JOURNEY TO THE SECURE CLOUD

Building the Transparent Cloud

Expedient expands to the cloud with a focus on auditability and security

Intel IT Centre

If you're like a lot of enterprise IT teams, you're interested in getting the benefits of cloud computing but have questions about the confidentiality, integrity, and availability of the cloud. Given highly publicised service failures and data breaches, I can't blame you. If you're going to get out of the hardware ownership business and focus on the IT elements that really matter to your business, you need to be able to count on consistently reliable and transparent cloud services.

My company, Expedient Communications, provides cloud computing, managed services, and network connectivity. As such, my team is working to extend or replace the technical foundation for many of our customers' businesses. The lessons we're learning might help your team as you build private clouds and evaluate external cloud services.

As a starting point for a secure and highly available cloud service, you need a redundant system architecture that builds security throughout the technology stack. My team created self-contained pods that include compute, storage, and I/O. We chose the Intel® Xeon® processor X5650 as the pod building block, since it gives us a good balance of compute and memory capacity. You can replicate this type of modular architecture across the organisation to give you a solid base for high availability.

To secure the cloud, you need to integrate security components at every layer of the Open Systems Interconnection (OSI) model, from the physical through the application layer. It's also important to ensure that each component has a robust reporting capability, so you can monitor and track potential issues and threats and respond quickly to address them.

If you're evaluating external cloud services for security, I recommend looking for vendors that are open and transparent and encourage you to put them to the test. They should welcome you to audit your deployed environment and encourage engineer-to-engineer collaboration. They should also make their personnel, policies, and practices available for you to audit. If your industry has regulatory requirements, look for a vendor that's willing to participate in your external audits. If it's relevant to your industry, you should be able to definitively know where your data physically resides. Bottom line, you should feel confident that your cloud provider is protecting your data with controls that are equivalent if not better than those you have within your own walls.

Threats continue to evolve, of course, so information security is never finished. That's true whether you're in the public cloud or the enterprise data centre. We continue to research, develop, and deploy new security solutions, and we're looking to new technologies such as Intel® Trusted Execution Technology (Intel® TXT) to help us start creating a chain of trust between our operating environment and our customers' environments. We are conducting a pilot using Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) with Intel® 10 Gigabit Ethernet Server Adapters to enhance encryption and decryption performance and overall throughput, and we expect to move toward implementation later in 2011.

Read more about Expedient's approach to the cloud at www.expedient.com.

expedient COMMUNICATIONS

Alex Rodriguez
Vice President, Systems Engineering and Product Development
Expedient Communications

What I did

- Led Expedient's expansion from managed service provider to cloud computing

What I learned

- Start with a modular architecture
- Address security throughout the solution stack
- Avoid black-box computing—aim for transparency
- Keep exploring

intel

0811/YMB/TDA/XX/PDF

325890-001UK