

**WHEN DOES A HOSTED TAX SOLUTION
EQUAL GREATER PEACE OF MIND?**



Written by Randy Cronk
greatwriting.com



TABLE OF CONTENTS

When Does a Hosted Tax Solution Equal Greater Peace of Mind?	3
Solution Security Defined	3
Case in Point — Corporate Income Tax.....	4
Advantage #1 — Best-of-Breed Technology.....	5
Shadowing	5
From-anywhere user access.....	5
Thin clients	6
Load balancing.....	6
Advantage #2 —Best Practices.....	6
Application Change	6
24/7 Monitoring	6
Segregated Client Databases	6
Advantage #3 — Data Integrity and Privacy	6
Thin clients	7
Data communications security	7
Protection from Internet threats	7
Virus protection	7
Advantage #4 — Asset Protection and Business Continuity.....	7
Physical security	8
Fire suppression.....	8
Disaster failover	8
Full Solution Security	8



WHEN DOES A HOSTED TAX SOLUTION EQUAL GREATER PEACE OF MIND?

Organizations should always consider whether a deployment model promotes or impedes security. Vertex[®] proves the security advantages inherent in hosted solutions.

With a hosted solution, a company utilizes software on a vendor's system via the Internet, as opposed to installing the software in-house on their own servers. Vertex Income Tax On-line is one example. Vertex installs and operates the software on Vertex servers and clients perform their income tax accounting, compliance, planning, and forms preparation activities by accessing this software across the Internet from wherever they are. Given the sensitivity and importance of such tasks, the hosted scenario inevitably raises questions around reliability, security, and business continuity — in short, questions about CFO peace of mind.

Hosted tax solutions have the potential to offer greater peace of mind versus the traditional in-house deployments. In the hosted solution, controls exist across multiple dimensions to create a secure and integral environment for the client to conduct their critical business functions. Competitive standards for commercial hosting providers dictate these controls, which address protection across dimensions that include: data interception, data loss, data corruption, system failures, compliance failures, intrusions, natural disasters, facility break-ins, and many more.

Independent client companies with in-house deployments often cannot address security and environmental controls to the extent that commercial hosts can; thereby leaving their key applications and data less secure than if they were in a hosted solution! Hosting addresses full "solution security" by working across all of the dimensions - not just one or two - and by integrating the dimensions successfully within a comprehensive policy that combines best practices with best-of-breed technology.

Solution Security Defined

The decision about whether to go with a particular provider will involve multiple issues, with security usually top-of-mind. One of the first questions IT managers typically ask is:

"If my data goes offsite, does that make my data less private and more susceptible to interception than if I host the applications myself?"

The answer is "no" — at least not at Vertex. Because we use a Citrix-based solution, we don't have to move data over a wire in order to use the data. We only move pixels and mouse movements (screen coordinates) across the wire — and we do that by using military-style encryption. Not only are these bits meaningless to any potential eavesdropper, but any would-be system intruders would be blocked by encryption keys, passwords, firewalls, and lack of physical access — just to name a few of the countermeasures a professional hosted solution, like Vertex, employs.

The concern for IT managers is not just a particular kind of threat, but all threats and all issues that might compromise assured service delivery regardless of where the solution is hosted.



When Does a Hosted Tax Solution Equal Greater Peace of Mind?

Most IT managers would agree there are at least six key business drivers to solution security, as outlined in Table 1:

Privacy	Privacy is what many people think of when they think of security. Companies can't operate if they can't control access to trade secrets, business strategies, customer data, employee data, and other sensitive information.
Integrity	You don't have to steal an organization's information in order to misuse it. Data corruption is possible in all sorts of ways — including rounding errors or because taxing authority changes were not programmed correctly or in a timely manner.
Reliability	Where integrity is about the data itself, reliability is about the process that handles the data. A reliable process always produces correct information and never lets it become incorrect. To be reliable, a system can't just be safe from hacker attack. It must also be safe from operator and system errors.
Business continuity	If part or all of a company goes "out of business" when disaster strikes then data can be lost. Even in cases where the data is backed-up, business continuity needs to be measured by how long it takes to bring operations back to normal after the disaster has past.
Compliance	Businesses can't operate if they violate rules set by the IRS, SEC, FASB, and Sarbanes-Oxley. All these rules focus on how data is handled. Companies must show they handle data properly.
Asset protection	Protecting assets also means protecting them efficiently — i.e., not wasting resources in the process. Wasting resources in the name of security robs assets just as would other threats.

Table 1: Business Drivers of Solution Security

Case in Point — Corporate Income Tax

To what extent these business drivers apply to a solution depends on the role that particular solution plays in the success of the business. Some solutions have a bigger security profile than others. Compromise a "bigger solution" (along these six metrics) and you incur more risk. Conversely, if you fortify that solution along these metrics, you'll also fortify much of the business as a whole.

For example, with corporate income tax there is tax accounting, compliance, forms preparation, and reporting. Vertex is a leader in this field and provides software which it makes available on a CD or in a hosted environment. Organizations can access the hosted versions over the Internet or install the Vertex software on their own servers. Since we support both deployment models, we have a natural vantage point from which to view each model's strengths regarding security.



First, it's important to recognize the reasons why corporate income tax has a big security profile, we see four key factors:

- Highly sensitive information
- Mission critical data
- Rigorous regulatory requirements
- High business payoffs

Hosted solutions measure up very well, especially for corporate income tax that has major security profiles to consider. Hosted solutions benefit from inherent advantages in four specific areas, as the Vertex experience proves. These four are:

- Best-of-breed technology
- Best practices
- Data integrity and privacy
- Asset protection and business continuity

Advantage #1 — Best-of-Breed Technology

Many best-of-breed technologies also, as a result, deliver best-of-breed security. Thus, by virtue of the hosting model itself, customers receive these benefits uniformly at low incremental cost. Those costs — measured in money, labor, and disruption — are amortized over all customers, all of which benefit simultaneously from any single technology upgrade. Here are four examples:

SHADOWING

One of the technologies used by Vertex to ensure data integrity and system reliability is shadowing. That's when a customer gives our technical support staff verbal and written permission to electronically "look over their shoulder" and see how the user is actually interacting with the software. This eliminates the need for a company's finance staff to describe what's happening over an open phone line or to fax screen shots over an open line — steps which are not only insecure but which increase the likelihood of errors. When a support person actually sees where the user is having issues, they can suggest resolutions quicker, confirm the user is actually performing the suggested fix, and see the result immediately.

FROM-ANYWHERE USER ACCESS

Perhaps the least obvious hosted advantage is the sheer ability to use the solution from anywhere there is a web connection. From-anywhere access, combined with other features like Citrix thin client and robust connection security (more on that later), means that information — on the one hand — is much easier to share among those that need it while — on the other hand — does not need to move around the Internet or internal networks in order to be shared. Offices in different regions can each gain access to the information for which they have a legitimate need; yet the information never leaves the host's facility. Information is more likely to remain private if users do not feel they have to share data through "out of band" channels.



THIN CLIENTS

The advantage — especially in the case of large profile solutions like corporate income tax — is that solutions can be optimized for performance and function without the restrictions imposed by “lowest common denominator” client hardware, web browsers, and operating systems. Vertex can make its corporate income tax solution as robust as needed without having to push the logic that implements that functionality over the wire. Much of that functionality, of course, enables the tax application — but much of it also enables security features to ensure those are also highly optimized.

LOAD BALANCING

When you host multiple clients and multiple application instances, you automatically have more servers over which to balance application loads. That means significant performance increases result from very small resource increases. It’s more economical and easier to keep applications “up to speed” without over-provisioning them, if they’re not isolated on customers’ sites — all factors that go to system reliability, business continuity, and asset protection.

Advantage #2 — Best Practices

Just as best-of-breed host technologies will likely have security benefits, so too will host best practices. These best practices include:

APPLICATION CHANGE

Every change to an application — whether its a new feature, performance improvement, or a bug fix — can open the door to unforeseen problems with security implications. Even an IRS rule change, which some might consider purely functional, can create data integrity issues if formulas are not implemented correctly or ripple effects are not fully considered. A hosted solution provider should implement change procedures that are as good as or better than those an organization would implement just for itself.

24/7 MONITORING

Where a client organization might not monitor its own systems and facilities around the clock, a hosted solutions provider will most certainly do that. This will include monitoring of the running applications as well as physical facilities for break-ins, fire, and other hazards.

SEGREGATED CLIENT DATABASES

Another best practice is to maintain each client’s data separately. This helps ensure privacy and data integrity. It also helps ensure compliance by establishing a clear audit trail of how the data is handled. At Vertex, each client has its own database and can only access its own database. Databases are also backed up separately — with each one individually compressed and encrypted.

Advantage #3 — Data Integrity and Privacy

The Vertex case illustrates the kinds of measures a hosted solution provider can take that are specifically focused on ensuring integrity and privacy. These measures include:



THIN CLIENTS

The hosting environment runs on Citrix Presentation Server, which provides application virtualization on a Windows platform. As previously mentioned, a thin client Citrix approach means financial professionals don't have to bring data in-house to protect it – only pixels and mouse movements go over the wire, not the data.

DATA COMMUNICATIONS SECURITY

Presentation Server uses Independent Computing Architecture (ICA) protocol, a communication protocol by which servers and client devices exchange data in a server environment to separate an application's logic from its user interface. The ICA protocol encrypts and transports an application's screens from the server it is running on to the user's client device, and returns the user's input to the application on the server. As an application runs on a server, Presentation Server intercepts the application's display data and uses the ICA protocol to send this data to the ICA client software running on the user's device.

Communications between the user and Vertex are done via Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) through a web browser and the secured thin clients. Both communication methods utilize industry standard 128-bit encryption algorithms. Communications among Vertex sites are routed over a Virtual Private Network using 128-bit 3DES IPsec tunnel and 1024-bit Diffie-Hellman IKE Phase1 with pre-shared secret key exchange.

PROTECTION FROM INTERNET THREATS

Enterprise-level Firewalls are in place to secure the hosted application and client data from the public Internet. Only encrypted HTTPS and secured thin-client (ICA) traffic can reach the hosted applications. To facilitate initial user connections, unencrypted HTTP traffic is permitted for initial contact but is redirected to the secured HTTPS protocol prior to login. Only secured traffic reaches the applications that contain client data. In addition to the protocol and port-specific blocks, the firewalls also employ Network Address Translation (NAT) to conceal internal network addresses from public view and probing across the Internet. A host of Denial-of-Service (DoS) prevention capabilities are also implemented within the firewalls at the application, session, transport, and network layers of the OSI model – minimizing the threat of downtime and further securing sensitive client data from malicious access.

VIRUS PROTECTION

With the firewall enabled to prevent attacks at the application layer, the firewall is able to block several forms of viruses. In addition, a second tier of protection is maintained on the servers. Industry standard enterprise level virus protection is installed on all servers in the host site. The servers are automatically updated, as new virus definitions are made available.

Advantage #4 — Asset Protection and Business Continuity

Other measures specifically focus on asset protection and business continuity. Vertex examples include:



PHYSICAL SECURITY

The Vertex data center is engineered with five levels of security. Biometric, fingerprint access scanning technology verifies identity for authorized access into the facility. Proximity card access with personal identification number, in addition to biometric clearance, is required to enter/exit the facility. All steel mesh cabinets are fitted with combination locks. As a result, no keys can be lost or duplicated. Video surveillance cameras are hidden throughout the facility which are monitored by a 24x7 network operations center (NOC) and track and record access throughout the facility. In addition, strategically placed sensor devices alert Data Center NOC personnel of any forced entry.

FIRE SUPPRESSION

The fire suppression system is a dry pipe system filled with compressed air. Stationary smoke detectors are also installed. All HVAC systems have internal sensors tied directly into smoke detection system. They also have sensors in self-contained pans, as well as a sensor inside the HVAC itself. This is set to a constant 50 percent humidity. All Alarms, sprinkler system, HVAC, fire suppression systems fire extinguishers are routinely inspected and are all tied into the central monitoring system.

DISASTER FAILOVER

To provide an alternate production facility for disaster failover, Vertex has contractually secured space and services in a separate site that is situated elsewhere in the country. This alternate site has been established with Vertex-owned application servers, database servers, and web servers. Current versions of the Tax Products are maintained on the alternate site. Full backups of individual client databases taken daily from the primary production site are restored the next day into the alternate site. Prior to the start of hurricane season, and during the approach of any named storm that threatens the Florida coast, a test of the failover process is done.

FULL SOLUTION SECURITY

A hosted solution provider is clearly well positioned to invoke best-of-breed technologies and practices at multiple layers — a position Vertex properly exploits. Often what's good for the solution's functionality is also good for the client organization's security — as the Citrix thin client example in particular illustrates. Just as hosted solutions deliver applications on-demand, they also deliver security on-demand, along with minimal implementation delays, lower total cost of ownership, and high professional standards.

Another way to assure those standards are applied is to ask to see a provider's Statement on Auditing Standards (SAS). For example, Vertex maintains a SAS No. 70 Type II. A Type II report includes an organization's description of controls and the detailed testing of those controls over a minimum six-month period. In addition, the requirements of Section 404 of the Sarbanes-Oxley Act of 2002 make SAS 70 audit reports even more important to the process of reporting on effective internal controls at service organizations.

Standards compliance, as well as peace of mind, requires full solution security. That's more than just protection from attacks and disasters. It means a platform fully optimized for business performance. Hosted solutions provide inherent advantages across the entire solution security spectrum when you work with a prepared, experienced partner like Vertex.