Important issues to consider including security before deploying Cloud ERP

Many organizations considering migrating from existing, lower performance and aging ERP systems with Cloud-based system face important challenges. As with any other change there are misconceptions and fears such as how secure is the system from hackers? First the misconceptions.

Misconception #1 – "Cloud-based applications only run over the Internet."
Explanation: Cloud-based applications run over the Internet by default, but the same applications also run on completely private networks. Even if your company has no intention of letting "Internet users" access your Accounting or ERP system, the fundamental advantages of cloud-based applications still provide a game changing edge vs. older systems.

Misconception #2 – "Cloud-based is the same as SaaS."
Explanation: Cloud-based applications enable Software as a Service (SaaS) – not the other way around. SaaS is a powerful business model for delivering cloud-based applications and corresponding services, but it is not the only business model, or even the most predominant one. Cloud-based applications are available under almost every conceivable deployment, licensing and support model – from traditional license to open source and from on-premises to hosted deployment.

Misconception #3 – "Cloud-based applications are not customizable."
Explanation: There is no technical barrier to adding the most sophisticated features for customizability to Cloud-based applications. Differences in customizability between products are a result of developer know-how, skill, choices and focus. If a product is not customizable enough, look to the developer, it's not the technology holding it back.

Misconception #4 - The biggest concern of all, Security?
Achieving the highest levels of security in a cloud-based ERP application, at reasonable cost, is now possible using the same standards-based web technologies used by bank web sites. At a minimum these include:

Encryption: Web standards like SSL and TLS encapsulate application-specific protocols like HTTP to form encrypted HTTPS so no one can hijack a web session or read the data – even if it is passing through an open Wi-Fi network. HTTPS introduces negligible computing overhead so there is no excuse to not use it. Even Google's free Gmail system supports HTTPS as its default behavior.

Server side processing: Most well designed ERP applications for the Cloud do not install files or components on user machines. Business logic is executed only in the server. Not only does this reduce expense by not requiring each machine to be updated with every version or patch, it also insures the system will not accept manipulated data from a malicious program in the browser.
Other techniques to improve security using cloud computing include:

Cloud Backup: Lost and misplaced backup tapes can potentially be the source of large security breaches. Even if you run your ERP application on-premises it may be safer and less expensive to automatically keep backups in the cloud. Vendors specialize in backing up live on-premises SQL databases and virtual machine images to large public cloud infrastructure providers like Amazon and Azure.

Security tokens: Borrowed or stolen passwords can circumvent the most sophisticated technologies. Augmenting passwords with key fobs that generate time limited passwords provides physical access control from anywhere at very reasonable cost. Secondary, one- time passwords can also be sent to a cell phone via SMS. Products include SecurID from RSA, and many others.