

Case Study

Ziekenhuis St Jansdal Selects Finjan to Secure Its Network from Web Threats



Challenge

To secure Hospital St Jansdal's IT infrastructure from Web-based Crimeware threats, while protecting patient data and increasing productivity.

Solution

Finjan Vital Security™ Web Appliances, featuring real-time content inspection to prevent malicious web content from entering the Hospital's network.

Results

Unsurpassed Web security and compliance with various patient information protection regulations.

Background

Ziekenhuis St Jansdal (Hospital St Jansdal) is a medium-sized Dutch hospital located in the City of Harderwijk (The Netherlands). With its 1,400 employees and 85 medical specialists, it strives to provide optimal and professional healthcare to the inhabitants of North-West Veluwe and part of Flevoland.

As a healthcare institution, St Jansdal must protect the personal and medical data of its patients. The Wet Bescherming Persoonsgegevens (WBP – Personal Data Protection Act) and the Directive Goed Beheerd Zorgsysteem (GBZ) provide guidelines that organizations such as hospitals must follow. They outline the minimal requirements for a system in the area of security, performance, connectivity and access, as well as storage and transmission of data.

All digital data need to be protected in accordance with the NEN7510-norm, consisting of national guidelines for security of information in the healthcare sector. This norm (specified for complex organizations such as hospitals in NEN7511-1) ensures the quality of availability, confidentiality, and integrity of patient data.

Hospital St Jansdal was looking at a security solution that could both protect personal and patient information as well as ensure safe Web browsing for their employees using the Internet. The hospital therefore needed a Secure Web Gateway solution that would protect its network against the growing wave of dynamic Web threats.

"Considering the sensitive nature of our information and communications, there is no room for us as a hospital to compromise in the area of information security and compliance," stated Karel Lankhorst, Head of Management & Support ICT at Hospital St Jansdal.

Business Challenge and Requirements

Hospital St Jansdal is both legally and ethically bound to protect personal and patient information that is a prime target for cybercriminals who are using obfuscated malicious code as their crime tool. At the same time, the Hospital also wants to guarantee its employees secure access to Internet and to be compliant with various applicable rules and regulations.

"We realized that our current security solution had limitations when it came to detecting and blocking Crimeware, which had not only an impact on the safety of our network, but also on our need to comply with the WBP and NEN7510 regulations," stated Karel Lankhorst, Head of Management & Support ICT at Hospital St Jansdal.

Previously, Hospital St Jansdal worked with a standard proxy server that could not fully detect and block dynamic malicious web content from entering the Hospital's network.

For its new security solution, Hospital St Jansdal was therefore looking at effective protection against Crimeware and Web 2.0 attacks in real time. The Hospital's employees must have safe Internet access while performing their duties. They must be sure that all their online activities are secured and that none of their confidential patient data and information will be compromised by Crimeware and malware.

After seeing Finjan's Secure Web Gateway solution in action at a fellow healthcare organization, Hospital St Jansdal opted for Finjan's real-time solution that prevents Crimeware, Trojans and other malicious Web content from entering its network.



"Since deployment of Finjan's Secure Web Gateway solution, our network security has dramatically improved, safeguarding our patient data and information"

Finjan's Secure Web Gateway Solution

With these requirements in mind, Hospital St Jansdal chose Finjan's Secure Web Gateway solution, especially after seeing its performance at a fellow healthcare institute.

It was clear to Hospital St Jansdal that Finjan was the preferred vendor with a true solution against dynamic malicious content such as Crimeware and Trojans.

The deployed solution is based on Finjan's award-winning Vital Security™ Web Appliance NG-5000. ISSUE Information Technology, Finjan's Premier Partner in The Netherlands, implemented the solution. It features patented active real-time content inspection technology to detect and block inbound and outbound known and unknown malicious Web threats.

Deployed at the Internet gateway, the two redundant NG-5000 appliances currently support the Hospital's 500 users in a high availability configuration. These "all-in-one" appliances feature Finjan's active real-time content inspection, Vulnerability Anti.dote, and Kaspersky's Anti-Virus.

Finjan's solution is known for its ability to assist organizations with their compliance issues, such as HIPAA. Since St Jansdal Hospital needs to be compliant with various rules and regulations, it was especially impressed with this ability.

Finjan's active real-time content inspection technology is uniquely capable of analyzing incoming and outgoing Web content in real time regardless of its source, by breaking down the code and understanding its true intent without executing it on the end user's machine. Finjan delivers malicious code detection and prevention, allowing organizations to safeguard one of their most valuable assets - their information.

Key Benefits and Results

Finjan's Secure Web Gateway solution enables Hospital St Jansdal to meet its requirements:

- Securing its IT network from malicious and stealthy Web threats, including Crimeware and Trojans, that often bypass signature-based security methods
- Protection of personal and patient information
- Compliance with WBP and NEN7510 regulations
- Integrated security solution with single point of management, provisioning and reporting

Finjan's solution enables St Jansdal Hospital to improve network performance and to comply with various rules and regulations. This is especially important for this hospital, since it uses the Internet as a main business tool.

With Finjan's solution, personal and patient data are protected, thus ensuring compliance with WBP, NEN7510, NEN7511-1, and GBZ.

It enables Hospital St Jansdal to secure its network granting its 500 employees secure Internet access.



“Finjan's active real-time web security protects our network from stealthy Trojans and Crimeware”

Karel Lankhorst,
Head of Management & Support ICT

For Additional Information

For more information, please visit www.finjan.com or contact our regional offices:

San Jose, USA

Toll Free: 1 888 FINJAN 8 (1 888 346 5268)
Tel: +1 408 452 9700
Email: salesna@finjan.com

New York, USA

Tel: +1 212 681 4410
Email: salesna@finjan.com

United Kingdom

Tel: +44 (0)1252 511118
Email: salesuk@finjan.com

Germany

Tel: +49 (0)89 673 5970
Email: salesce@finjan.com

The Netherlands

Tel: +31 (0)33 454 3555
Email: salesne@finjan.com

Asia Pacific

Tel: +972 (0)9 864 8200
Email: salesapac@finjan.com

Israel

Tel: +972 (0)9 864 8200
Email: salesis@finjan.com

Finjan - Securing Your Web

Finjan Secure Web Gateway Appliances for Enterprises



NG-8000S



NG-6000S



NG-5000S

© Copyright 1996 - 2008. Finjan Inc. and its affiliates and subsidiaries. All rights reserved.

All text and figures included in this publication are the exclusive property of Finjan and are for your personal and non-commercial use. You may not modify, copy, distribute, transmit, display, perform, reproduce, publish, license, create derivative works from, transfer, use or sell any part of its content in any way without the express permission in writing from Finjan. Information in this document is subject to change without notice and does not present a commitment or representation on the part of Finjan. The Finjan technology and/or products and/or software described and/or referenced to in this material are protected by registered and/or pending patents including European Patent EP 0 965 094 B1 and U.S. Patents No. 6092194, 6154844, 6167520, 6480962, 6209103, 6298446, 6353892, 6804780, 6922693, 6944822, 6993662, 6965968, 7058822, 7076469, 7155743, 7155744 and 7185358 and may be protected by other U.S. Patents, foreign patents, or pending applications.

Finjan, Finjan logo, Vital Security, Vulnerability Anti.dote and Window-of-Vulnerability are trademarks or registered trademarks of Finjan Inc., and/or its affiliates and subsidiaries. Sophos is a registered trademark of Sophos plc. McAfee is a registered trademark of McAfee Inc. IBM Proventia Web Filter technology is a registered trademark of IBM Internet Security Systems. Kaspersky is a registered trademark of Kaspersky Lab. SurfControl and Websense are registered trademarks of Websense, Inc. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation.

All other trademarks are the trademarks of their respective owners. Q2 2008.