Instituto de Salud Carlos III Protects Its Web-Based Applications With Fortinet

Spanish National Organization Chooses FortiWeb(TM) Web Application Firewall for Its Advanced Features and Simplified Deployment

SUNNYVALE, CA -- (MARKET WIRE) -- 04/11/11 -- Fortinet® (NASDAQ: FTNT) -- a leading network security provider and the worldwide leader of unified threat management (UTM) solutions, today announced that the Instituto de Salud Carlos III, a national public research and scientific support organization for the promotion of biomedical and health science research in Spain, has selected its FortiWeb™ to protect its web-based applications from security threats. Fortinet's web application firewall was chosen for its advanced features and simplified deployment.

Instituto de Salud Carlos III (ISCIII) is missioned to develop and provide high-quality techno-scientific services for the Spanish National Healthcare System and society as a whole. One year ago, the ISCIII decided to optimize its IT infrastructure in order to eliminate server duplication and further increase information security. Since the public organization had been relying on the FortiGate® multi-threat security appliances for its network security for the past three years and had been very satisfied with Fortinet's technology, it decided to replace its DMZ configuration, which involved multiple servers, with FortiWeb appliances. Configured to redirect web application requests to internal servers, FortiWeb became the sole point of access for all web-based applications from any of ISCIII's internal and external networks.

"The number of users and the variety of access points used to enter our network means that we need a fast, reliable and secure communications network, which includes the protection of our web applications from Internet threats," said Antonio José Arenas from the Systems Coordination and Information Technologies Unit at ISCIII. "Protect all our web applications, using different technologies, and maintain a high level of security throughout the life cycle of those applications was simply impossible. We chose FortiWeb because it provides us with a uniform and umbrella solution for web applications security and reduces complexities while representing a cost-effective investment."

Working with Fujitsu España, through the Altimate distributor, ISCIII deployed last October two FortiWeb-400B to secure the sensitive information accessible from its Web applications, leveraging the following key features:

- The Institution has protected its webmail against user identity theft by implementing a "Brute Force Login" security policy,
- A "SQL Injection" policy was configured in order to prevent web application hacking. In fact, several of the ISCIII's applications were hacked in the past with links to malicious websites incorporated in the applications,
- The institution has applied the "Information Disclosure" policy to help prevent attacks on servers, which store the applications containing sensitive information.

FortiWeb has also been configured to perform SSL application processing, which frees up valuable resources (CPU & RAM) that can then be used by other servers as the environment is fully virtualized.

Instituto de Salud Carlos III started to use Fortinet's technology in 2007 when it replaced its perimeter firewalls, which could no longer cope with the increasing demand for network services. ISCIII deployed two FortiGate-1000A appliances in its main data center to provide high-performance, reliable network security while simplifying configuration. ISCIII activated the following security functions within the devices: firewall, IPS, antivirus, antispam, web filtering, and VPN. In addition, Instituto de Salud Carlos III has implemented two FortiGate-800 and two FortiGate-60C appliances to provide IPS and antivirus functions in two of its campuses. ISCIII also opted for one FortiAnalyzer™-800B device, which aggregates log data from the various FortiGate appliances and provides key reporting and analysis tools, as well as one FortiManager™-400B, which is used for the centralized configuration and management of the Fortinet deployment.

"As all organizations, public or private, are increasingly relying on the Internet for critical applications, they de facto become more vulnerable to cybercriminal attacks," said Patrice Perche, senior vice president of international sales & support at Fortinet. "FortiWeb improves the security of confidential information and goes beyond traditional solutions to provide XML security enforcement, application acceleration, and server load balancing. It represents a natural expansion of FortiGate deployments to offer our customers a broad solution for protecting networks and applications at the core and perimeter."

About Fortinet (www.fortinet.com)
Fortinet (NASDAQ: FTNT) is a worldwide provider of network security appliances and the market leader in unified threat management (UTM). Our products and subscription services provide broad, integrated and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Our customers include enterprises, service providers and government entities worldwide, including the majority of the 2009 Fortune Global 100. Fortinet's flagship FortiGate product delivers ASIC-accelerated performance and integrates multiple layers of security designed to help protect

against application and network threats. Fortinet's broad product line goes beyond UTM to help secure the extended enterprise -- from endpoints, to the perimeter and the core, including databases and applications. Fortinet is headquartered in Sunnyvale, Calif., with offices around the world.

Copyright © 2011 Fortinet, Inc. All rights reserved. The symbols ® and ™ 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, such as ISCIII, 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. These trends may be 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

Add to Digg Bookmark with del.icio.us Add to Newsvine

Media Contacts:

Barbara Maigret

Fortinet, Inc.

+33 (0)4 8987 0552

bmaigret@fortinet.com

Source: Fortinet

News Provided by Acquire Media