

implanting malicious code and other vulnerabilities to exploit only after the devices have been implemented in an enterprise environment. It may prove necessary to adopt a security paradigm like the Forrester Zero Trust model for IoT devices.

Where possible, enterprises should proactively set the stage by isolating these devices to their own network segment or V-Lan. Additionally, technologies such as microkernels or hypervisors can be used with embedded systems to isolate the systems in the event of a security breach.

## 7. Rapid demand in bandwidth requirement



A study conducted by Palo Alto Networks Inc. revealed that between November 2011 and May 2012, network traffic jumped 700% on networks the vendor observed, largely due to streaming media, peer to peer applications and social networking. As more devices connect to the Internet, this number will continue to grow.

To ensure high availability of their services, enterprises must consider adding bandwidth and boosting traffic management and monitoring. This will not only mitigate business continuity risks, but also prevent potential losses. In addition, from the project planning standpoint, organizations would need to do capacity planning and watch the growth rate of the network so that the increased demand for the required bandwidth can be met.