AWE Statement on Security

AWE's workstation-based products utilize proprietary security processes and tests to protect against viruses when connected to a network. The operating system is purpose-built as a kiosk to run only AWE applications and AWE licensed materials. Any operating system components or functions that are not specifically required for our systems to operate are either disabled or are removed completely. The network functions permitted by AWE are carefully limited to sideline the types of network capabilities that create vulnerabilities to viruses and worms.

AWE's products share a common set of secure, encrypted network functions specific to the tasks of downloading updates, uploading utilization statistics, activating personalized education plans, synchronizing children's data and accomplishments, and cloning workstation configurations. Only these secured network functions are permitted into and out of AWE's workstations and they are only permitted to and from AWE's secure servers.

All of these feature sets can be individually activated or deactivated by the customer including allowing or disallowing any networking. Additionally, during synchronization transactions, data passed to the cloud for synchronization to other workstations are virus scanned as a component of that process.

AWE features enhanced capabilities to import both configuration and user files from one AWE workstation to another (Cloning). File encryption within the export and decryption of manual import processes limits any exposure to viral modification. Any files not created by and adhering to these processes are simply not recognized nor imported.

In addition, corresponding limits are placed on network port access to activities not corresponding to AWE controlled functions.

While no computer communicating with external computers is 100% invulnerable to viral attack, there are no recorded virus incidents with any of the thousands of AWE workstations at customer locations.