Prologix signs up with Tramigo

Prologix Distribution has signed the Authorized Distributorship Agreement with Tramigo, the world leader in tracking products which is headquartered in Finland and has operations worldwide. The company is a pioneer in the field of vehicle and fleet management software and hold the reputation of creating first global consumer brand in tracking products.

Tramigo vehicle tracking device combines the GPS (Global Positioning System), GSM (mobile network) and geographical information (TLD Tramigo Landmark Data) into one device. Tramigo uses GPS satellites in positioning itself in very accurate standing, after which it finds the closest and well known landmark to that point from its internal memory and sends the information across to any authorized mobile phone as a text message using the GSM network. The actual location of your Tramigo tracking device is sent back to your phone as a message.

Tramigo product range includes T23 Tracking Device Series, Tramigo for Service Providers , User Interface Software, Personnel Tracking software and Accessories. Tramigo is accessible anytime, anywhere – even when offline. It can be used in any specific language. It controls your cost because there is no monthly fees or licensed payments. The software is highly reliable with support services which are beneficiary after purchase. With Tramigo, the location data is easily accessible.

Bit9 + Carbon Black extends reach in UAE

Bit9 + Carbon Black has continued to reinforce its presence in the UAE, with its leading advanced endpoint threat detection and response solution, Carbon Black--generating high interest from the local market. The company recently showcased Carbon Black's modern features before industry leaders, stakeholders and prospective clients in a high-level seminar in Dubai. The solution's real-time detection and response capabilities were also highlighted during the event through the presentation delivered by Dell SecureWorks, which uses Carbon Black in its Advanced Endpoint Threat Detection (AETD) managed service.

The seminar held at the Burj Al Arab presented how Carbon Black delivers continuous monitoring and recording of all activities on endpoints and servers, customizing detection, and responding to network intrusions in seconds. Aquib Aftab, Regional Director, Bit 9 + Carbon Black in the Middle East said," Carbon Black reduces the cost and complexity of incident response by replacing 'after-the-fact' manual data acquisition with continuous monitoring and recording of all activity on endpoints and servers. Our collaboration with Dell SecureWorks helps its clients significantly reinforce their online defenses. We look forward to forming partnerships with other organizations in the UAE and other Middle Eastern countries as we continuously intensify our initiatives against cyber attacks in the region and the rest of the world."

Fortinet announces HP AllianceOne program membership

Fortinet has joined HP's AllianceOne Partner program with the HP Networking Specialization. As enterprises and Service Providers look to effectively deploy security in their datacenters, leveraging the benefits of Software Defined Networking (SDN) and Network Function Virtualization (NFV), this partnership lays the foundation for Fortinet to deliver pre-integrated SDN-optimized security solutions to enhance HP's SDN security portfolio. These solutions will extend the agility and operational benefits of SDN security solutions, delivered from physical or virtual FortiGate security appliances, enabling customers to reduce OPEX, strengthen security and derive more value from their investments in HP SDN and Fortinet Security.

As enterprises and Service Providers move towards SDN architectures, not only is security a logical intrinsic Data Center element that needs to fit seamlessly in such architectures, but security services like those from FortiGate appliances can utilize the programmability of the network to deliver more capabilities than previously possible.

In HP SDN environments, FortiGate appliances or virtual machines (VMs) could proactively instruct the HP VAN controller to contain infected endpoints at the closest switch in an automated programmable way. This would significantly reduce the risk of threat proliferation and data theft, without any incremental investment required for containment technologies.