

UNIQUE FABRIC LAYER TO STREAMLINE AND SECURE DATA TRAFFIC WITH CLOUD INFRASTRUCTURE

Since its introduction, cloud computing is steadily garnering strong momentum from corporate customers, mainly attributed to its unique capacity to transform static and privately dedicated resources to a more dynamic and agile information technology (IT) computing framework. However, a major concern impeding its widespread adoption is the inability of enterprises to stringently control data and application traffic between the physical and cloud environment. With different types of hypervisors utilized for private and public cloud frameworks and the intensely diverse network configuration for legacy physical network infrastructure; network administrators are facing a daunting challenge to secure enterprise data traffic.

In an attempt to address this recurring concern, Silicon Valley-based Imera Systems has come to the forefront and developed the Imera Virtual Fabric solution. This innovative solution represents a logical fabric layer, which envelops the existing physical infrastructure.

Built on a hypervisor-independent model, the solution's core functionality is to provide utmost protection for all data and application traffic between the physical and cloud environment. A key component of the solution is the Unified Cloud Security Management feature, which primarily offers a more intelligent mechanism to control all access to the enterprise or data center cloud network. Resultantly, leveraging on its criticality, this security feature could precisely identify any external threats and could instantly implement adequate countermeasures. Another noteworthy element of the solution is the Virtual Compliance feature, which empowers the solution to execute end-to-end monitoring of all operations for cloud or enterprise access and guarantees that each application complies with corporate and regulatory policies. Further to this, it could also astutely identify any suspicious behavioral activities within the corporate network. On top of that, the solution has equally incorporated the Secure Collaboration feature. As a result, this virtual security platform could offer continuous protection for countless communication channels for dispersed remote users across disparate geographical locations. This could prove fundamental to shield the enterprise perimeter against unwarranted access via remote terminals.

Leveraging on its highly elastic characteristics, it could dynamically safeguard critical communication and access channels established between the two disparate aforementioned environments. Thus, this integrated security solution promises to go beyond the typical security appliances for legacy physical servers and hence provides a more comprehensive security defense for the enterprise network. That apart, the solution could allocate adequate business resources to ever-changing user demands. Hence, the solution could deliver unparalleled IT agility and optimize business operations to a new dimension altogether. Another notable aspect of the solution is that it could seamlessly integrate with existing physical infrastructure without the need for any remodeling or reconfiguration. Via a centralized management unit, it could effectively administer all operations running synchronously. As such, it promises to decrease operating cost and resources while offering sound protection for the enterprise network.

At this point of time, Imera Systems has established strategic partnerships with VMware, leading semiconductor companies and leading electronic design automation (EDA) vendors. This could thereby demonstrate the viability of their solution suite and the immense potential of Imera Systems to have a leading role within the virtual security space. With satellite offices in Taiwan and China; it could serve as a conduit to further expand their global presence and solidify their position within this domain in the years to come.

Details: Timothy Goh, Media Contact, Imera Systems Inc., 100 Century Center Court, Suite 403, San Jose, CA 95112. Phone: 408-453-2464. E-mail: timgoh@imeras.com. URL: www.imeras.com.