIs pre-existing relationships with the end user
- IQware wins because we get access to the SIs customer base
- IQware wins because we get access to the SIs pipeline
- The end user wins because the delivered system has the highest performance
- The end user wins because the system is deployed in minimum time

- The end user wins because the system has a longer operational lifetime

IQWARE'S PRODUCTS

IQware, Inc. makes industry-specific, patented (US #7,322,028) content management and delivery software, sometimes called "*Master Data Management (MDM)*" or "*Business Intelligence (BI)*" Software. Content management and delivery may include medical records, pharmaceutical data, drug interactions, demographic data, business operational data, command / control center data, etc. Content management and delivery may also include POS (point-of-sale) advertising, ad tracking, effectiveness monitoring, etc.

IQware does centrally-managed, individually-tailored, context-sensitive content acquisition, content management, content delivery and content presentation across multiple vertical markets. The software performs interactive data acquisition, analysis, reporting, auditing, presentation, mining and archiving. The unique value of IQware software is that it is secure, immune to desktop viruses, platform-independent and rule-based.

IQware's MDM/BI software translates raw data into useful information through assured, accurate interactive analysis and presentation. IQware helps convert that information into knowledge by supporting its successful application - and then by managing the results.

IQware also provides information assurance through a variety of patented (US #7,322,028) internal, secure mechanisms. Information assurance is an essential component of MDM because errors embedded in the "original content" – or in the acquired raw data – are significantly amplified and magnified by the "downstream" IT systems. Such IT systems have few reliable, independent mechanisms(s) for information verification. The consequences of such errors percolating through the organization are severely expensive at best - and fatal at worst.

IQware can acquire data from any source. This makes IQware ideal for deployment across existing and disparate IT systems. IQware's products also extend rather than compete with the functionality of traditional Enterprise Resource Planning ("ERP") systems. IQware focuses on the regulated industries, which have the following requirements and/or desires:

- Tailored, secure content management, analysis, delivery and presentation
- Information assurance and validation
- Interactive and comprehensive reports
- Interoperability and compatibility with new, emerging technologies
- Very high security with complete, tamper-proof audit trail
- Integrate information disparate IT and legacy IT systems
- Real-time (or nearly so) performance
- Inadequate information integration
- Inadequate tracking, auditing, reporting capability
- Cannot meet regulatory compliance with existing IT systems
- Cannot meet performance requirements with existing IT systems

These industries generally have one of more of the following characteristics:

- Deployment of legacy systems
- Many disparate data sources
- Multiple disparate IT systems
- Inadequate information assurance
- Inadequate information integration

- Inadequate tracking capability
- Inadequate auditing capability
- Inadequate reporting capability
- Cannot meet compliance with existing IT systems

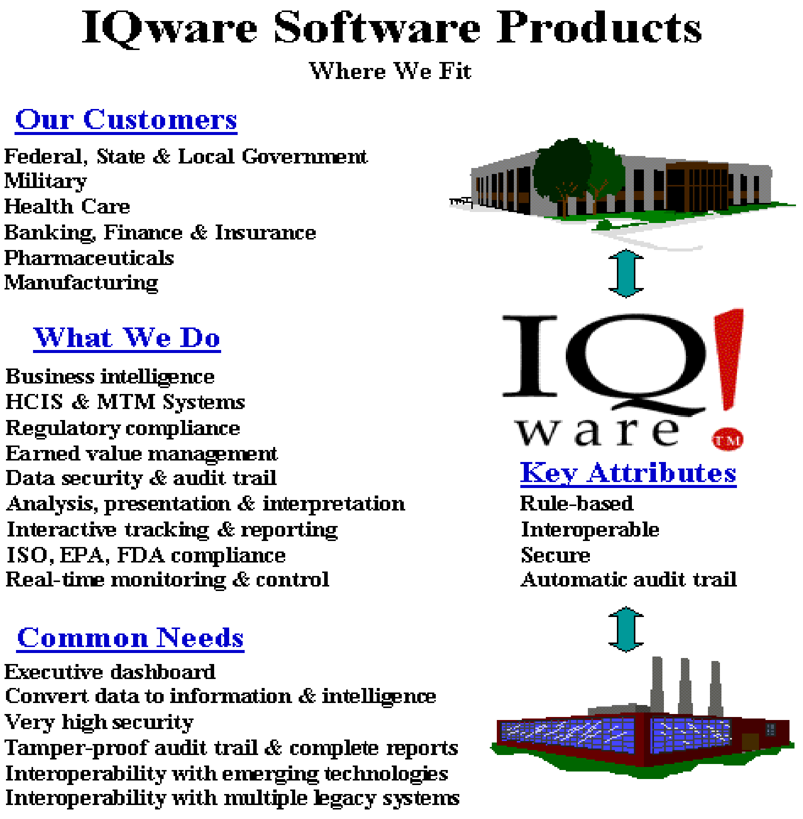
IQware's patented (US #7,322,028) software has three critical attributes:

- It is hacker-resistant and immune to desktop viruses (US Patent #7,322,028)
- It is rule-based so it can be changed on-the-fly and without programming
- It is interoperable so it works with emerging hand-held wireless devices

With heightened customer interest in IT security, IQware software provides customers a solution to secure software application requirements. The rule-based nature of IQware's products significantly reduces or eliminates the need for expensive custom code development. This unique, patented (US #7,322,028) feature allows third-party system integrators to compete effectively with ultra-low-cost offshore software developers because they can do a better job in far less time using IQware – *and* provide desktop-virus-immunity as well.

IQware's products are currently targeted toward the following industry segments:

- Pharmacies (retail MTM implementation and regulatory compliance)
- Pharmaceutical production (regulatory compliance, manufacturing)
- Health care (regulatory compliance, information integration, reporting auditing)
- Federal government (communications, auditing, tracking, analysis)
- Military (DoD, information integration, analysis, reporting, C^3I)
- State / Local government (infrastructure monitoring, control and auditing)



IQware Software Products

Where We Fit

Our Customers

Federal, State & Local Government
Military
Health Care
Banking, Finance & Insurance
Pharmaceuticals
Manufacturing

What We Do

Business intelligence
HCIS & MTM Systems
Regulatory compliance
Earned value management
Data security & audit trail
Analysis, presentation & interpretation
Interactive tracking & reporting
ISO, EPA, FDA compliance
Real-time monitoring & control

Key Attributes

Rule-based
Interoperable
Secure
Automatic audit trail

Common Needs

Executive dashboard
Convert data to information & intelligence
Very high security
Tamper-proof audit trail & complete reports
Interoperability with emerging technologies
Interoperability with multiple legacy systems

VALUE TO THE CUSTOMER - Customer "Pain" and IQware Prevention

IQware deals with two classes of customers. The first is the “System Integrator” (SI) who configures and deploys IQware for a specific end user and tailors it to their specific needs. The second is the end user, who uses the completed system and has to live with the results. IQware delivers significant and sustainable benefits to both classes of customers.

Both types of customers have “pain” – and they really feel it. IQware soothes their pain by preventing it so that the pain never occurs. IQware does things differently.

The SI’s “pain” is the increasing cost of designing, building and deploying complex software systems. The SI competes with offshore “code sweat shops” to deliver software on time and on budget - and they are losing that battle. They lose that battle because they are using the same tools and doing things the same way that the offshore shops do. Good software engineers are hard to find and are very expensive. Software development tools are ubiquitous and global – the SI’s offshore and domestic competitors use the same tools. There are only three ways to gain an edge:

- Deliver superior & unique software that your competitor cannot match.
- Deliver similar software functionality - but create it in a very different way that significantly reduces the labor cost.
- Deliver similar software functionality - but create it in a very different way that significantly reduces the time-to-delivery.

IQware gives the SIs a sustainable, patented “edge”. IQware is both a standalone product and a rule-based development tool. IQware is uniquely rule-based which significantly reduces - and may even eliminate - the need for expensive, error-prone custom code development. This unique, patented (US #7,322,028) IQware feature gives you two advantages by significantly reducing **both** time-to-delivery and labor hours. This IQware feature lets you compete effectively with ultra-low-cost offshore software developers by delivering better software solutions sooner and at a total lower cost.

IQware's other edge is that is uses a TCB (Trusted Computing Base) with a DoD rated security level of B2/C2 that is immune to desktop viruses. You can offer your customers unique, secure, desktop-virus-immune software that is less expensive and installed in far less time using IQware. IQware helps SIs compete and profit by:

- Shortening software delivery time
- Reducing deployment effort
- Giving you confidence for successful fixed-bid proposals
- Reducing labor hours
- Offering a unique desktop-virus-immune solution

The end user’s “pain” is an IT system that is inflexible, cannot adapt, is not secure and is prohibitively expensive to maintain and upgrade. IQware benefits the end user by providing a system that is secure, that can adapt – even while running – as the end user’s needs change. IQware also ensures that the deployed system does what the end user wants it to do and works with new and emerging technologies such as wireless and the wide variety of handheld devices.

For both types of customers, IQware addresses the need for secure, flexible, adaptable & reliable content management and delivery. Content management and delivery may include medical records, pharmaceutical data, drug interactions, command and control center data, etc. Content management and delivery may also include POS (point-of-sale) advertising, ad tracking, effectiveness monitoring, etc. As concerns about cyber security, hacking and cyber terrorism build, it is anticipated that 100% secure and reliable software will be a requirement (not merely a "want") for virtually every application. Some specific benefits of IQware's software are:

- Secure Operation – Because of IQware's patented (US #7,322,028) Secure and Desktop-Virus-Immune features, critical customer data is protected from cyber attacks, malicious hackers or other compromise.

- Rule-based – Using "rules" rather than traditional programming allows on-the-fly changes to the system for maximum flexibility. This patented capability lets system integrators (SIs) compete with offshore programmers.

- Interoperable – Works with all desktop platforms. Works with hand-held and wireless devices.

- Central Deployment – IQware can be deployed centrally without interference with ongoing IT operations. IQware's operations can also be tracked centrally for billing, auditing and compliance.

- Central Management – IQware can be centrally managed and tracked so that customer feedback and data mining are accomplished in one secure location. This ensures secure data access control which is essential for compliance, billing and auditing.

- Huge Incentive for Adoption by System Integrators (SIs) – Currently, SIs compete with offshore programming shops and they are losing that battle. With IQware, SIs can produce and deploy complex content management systems for less money and win that battle.

Most medium- and large-scale business and manufacturing applications are "glued together" from multiple software packages produced by different vendors. Systems Integrators (SIs) or other third party consulting firms typically do this work by writing reams of custom code and desktop-virus-prone script files. The end product typically combines statistical packages, graphics and man-machine interface packages, database packages and data acquisition systems. This combination of products is a "patchwork quilt" of dubious quality, which greatly increases project cost, delivery time and overall security risk.

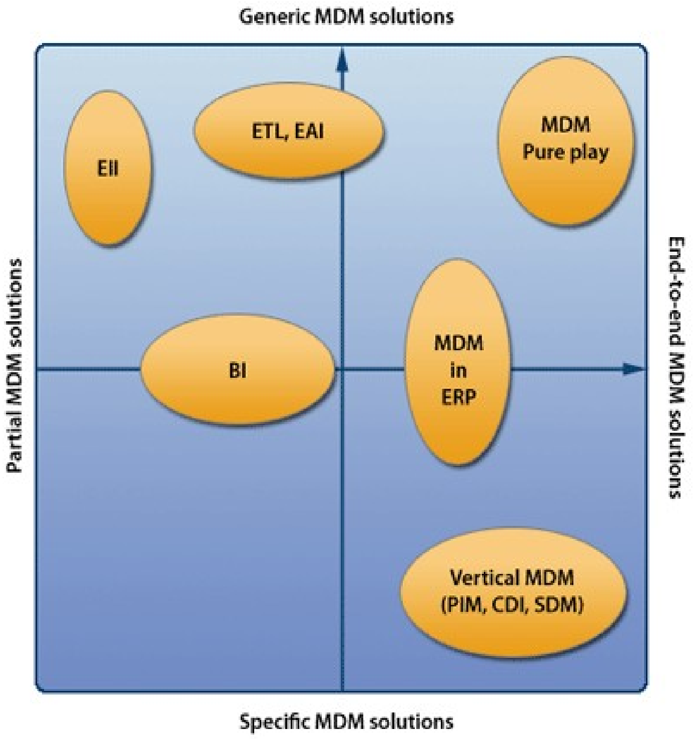
The end product from this "traditional" software creation process is expensive to maintain and cannot adapt as business needs change. It also cannot keep pace with changing technology - so it is usually discarded long before the end of its expected lifetime. This is a huge expense for most customers - and they know it.

IQware solves this problem by preventing it. IQware does things differently. IQware eliminates the need for custom code when creating a content management system. IQware also eliminates the need for integrating often-mismatched products from multiple vendors. In addition to these risk-reducing benefits, IQware provides complete immunity from desktop viruses, which have cost companies billions of dollars in downtime and lost productivity. IQware's software and application creation approach increases security as well as reducing total cost, delivery time and project risk. IQware's rule-based architecture allows functionality to be added at any time, "on-the-fly," creating additional market opportunities.

MARKET ANALYSIS

IQware sells into the Master Data Management ("MDM") and the (subset) Business Intelligence ("BI") spaces. IQware's unique flexibility also lets it sell into the HMI (Human-machine Interface), manufacturing and control spaces. These markets overlap many traditional market verticals and collectively are over $13 billion in annual sales in the United States alone. IQware also has significant contacts into the Australian and Pacific Rim markets which are expanding at a rapid rate.

The market for MDM software is $19 billion with a 10% growth rate, based upon a compilation of analyses prepared by the Gartner Group, International Data Corporation and the US Department of Commerce. The MDM market space has several components.
By way of background, traditional "MDM/BI" product offerings may be classified as shown in the diagram below. This diagram, along with the accompanying descriptions, illustrates how these solutions address the larger MDM issue. The horizontal ("x") axis plots solutions that bring end-to-end MDM features versus solutions that solve only a part of the "MDM problem". The vertical ("y") axis plots solutions that can manage any type or nature of Master Data (Generic) versus solutions that are limited to a specific domain (product, customers, etc.) or data nature (in ERPs, analytics, etc.). The various component areas within this diagram are defined and described below.



- **EII (Enterprise Information Integration):** These solutions allow query operations to multiple data sources across the IS and bring them to a common display presentation. These queries may be done interactively so that a pseudo-real-time view of the requested enterprise information is presented. This approach solves only part of the "MDM issue" because it lacks a central repository for enterprise data. Further, such a central repository requires a corresponding data management and analysis capability to be operationally useful.

- **ETL (Extraction Transformation Loading) & EAI (Enterprise Application Integration):** These approaches are really processes that translate/transfer data from one repository to another. Such technologies are necessary at least once to set up a central repository for enterprise data. However, such approaches do not work well interactively or on an "as requested" basis because they are both computation-intensive and bandwidth-intensive. Further, many existing IT installations are not architecturally amenable to this approach.

- **BI (Business Intelligence)**: This approach tries to present a "common operational picture" of the enterprise via an executive dashboard. The problem occurs when such solutions are layered on top of

ETL/EAI approaches because they inherit the attendant severe computational and bandwidth limitations problems (see above). This approach is logically extensible to MDM, but nearly all existing BI systems emphasize data analysis at the expense of data integration and management. Further, none of them (other than IQware) are interoperable and none of them provide the operational security and audit trail of IQware. Also, none of them can handle true real-time data where there is a guaranteed, finite limit to the latency between an event and its response. True MDM must properly manage operational Master Data. IQware significantly ***extends*** MDM by including real-time performance, interoperability and a rule-based approach.

- **MDM in ERPs**: Large Packaged Applications vendors are upgrading their platform with MDM. Such MDM features are often limited to the ERP itself and its subset of existing, pre-programmed functionality. Expanding the ERP to include true MDM is usually infeasible because of the significant client piece that such ERP installations have. A change to any part of the IT infrastructure inevitably causes costly “ripple effects” throughout the IT system. Such “ripple effects” serve as a significant barrier to IT system expansions and/or adaptation. ERP systems, once deployed, are essentially “frozen in time” and cannot be expanded without significant operational disruption and expense.

- **Vertical MDM (PIM , CDI, SDM)**: Historically, MDM was achieved in a limited way by “gluing together” various vertical solutions. Examples of this approach are PIM (Product Information Management), CDI (Customer Data Integration), SDM (Spend Data Management) and CRM (Customer Relationship Management). Implementing a vertical solution is almost always limited to a specific operational domain. Further, such an approach nearly always forces a proprietary model for Master Data. Even worse, any change in one (or more) of the underlying software systems automatically forces an expensive and disruptive change in MDM system. This, in turn, may force a complete re-design and re-deployment.

- **MDM Pure play**: New pure-play MDM solutions have emerged during the last few years. They try to solve the entire MDM issue in a generic way (not limited to a specific type or nature of data) and end-to-end (managing the entire Master Data life cycle). This is where IQware is positioned. Further, IQware separates the data acquisition, translation, analysis, archiving and presentation functions and does not tie them to any specific technology (US #7,322,028). This lets IQware take advantage of new and emerging technologies ***in all areas*** so that they may be may be successfully deployed without any interruption in IT system operation.

IQware addresses all major segments of the MDM market and adds other functionality as well. Specifically, IQware performs EII, ETL, BI and “pure play” MDM. IQware does NOT do ERP but it can be a part of an existing ERP system. This was an intentional design choice because the ERP space is crowded and needs no new entrants. Further, most customer already have an ERP system and are reluctant to change it. With IQware, customers may keep their existing ERP investment and still take advantage of new and emerging technologies.
IQware also addresses other market needs which are NOT part of the MDM space. IQware has additional capabilities that cross most market verticals. Because of these capabilities, IQware can support data sharing, data management and IT system integration in a way that no other software system can do. These additional capabilities include:

- Real-time monitoring and control
- Human-Machine Interface (HMI) and Supervisory control and Data Acquisition (SCADA)
- Security policy implementation
- Secure operation audit trail generation
- Interoperability and legacy system interface
- Thin client and wireless deployment

This market need is currently met by package vendors and System Integrators (SIs) and other third parties writing costly, non-secure, error-prone and high-risk custom code. IQware can position itself as the "preferred tool" to the SIs so that they can better sell to their end users. IQware's unique MDM/BI approach lets the domestic SIs be price-competitive with offshore, low cost programming since the application is established and deployed in a far more efficient and secure way. This creates a significant "demand-pull" into the market for IQware; i.e., SIs will have to use IQware to remain competitive.

IT system security – ***not simply network security*** - continues to be a major national and international issue. As of January 2, 2006, The Gartner Group reported:

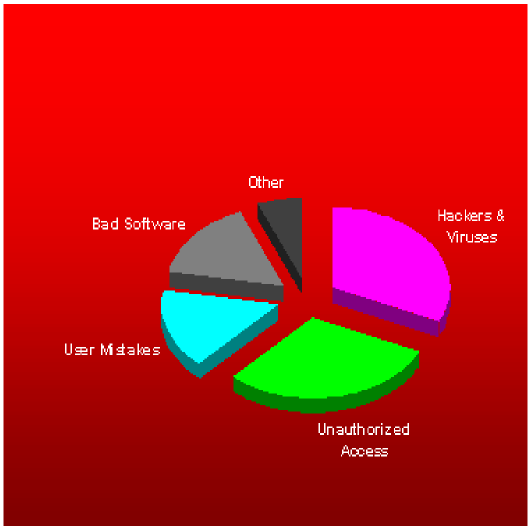
> "Two more major data security breaches show that U.S. data protection measures are still entirely inadequate. Enterprises and lawmakers must do much more to protect consumers. On 16 December 2005, ABN AMRO Mortgage Group acknowledged that a computer tape containing data on approximately 2 million customers — including social security numbers — had disappeared in transit. This announcement followed Sam's Club's 2 December 2005 disclosure that at least 600 cardholders who had purchased gas at the retailer's locations had been affected by credit card fraud. Sam's Club has stated that the breach did not involve electronic systems or databases used inside its stores

In January 2006, ChoicePoint was fined $15M for security breaches that led to identity theft. Note that network security was not the issue here – this was an "inside job". All the firewalls, anti-virus and other "protective software" did not prevent the "attack" nor will such tools prevent future successful attacks. A recent study rated "IT System Error Sources" by cost to the organization. As illustrated in the adjacent diagram, the costs are staggering and on the rise, creating a significant risk exposure for many companies. This is an area that an IQware deployment directly addresses. ***IQware deals with the correct, reliable operation and security of the entire MDM/BI system – not just the network. Network security alone is never enough to guarantee proper IT system operation and information assurance.***

IT System Error Sources

(Percentages by Cost)

- (32%) Hackers & viruses (declining)
- (30%) Legit users intentionally doing bad things (called unauthorized access - rising)
- (16%) Legit users accidentally doing bad things
- (16%) Bad software
- (6%) Other



A recent Gartner Group survey concluded that 2006 IT budgets are increasing from 2005 levels. The IT spending growth is largest in the federal, health care and financial sectors where regulation imposes a higher security and data integrity standard. Regulation also imposes a higher standard for systems and data integration as is the case with the Health Information Portability Authorization Act ("HIPAA"), Medicare Part D, etc. and government "C-cubed-I mandates for secure data integration, analysis and communication. The Company thus anticipates a stronger market for its products even as the general software market continues to grow.

BUSINESS AND MARKETING STRATEGY

IQware recognizes the significant potential of its technology and intends to maximize its financial return. Accordingly, IQware's business goal is to be a technology provider to key players in the market verticals of interest. As an example, our existing MTM License Agreement in the pharmacy space makes IQware the exclusive technology provider to NWS/Healthpoint Technologies, an international company. The salient points of this agreement are simple: NWS/Healthpoint Technologies gets exclusive access to patented software that is configured for their market-specific application. In return, IQware gets license fees and IQware shares in the gross revenue stream. IQware also gets recognition by a "Powered by IQware" sticker on the delivery point for the particular software application. This existing agreement is the template for the other agreements that are currently contemplated and ones in the future.

Clearly, the key to penetrating the vertical market opportunities is the working relationships that IQware is developing with firms like NWS/Healthpoint Technologies. Such firms include the SIs and various IT consulting companies. Forming and nurturing these relationships is essential to long-term growth because it creates leverage that will allow IQware to remained focused on its core competency - that of a technology company.

The strategy of partnerships with third party SIs is further recognition of the state of the enterprise software market. In addition to the pure numerical leverage provided by the partnership approach, the most significant advantage to use of partners in the early stages of IQware’s growth is the relationships that the partners bring to the table. Enterprise software sales are complex long cycle processes where shortening the cycle by leveraging the customer goodwill of the partner makes a significant impact on the cost of sales and the near term volume potential. The relationship with the partners are truly symbiotic in that the IQware technology gives them a significant "value add" to bring to their customers as well as a point of differentiation from other SI competitors.

Accordingly, IQware’s “go-to-market” strategy is to identify, educate, motivate, evaluate, and prune relationships with key system integrators (SIs). The benefits of this approach are the following:

- It leverages the SIs pre-existing relationships with the end user
- The SI is motivated to use IQware because it is a differentiator to their customer base
- IQware gets access to the SIs customer base
- IQware gets access to the SIs pipeline

Working relationships are established with the following companies:

- MSIT (DoD sales)
- NuPath Technologies (Pharmacy sales & Health Care sales)
- Oracle (database supply and marketing channels)
- HP (hardware and O/S supplier)
- BAE Systems (DoD bid partner)

Working relationships are in progress with the following companies:

- CACI (DoD bid partner)
- TKC Communications (DoD)

- SAIC

These system integrator (SI) relationships significantly reduce the sales cycle, afford IQware deeper penetration into accounts and shift much of the sales burden from IQware to the SIs. The SIs are starting to embrace this product offering because it gives them a superior alternative to traditional products and application creation approaches, particularly from a security perspective. IQware software also increases SI productivity, allowing them to make more money per project and complete more projects per unit of time. IQware's offering further allows the SIs to compete with overseas software companies that have much lower labor costs. IQware is expanding its relationships with SIs who service the medical/health care, government, manufacturing, telecommunications and pharmaceutical markets. IQware is also developing new relationships with SIs in banking and financial services.

COMPETITION

The Company faces competition from SIs, Business Intelligence software vendors (e.g., Hyperion, Business Objects, Cognos) and some manufacturing software companies such as Rockwell Software, USDATA and Wonderware. IQware plans to compete with these companies by leveraging its success in the pharmacy space, using its competitive advantages and by vigorously enforcing the its significant intellectual property rights (US Patent #7,322,028).

Competitive products have a fundamentally different architecture. They do not segregate functionality between the secure server and the client in a manner that IQware's products do. Competing products cannot duplicate IQware's functionality with patches or new modules. Rather, the competing products would have to be thoroughly rewritten using a new architecture, which would be extremely time consuming and be incompatible to current products. This makes the transition impractical due to the large installed base of current products. Further, the new architecture that would be required would most likely infringe IQware's patented (US #7,322,028) architecture (both US and international), creating another significant roadblock for the competition. This is a significant weakness of competing products because it ties them too closely to a particular deployment platform and significantly reduces their flexibility. As new technologies emerge, competing products cannot take advantage of them without major, expensive redesign and/or rewriting.

New computer products and portable, hand-held devices are entering the market rapidly. IQware can work with these new and emerging technologies without being rewritten. The competing software products are generally incompatible with these new devices. This situation gives IQware a huge economic and technological advantage.

The Company also foresees potential competition from ERP companies and operating system companies. However, Management believes that, at least in the short run, the Company's products are complementary rather than competitive with these products and that ERP or operating system companies may ultimately be candidates to acquire the Company and thus provide an exit strategy for investors.

COMPETITIVE ADVANTAGES

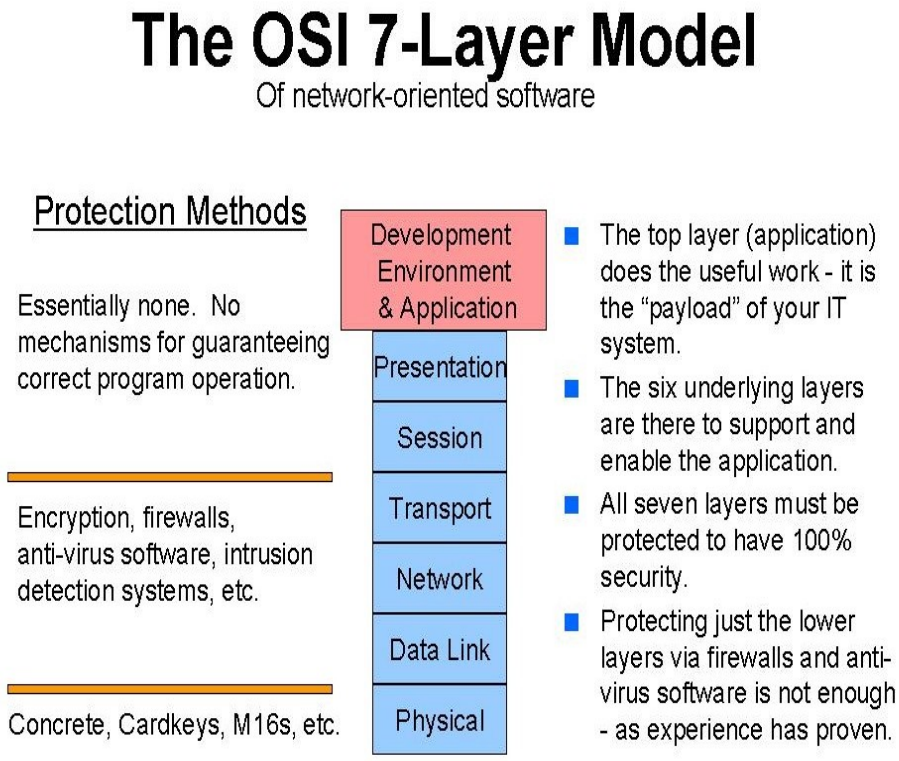
IQware's competitive advantages are patented (US #7,322,028) and the following:

- **Efficiency**. IQware's patented (US #7,322,028) rule-based software employs "rules" as opposed to traditional code-driven programming. Custom coding is the largest cost item in nearly all IT projects, so eliminating or reducing it greatly reduces project cost, risk and duration. This is a significant advantage to Systems Integrators in the US who have been losing business to offshore competitors who can write code at a fraction of their cost. IQware directly addresses this issue.

- **Security**. IQware complements and supplements anti-virus software. Anti-virus products offer protection only against known viral strains. IQware uses a "thin client" architecture, which puts the critical functionality on the server where the critical portions of the IQware secure applications run. The client handles the less critical user interface functions and miscellaneous interface operations where tampering will not affect the proper execution of the IQware applications. This architecture lets IQware work seamlessly with new, emerging computer technologies and platforms.

- **Interoperability**. IQware's products work with all major operating systems, whereas many competing products are limited to Microsoft-based platforms. The segregation of functionality lets IQware with new, emerging client devices, including PDA's, Linux, iMACs, Blackberry devices, etc.

From a security perspective, IQware is quite complementary to the various firewall and anti-virus products on the marketplace. As the diagram illustrates, software can be modeled as a 7-layer structure. These layers are logical layers that perform different functions. Each layer performs function to the layer above it in the diagram. The top layer is the application layer - it's the layer that does the useful work. The underlying six layers are only there to support the top, or application layer.



The OSI 7-Layer Model

Of network-oriented software

Protection Methods

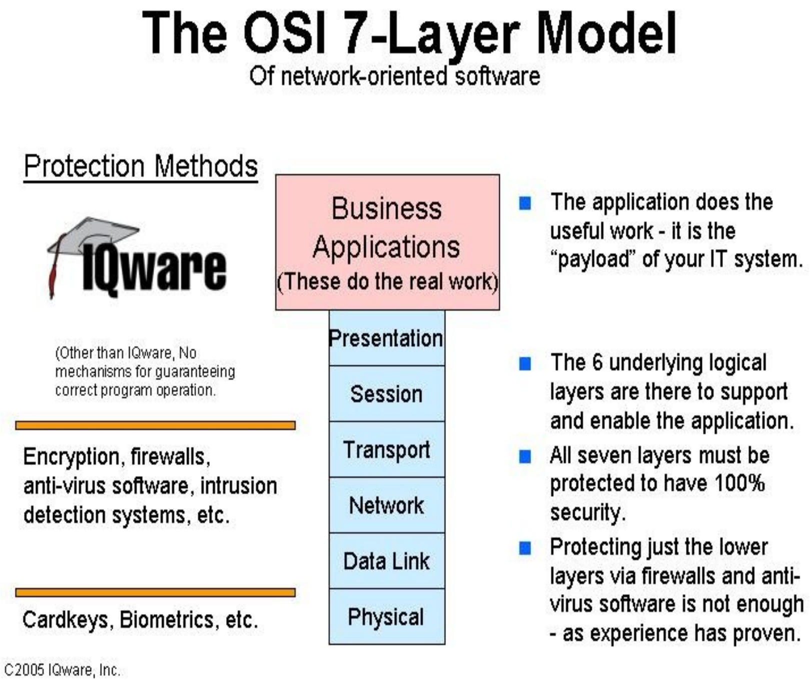
Essentially none. No mechanisms for guaranteeing correct program operation.

Encryption, firewalls, anti-virus software, intrusion detection systems, etc.

Concrete, Cardkeys, M16s, etc.

- The top layer (application) does the useful work - it is the "payload" of your IT system.
- The six underlying layers are there to support and enable the application.
- All seven layers must be protected to have 100% security.
- Protecting just the lower layers via firewalls and anti-virus software is not enough - as experience has proven.

Firewalls, anti-virus software, encryption and intrusion detection systems only protect the lower logical layers of the software model. Both research and experience have shown that this amount of cyber defense is not enough. IQware works to protect the higher layers – which is essential for 100% security. Using IQware software ensures that the software application – whatever it may be – will operate correctly even in the presence of a cyber attack. As shown in the diagram below, a total security solution for a customer would include firewalls, anti-virus software and IQware's secure applications. **This situation lets IQware to position itself cooperatively and complementarily with these vendors**.



The OSI 7-Layer Model

Of network-oriented software

Protection Methods

IQware

(Other than IQware, No mechanisms for guaranteeing correct program operation.

Encryption, firewalls, anti-virus software, intrusion detection systems, etc.

Cardkeys, Biometrics, etc.

Business Applications (These do the real work)

Presentation

Session

Transport

Network

Data Link

Physical

- The application does the useful work - it is the "payload" of your IT system.
- The 6 underlying logical layers are there to support and enable the application.
- All seven layers must be protected to have 100% security.
- Protecting just the lower layers via firewalls and anti-virus software is not enough - as experience has proven.

C2005 IQware, Inc.

From an operational perspective, IQware's software products compete with Systems Integrators, Business Intelligence companies such as Brio, Business Objects, and Cognos and against manufacturing software companies such as USDATA, Real World Technologies and Wonderware (see the competitive matrix). IQware's software is superior to its competition because the software is not limited – as others are – to Microsoft-based platforms. Most importantly, IQware unique software is immune to desktop viruses and is secure.

IQware's software products all use the exact same executable code – only the configuration information is changed. Since the same code is used in all implementations, the time, cost and risk involved in developing, debugging and testing applications is reduced dramatically. IQware's unique, patented (US #7,322,028) software architecture provides the maximum in IT system security and cyber-attack protection. Competitors who do not reuse the exact same code must go through extensive and expensive application creation, development and implementation processes. Further, competitor's software development efforts must be tailored to each vertical market that they pursue – an expensive, virus-prone, time-consuming and hard-to-manage effort.

IQWARE'S APPROACH TO SOFTWARE AND IT SECURITY

The Need for Security

Security is essential in Business Intelligence (BI) systems since they have access to critical and proprietary enterprise information. The expenses associated with cyber attacks fall into four categories:

1. Damage cleanup
2. Business disruption
3. Enterprise data theft and/or corruption
4. Discovering and defusing a software "time bomb"

The proper goal of IT and software security is to ensure that the business operations are tamper-proof and that they will not be interrupted by a cyber attack. Cyber attacks and viruses are problematic because of the potential harm that they can cause. If the IT system – and the component software products – are properly architected, then cyber attacks and viruses will do no damage. This is what IQware does. IQware's application software will work properly – even during a cyber attack – without any data loss or interruption in business operations.

In late January 2003, a cyber attack originated outside the U.S. and did extensive damage. The worm, called "SQL Slammer" plugged network channels with excessive traffic, interfered with Bank ATM communication, and even interfered with Microsoft's internal network. This "worm" exploited weaknesses in Microsoft's operating systems and exploited weaknesses in SQL server and MDSE 2000, which are popular Microsoft applications.

Clearly, such cyber attacks are increasing in frequency and in severity. Future attacks will exploit other "holes" in popular desktop operating systems and applications. Further, the "best-of-breed" anti-virus software, firewalls and intrusion detection systems that failed to defend against SQL Slammer in January 2003 will again be insufficient to defend against the next attack. The last two years have seen too many successful cyber attacks to mention them individually – they're in the news all the time.

The Seven Layer Software Security Model

The critical issue of software security is one that IQware addresses within this new IT environment. IQware's unique architecture -- and its use of a secure server environment -- makes IQware software desktop virus immune and provides the maximum possible IT system protection.

Security is the cornerstone of IQware Software. Other IT systems use code patches and security updates, which only prevent further infections of the same viral strain. These approaches do nothing to clean up the damage from the initial attack nor do they inoculate against unknown, future virus attacks.

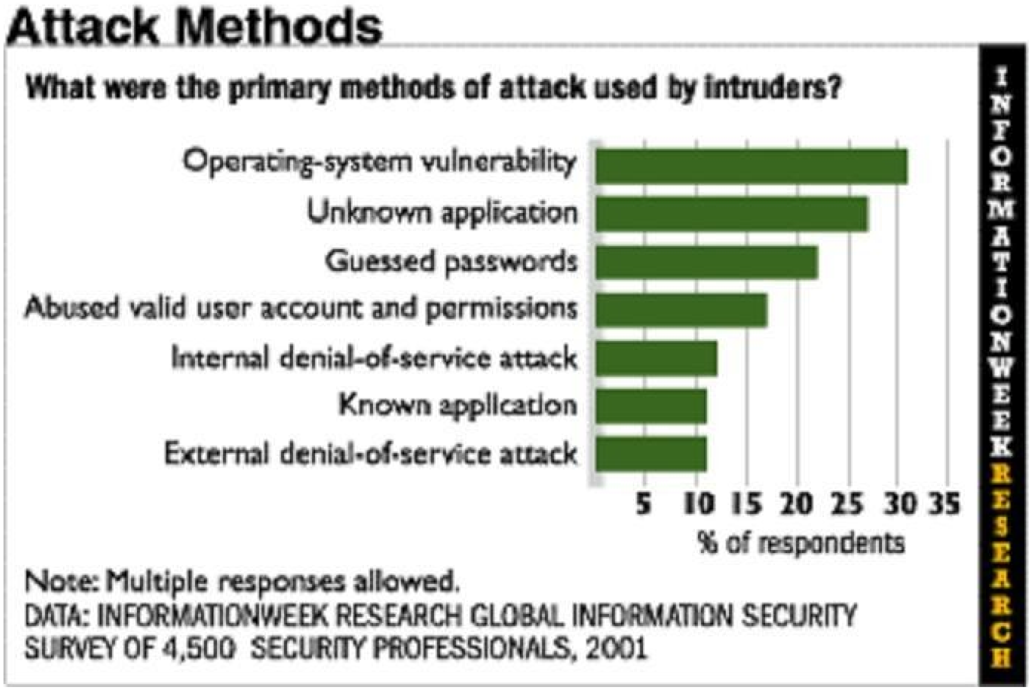
From a security perspective, IQware is quite complementary to the various firewall and anti-virus products on the marketplace. As previous diagrams have shown, software can be modeled as a 7-layer structure. These layers are logical layers that perform different functions. Each layer performs function to the layer above it in the diagram. The top layer is the application layer – it's the layer that does the useful work. The underlying six layers are only there to support the top, or application layer.

As is clear from the seven-layer software model, firewalls, anti-virus software, encryption and intrusion detection systems only protect the lower logical layers of the software model. Both research and experience have shown that this amount of cyber defense is not enough. IQware works to protect the higher layers – which is essential for 100% security. Using IQware software ensures that the software application – whatever it may be – will operate correctly even in the presence of a cyber attack.

A total security solution for a customer, which would protect all seven layers of the software model, would include firewall(s), anti-virus software and IQware's secure BI applications. *This allows IQware to position itself cooperatively and complementarily with these vendors*.

Cyber Attack Methods

IQware's security is based upon its architecture, coding and deployment. All software applications, including IQware's, execute in the context of the operating system (O/S) and related run-time systems. A secure system results from the proper architecture, coding and deployment of the operating system and application.



Note: Multiple responses allowed.
DATA: INFORMATIONWEEK RESEARCH GLOBAL INFORMATION SECURITY SURVEY OF 4,500 SECURITY PROFESSIONALS, 2001

A survey showed that the primary attack method used by hackers and cyber terrorists is to exploit weaknesses within the operating system. Another significant attack method was to exploit existing weakness in the application layer. The cyber attack survey results are given in the above diagram. IQware's approach directly addresses this significant problem by using a secure operating system on the server side in its client-server architecture. This technique lets IQware applications safely interact with common, off-the-shelf (COTS) desktop computers that are very vulnerable to cyber attacks and viruses. IQware's unique and patented (US #7,322,028) architecture lets customers have the best of both worlds by combining a secure environment with inexpensive and popular desktop technology.

IQware Uses a Secure Operating System (O/S)

IQware uses a Secure Operations System (O/S) and gains its capabilities from its architecture. The significant components are:

- Department of Defense rating of B2; National Information Assurance Partnership (NIAP) Common Criteria (ISO 15408) minimum rating of EAL5.
- A "Reference Monitor" mediates attempts by a subject to gain access to an object. An access control list is maintained as well as a tamper-proof audit trail of security-related events.
- An authorization database serves as a repository of subject and object security attributes, including access modes and allowed operations.
- The IQware application is layered on the secure O/S, using the Reference Monitor architecture to implement the security policy while providing full accountability, tracking and assurance. This design ensures that the combination of the application and O/S will operate in accordance with the Department of Defense Secure System standards.

Both the operating system and application software must be architected, coded and deployed properly in order to be secure. Patching is ineffective. True-to-form, the SQL Slammer worm that hit in late January 2003 exploited weaknesses in Microsoft's operating systems, SQL Server 2000 and MDSE 2000 software. Even though Microsoft had a patch for this particular security flaw, most IT managers simply did not install it. Patching is so commonplace that it has become impractical for IT managers to install every one of them because they would be modifying their IT systems more than once per day. This "change rate" is impossible to sustain and to manage. Besides, future viruses will surely exploit other existing software flaws for which patches are not yet available. Another question is "how did this worm get through businesses' best-of-breed anti-virus software and firewalls?"

Limitations of Anti-Virus Software and Firewalls

As the seven-layer software model clearly shows, defense techniques such as firewalls (FWs), anti-virus software (AVS), intrusion detection systems (IDS), etc. are effective only in the lower layers of the model. These techniques do nothing to address the critical issue of ensuring that your application software operates properly even in the presence of viruses and cyber attacks.

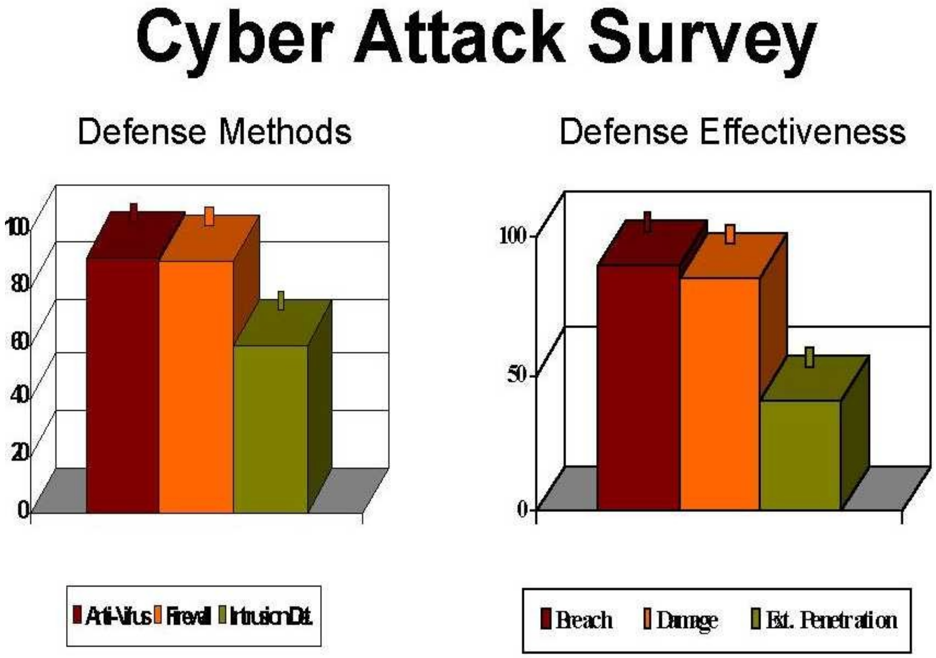
Anti-virus software can only defend against known viral strains. Firewalls help protect systems from network-transmitted viruses. Unfortunately, anti-virus software and firewalls cannot do the following critical functions:

- Cannot prevent damage from unknown viral strains
- Cannot clean up damage from cyber attacks
- Cannot prevent critical data loss from cyber thieves
- Cannot prevent damage from user errors
- Cannot ensure the 100% correct operation of application software
- Cannot make an IT system tamper-proof
- Cannot provide 100% security

Man-in-the-middle attacks, IP-spoofing, etc. are all techniques that can defeat firewalls and other defense schemes. Entire websites are devoted to the tools and techniques of hacking, including footprinting, scanning and enumeration. Some example websites that feature these tools and techniques include www.cultdeadcow.com, www.phrack.org, www.foundstone.com/rdlabs and www.nwpsw.com.

Cyber Defense Ineffectiveness

If firewalls, anti-virus software, intrusion detection systems and the like were truly effective, then networks and IT systems would be impregnable and there would be no concern about cyber attacks. Unfortunately, the exact opposite is true. Both experience and research have shown that firewalls, anti-virus software and intrusion detection systems cannot provide anywhere near 100% protection.



Source: Computer Security Institute, Computer Crime and Security Survey, April 7, 2002

The Computer Security Institute conducted a survey of cyber defense effectiveness in April 2002. The survey results clearly show the ineffectiveness of these defense mechanisms. Nearly all organizations that were surveyed had experienced breaches, damage and external penetration of their IT systems - *even though they had installed the best cyber defense systems*. These defense mechanisms included anti-virus software, firewalls and intrusion detection systems. The Computer Crime and Security Survey results are shown in the bar graphs.

What Secure Systems Must Do

Security research has been ongoing since the 1960s. The research has shown that "putting out security fires" by patching code can never be 100% successful. Rather, software systems must be architected from their foundations in accordance with a secure system model. This is the only way to create a secure and tamper-proof software system.

Secure systems must control access to information and information processing operations. Only properly authorized people are allowed to read write, create, edit or delete information. Further, only properly authorized processes are allowed to read, write, create, edit or delete information.

The three main characteristics of a secure system are policy, accountability and assurance. These three characteristics must be present in order for a software system to be secure. Each of these critical characteristics is explained in the following paragraphs.

Policy

Secure systems must have a well-defined, clear and practically enforceable security policy. This policy includes object marking so that the sensitivity and allowed access modes of each object are clear and computable. Further, each "object" in the software system (e.g., files, directories, RAM locations, external devices, etc.) must have an access control label that summarizes this information attached to it in a secure way. This access control label is critical to a secure system. The lack of this "object marking" is one of the reasons that popular, virus-prone desktop software cannot be made secure by simply adding other software to it.

Accountability

Secure systems must have accountability so that any data processing actions may be accurately traced to the responsible party. This accountability includes a secure identification method so that system users can be associated with their authorizations in a secure manner. An audit trail is also required so that all security-related actions can be accurately and securely traced to the responsible party and then recorded for later review and analysis. This audit trail must be continuously maintained and protected.

Assurance

Secure systems must periodically evaluate the "trusted" hardware and software security mechanisms to provide assurance that the security policy is enforced properly. The corresponding mechanisms that handle accountability must also be periodically (and independently) evaluated. These hardware and software mechanisms for policy and accountability must also be continuously protected from tampering and free from external observation. For example, if an unauthorized user (or process) attempts to access a protected set of files or directories, the mechanism that prevents this cannot tell the user or process "why" they were denied access. Such an explanation might provide too many clues to hackers about how to get around the mechanism. The table below summarizes the three critical secure system characteristics.

Secure System Characteristics (Summary)

Policy

- **Security Policy** - System must enforce a well-defined security policy.
- **Marking** - System must associate all objects with access control labels (sensitivity & access modes).

Accountability

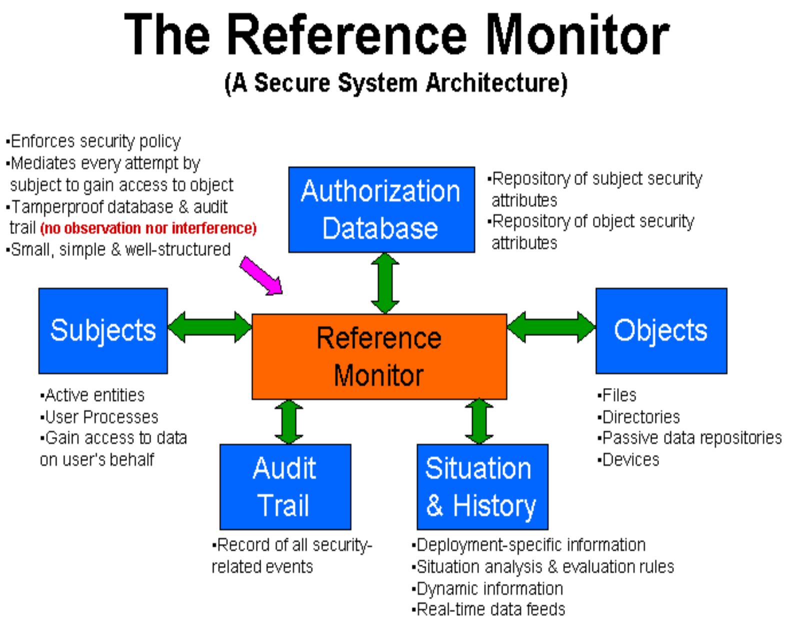
- **Identification** - System must identify individuals and their corresponding authorizations in a secure manner.
- **Audit Trail** - System must keep & protect audit trail so actions may be traced to responsible party.

Assurance

- **Evaluation** - System must have hardware/software mechanisms that can be independently evaluated to assure that policy & accountability are enforced.
- **Continuous Protection** - System must continuously protect trusted mechanisms that enforce policy & accountability from tampering.

The Reference Monitor – A Mechanism for a Secure System

A trusted mechanism for a secure system is known as the Reference Monitor. It is an architecture that can be implemented through software, hardware or a combination of the two. This structure implements the security policy by controlling the access of every subject (users, processes, etc.) to every object (files, directories, RAM locations, external devices, etc.) in the software system.

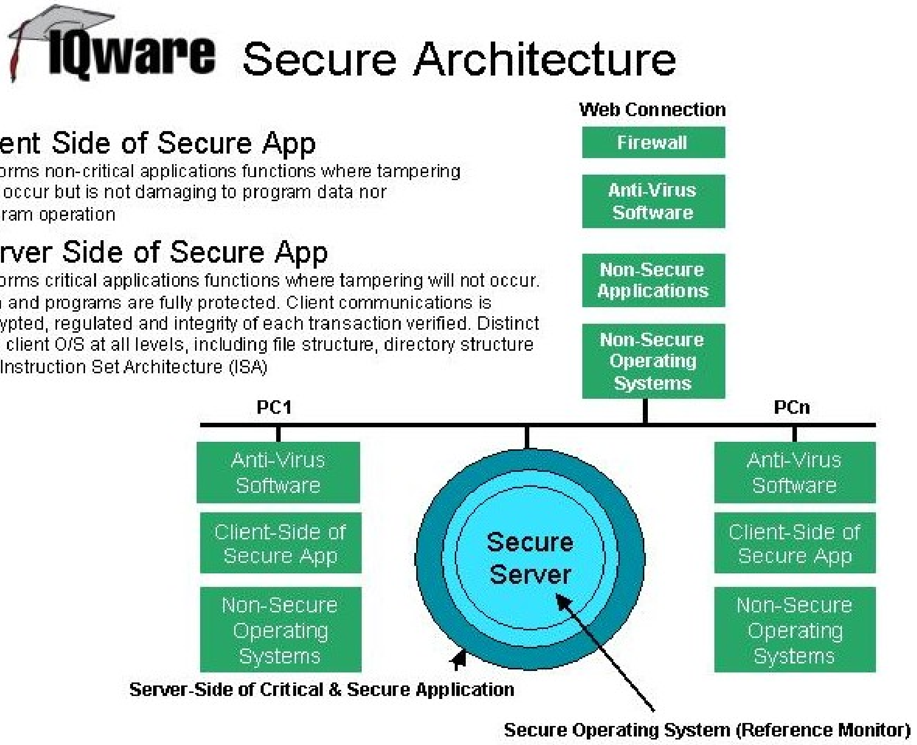

The Reference Monitor
(A Secure System Architecture)
•Enforces security policy
•Mediates every attempt by subject to gain access to object
•Tamperproof database & audit trail (no observation nor interference)
•Small, simple & well-structured
Authorization Database
•Repository of subject security attributes
•Repository of object security attributes
Subjects
Reference Monitor
Objects
•Active entities
•User Processes
•Gain access to data on user's behalf
Audit Trail
Situation & History
•Files
•Directories
•Passive data repositories
•Devices
•Record of all security-related events
•Deployment-specific information
•Situation analysis & evaluation rules
•Dynamic information
•Real-time data feeds

The reference monitor maintains an authorization database that contains security attributes of all subjects and objects. The Reference Monitor also maintains an audit trail of all security-related events. As mentioned earlier, the Reference Monitor can be implemented in a variety of ways but it must be tamper-proof and non-observable.

As an example, viruses are generally composed of script files, executable images or a combination of the two. The reference monitor ensures that such virus script files and executable images cannot access any system resources (including files, directories, RAM, hardware devices, etc.). ***This architecture and approach prevents the virus from operating – even if it is a new and never-seen-before virus.***

Malicious software cannot spawn or launch other applications nor can it propagate itself via replication and retransmission. As another example, common virus scripting languages such as VisualBasic™ will not execute in IQware's secure server environment because the security policy implemented by the Reference Monitor prevents it. Access to email lists, addresses and data transfer channels is also prevented so viruses cannot spread. The reference monitor also prevents harmful application macros from executing, which closes another door to cyber attacks and hackers.

IQware uses this Reference Monitor and a secure operating system to create a secure software system. The secure server uses the Reference Monitor to ensure that the system security policy is implemented properly. All critical software functions and system operations are handled by the IQware application operating on the secure server.


IQware Secure Architecture
Web Connection
Firewall
Anti-Virus Software
Non-Secure Applications
Non-Secure Operating Systems
PC1
PCn
Anti-Virus Software
Client-Side of Secure App
Non-Secure Operating Systems
Secure Server
Anti-Virus Software
Client-Side of Secure App
Non-Secure Operating Systems
Server-Side of Critical & Secure Application
Secure Operating System (Reference Monitor)

Client Side of Secure App

Performs non-critical applications functions where tampering may occur but is not damaging to program data nor program operation

Server Side of Secure App

Performs critical applications functions where tampering will not occur. Data and programs are fully protected. Client communications is encrypted, regulated and integrity of each transaction verified. Distinct from client O/S at all levels, including file structure, directory structure and Instruction Set Architecture (ISA)

IQware also uses a "thin client" architecture that puts the critical functionality on the secure server where the majority of the IQware secure application executes. This segregation of software functionality allows IQware to work with common desktop (non-secure) clients without creating any security issues. Any security breach occurring on a client machine will not propagate to the IQware application and will not interfere in any way with its operation. This unique functional assignment between client and server lets IQware provide the best of both worlds: a secure software environment with the convenience of the desktop machine.

All critical data and functions are executed in a secure environment. The clients can be any common desktop, even ones with virus-prone operating systems and/or applications. Computer virus "infections" on the client machines cannot get into the secure environment and will not damage files or interfere with the proper execution of the IQware application. IQware's secure and patented (US #7,322,028) architecture is shown in the diagram.

The client handles the non-critical user interface functions and miscellaneous interface operations where tampering will not affect the proper execution of the IQware application. This functional segregation is an important part of protecting an IT system against cyber attacks. Further, this distribution of software functionality lets IQware work with any client device, including PDAs, Linux, Mac, Windows, cell phone, etc. As technology changes, this level of software flexibility is the only way that businesses can incorporate new technology without disturbing operations.

IQWARE SOFTWARE PRODUCT TECHNICAL DETAILS

IQware software is a desktop virus immune, platform independent, interactive general-purpose data acquisition, analysis, reporting and archiving system.   IQware is immune to desktop viruses and has a rule-based architecture. IQware has created various industry-specific products from the IQware “template”. The patent was filed on 9/19/2001 and IQware serves Fortune 500 environment across multiple verticals.

Because of its unique architecture, IQware reduces and/or eliminates the need for expensive custom code to implement data and automation projects. IQware is configurable on-line via "point-and-click" mouse operations and/or data file editing. IQware applications are assembled with “IQ Blocks™”, which are intelligent objects that alter their behavior as needed to reflect the specific needs of the application. This powerful and flexible architecture transcends traditional programming methods and gives your applications a much longer lifetime.

Incorporating the Oracle database for data archiving, IQware can operate with any desktop platform including Vista, Windows-XP, W2003 Server, Windows-2000, Windows NT, Windows-98, Macintosh, iMacs, Mini-Macs, Berkley UNIX, SuSE-64 Linux, OVMS, Unix and other versions of Linux, which is rapidly gaining market share. Attributes of IQware software follow:

Architecture

- IQware's architecture is client-server and rule-based.
- IQware uses the Reference Monitor concept and a secure non-Microsoft O/S to provide complete immunity from desktop viruses.
- Object-oriented programming is used for the graphic display objects and the user interface objects.
- In areas where duplication of the object's methods is not appropriate, standard multi-thread programming techniques are used.
- All display objects in IQware are very intelligent and carry with them all the knowledge they need to acquire, analyze and display whatever data is requested of them.
- Vendor-specific language extensions are assiduously avoided to guarantee compatibility with future releases.
- All display objects are designed and written completely independently from the display hardware and client platform. They are easier to write, test, debug and they work correctly on all client platforms.

Database

- IQware prefers Oracle™ as its database (but it can use any ANSI-compliant relational database).
- It may be accessed via SQL and supports ODBC network access as well.
- The database size is limited by only by the combined capacity of the specific database selected and the hardware platform’s capabilities.

Interfaces

- IQware interfaces to ERP/MRP systems, including PeopleSoft, SAP and Oracle.
- IQware can also interface to legacy systems for HR, AR/AP/GL and to MES systems.

Client Platforms

- The clients for IQware are all desktop machines, including Vista, Windows-XP, 2003 Server, 2000, ME, NT, 98, Mac O/S X, Berkley BSD UNIX, SuSE 64 Linux and all other Linux variants.
- Other PDA clients are in development.

Standards and Compliance

- IQware can help provide automation support for ISO-9xxx compliance and ISO-14xxx compliance.
- EPA compliance, including 40CFR part 60, 40CFR part 75.
- FDA compliance, including 21CFR part 11.
- HIPAA compliance, including 45CFR part 164, 162 and 160.
- Internally, IQware obeys all relevant multi-platform/multi-vendor IEEE, ACM and POSIX interface standards, which ensures interoperability, platform independence and maximum lifetime.

Flexibility

- IQware, by architectural design, is extremely flexible using rules for configuration.
- The exact same software engine is used for each target market. The component IQware objects are simply configured to meet the needs of the specific application. This lets IQware deliver customer solutions securely, quickly and reliably.
- IQware removes software development risk by either eliminating or greatly reducing the need for much custom code. Simply configuring IQware using “point-and-click” mouse operations can create an application.
- Since IQware has all of the pieces (statistics, MMI, database and data acquisition), no "gluing together" of distinct (and often incompatible) software packages is required.
- IQware's unique, patent-pending architecture makes all this happen**.**

Other

- IQware can provide OLAP services wherever required.
- IQware provides e-commerce support and back-office database search/sort functionality for web portals and other web-enabled applications.