Honda New Zealand Secures Nationwide Network With Fortinet

eLearning Made Easier With Fortinet

SUNNYVALE, CA, Sep 07, 2010 (MARKETWIRE via COMTEX News Network) -- Fortinet(R) (NASDAQ: FTNT) -- a leading network security provider and a worldwide leader of unified threat management (UTM) solutions -- today announced that Honda New Zealand has deployed FortiGate-310B appliances as well as Fortinet's analysis and management appliances, FortiAnalyzer(TM) and FortiManager(TM). The FortiGate appliances are being used for broad network security protection including firewall, antivirus, Web content filtering, intrusion prevention and SSL VPN functionality. In addition, franchises can securely connect via SSL VPN tunnels back to headquarters to access eLearning videos rather than using unsecure memory sticks.

Honda New Zealand is the regional division of Honda Motor, a Global 51 company. After looking at other vendors including Juniper, Cisco and SonicWall, Fortinet was selected for the product line's ease-of-use, multi-threat approach to network security and easy reporting on network usage.

Using an MPLS network provided by a third party was proving to be extremely costly for Honda New Zealand. As part of a larger network infrastructure overhaul, the company decided to look at best of breed vendors for multiple parts of their network including security.

"Since deploying the Fortinet solution, we've reduced communications costs by nine times because we no longer have to pay for an expensive MPLS network," said Simon Taylor, project manager for Honda New Zealand. "In addition, Fortinet made it extremely easy for us to add new functionalities because we don't have to buy new appliances."

Two FortiGate-310B appliances are deployed in high availability active/passive mode and are located at the company's Auckland headquarters. The appliances are providing firewall, antivirus, Web content filtering, intrusion prevention protection as well as SSL VPN connectivity and all Honda New Zealand corporate data, including information from the used car Website, passes through the FortiGate-310B appliances.

A new aspect of the Fortinet deployment is the portal for eLearning. Previously, employees and franchises would use memory sticks and DVDs in order to access educational videos. Since deploying the FortiGate appliances, these employees and franchises can now create an SSL VPN tunnel back to headquarters to access the videos. Not only is time saved, but the threat of viruses and videos getting into the wrong hands is now diminished.

FortiManager and FortiAnalyzer are reducing management complexity and allow for much more detailed analysis of network usage as well as easily and automatically creating monthly and ad hoc network reports. These reports provide management teams with greater visibility into employee usage on company network infrastructure. Un-monitored computers in public areas are set up for employee personal use during lunch hours or break time.

"The Fortinet appliances have allowed us to deploy one appliance and use it for multiple functionalities," said Simon Gould-Thorpe, CIO at Honda New Zealand. "As part of a globally ranked company, it was imperative for us to have the best products available on the market. Honda's network is only as strong as its weakest link and we're very confident in what Fortinet has provided us."

"Worldwide enterprises are increasingly turning to Fortinet to protect their most critical assets," said Kevin Dyson, vice president for Fortinet Australian and New Zealand. "By enabling an enterprise to pick and choose which network security functionality they'd like to deploy, and, all within a single appliance, Fortinet is reducing capital and operational expenditure costs associated with protecting the network infrastructure."

Honda New Zealand is currently deploying either a FortiGate-51B appliance or FortiGate-110C appliance, depending on the network requirements at each dealership, at all of its 35 nationwide dealerships. The appliances will allow dealerships employees to securely and efficiently connect back to Honda New Zealand's headquarters as well as to help protect the dealership network from malware and network attacks.

Fortinet's FortiGate systems are ASIC-accelerated security appliances that integrate essential security and network functionalities such as firewall, VPN, intrusion prevention, Web filtering, antivirus, anti-spam, data leakage protection, application control, traffic shaping and WAN acceleration. All FortiGate systems are kept up-to-date automatically by Fortinet's FortiGuard(R) Network, which helps ensure protection against the most damaging, content-based threats from email and Web traffic such as viruses, worms, intrusions, other unwanted network traffic and more -- around the clock and around the world.

About Fortinet (www.fortinet.com) Fortinet (NASDAQ: FTNT) is a leading network security provider and a worldwide leader of unified threat management (UTM) solutions. Fortinet solutions were built from the ground up to integrate multiple levels of security protection -- including firewall, VPN, antivirus, intrusion prevention, Web filtering, spyware prevention and antispam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in five programs by ICSA Labs: Firewall, Antivirus, IPSec VPN, Network IPS and Antispam. Fortinet is based in Sunnyvale, California.

Copyright Copyright 2010 Fortinet, Inc. All rights reserved. The symbols (R) and (TM) denote respectively federally registered trademarks and unregistered trademarks of Fortinet, Inc., its subsidiaries and affiliates. Fortinet's trademarks include, but are not limited to, the following: Fortinet, FortiGate, FortiGuard, FortiManager, FortiMail, FortiClient, FortiCare, FortiAnalyzer, FortiReporter, FortiOS, FortiASIC, FortiWiFi, FortiSwitch, FortiVoIP, FortiBIOS, FortiLog, FortiResponse, FortiCarrier, FortiScan, FortiDB and FortiWeb. Other trademarks belong to their respective owners. Fortinet has not independently verified statements or certifications herein attributed to third parties and Fortinet does not independently endorse such statements. This news release may contain forward-looking statements that involve uncertainties and assumptions. If the uncertainties materialize or the assumptions prove incorrect, results may differ materially from those expressed or implied by such forward-looking statements and assumptions. All statements other than statements of historical fact are statements that could be deemed forward-looking statements, including but not limited to, any statements related to expected trends in cybercriminal activity. These trends are difficult to predict and any stated expectations regarding these trends may not ultimately be correct. Fortinet assumes no obligation to update any forward-looking statements, and does not intend to update these forward-looking statements.

FTNT-O

Media Contact:

Maeve Naughton
Fortinet, Inc.
(408) 486-7819
mnaughton@fortinet.com

SOURCE: Fortinet

mailto:mnaughton@fortinet.com

Copyright 2010 Marketwire, Inc., All rights reserved.

News Provided by COMTEX