

Case Study

Finjan Delivers Top-Flight Web Security to Munich Airport



Challenge

To secure Munich Airport's strategic IT infrastructure from web-based threats, while ensuring zero downtime of mission-critical systems

Solution

Finjan Vital Security™ Web Appliance for proactive behavior-based security against known and unknown web attacks

Results

Unsurpassed web security, zero downtime of mission critical airport IT systems and secure information flow with external systems

Background

The "Franz-Josef-Strauss-Airport" in Munich is the second largest airport in Germany. For the second year in a row, this international airport was named the "Best Airport in Europe" in 2006 in an international survey of more than seven million passengers from 93 countries.

Munich Airport continues to play a central role in Bavaria's economic development. Geographically situated in the center of the world's largest market – the European Union – Munich Airport serves as a major transportation hub for both Germany and the rest of Europe. In terms of air traffic, the airport handles approximately 400,000 take-offs and landings per year, while approximately 30 million passengers are dispatched annually.

Munich Airport depends on an extensive and complex network of information systems to manage logistics, baggage transfer, catering services and cleaning crews for its high-volume operations. If any of these systems were to shut down, flights could be delayed and passengers' baggage might be lost. Passport control, customs and immigration systems must all work in sync in order to allow busy passengers and cargo shipments to stay on schedule.

Accordingly, Munich Airport has very demanding security and availability requirements for its IT systems, which must remain online at all times to ensure the efficiency of its daily operations.

Business Challenge and Requirements

Downtime of information systems, due to any reason, can wreak havoc with flight schedules and spoil the passenger experience. High availability dictates proactive security, since web-based attacks (e.g., Denial of Service attacks) and undetected malicious code may compromise information systems and crash user terminals. **"We required a proven solution that ensures the highest level of security against web attacks, known and unknown, which often elude traditional security measures,"** stated Marc Lindike, Vice President Operations and Services at Munich Airport.

Many of the airport's business-critical applications use Active Content technologies (e.g., JavaScript, VB Script, ActiveX, Java Applets) to display and update dynamic information. Unfortunately, these same Active Content technologies are often used by hackers to drive sophisticated web-based attacks, such as Spyware, Phishing, Trojans and malicious code. **Thus, in order to secure its IT infrastructure without impairing business operations, Munich Airport required an intelligent solution that could differentiate between legitimate and malicious Active Content.** It also needed the ability to create granular and specific security policies for different user groups.

Munich Airport maintains a common application data connection among the Customs Authority, Police, Immigration Authority and Ministry of Interior to enable efficient transfer of data. The security of this connection is crucial to ensure data privacy and to enable safe information transfer.



Finjan Vital Security™
Web Appliance NG-5100



“ A secure IT infrastructure is paramount to ensure efficient operations and to enhance our passengers' overall experience ”

Marc Lindike, Vice President Operations and Services at Munich Airport

Finjan's Vital Security™ Web Appliance Solution

After a comprehensive evaluation phase involving several different vendors, Munich Airport chose to work with Finjan and its local reseller, Controlware. Finjan's proactive Vital Security™ Web Appliance blocked all of the attack scenarios created by Munich Airport in the evaluation phase. This proven and comprehensive web security solution features patented behavior-based technology to proactively detect and block known and unknown malicious web threats at the Internet gateway.

A satisfied Finjan customer since 2002, Munich Airport migrated its initial software-based solution to the Vital Security Web Appliance NG-5100 in 2005. Deployed at the Internet gateway, three NG-5100 appliances currently support the airport's 1500 users in a high availability configuration. These "all-in-one" appliances feature Finjan's patented behavior-based security, Vulnerability Anti.dote™ and Anti-Spyware engines, as well as Sophos' fully integrated Anti-Virus engine. The Finjan solution is deployed across the complete IT infrastructure at the airport, securing a wide array of systems.

Finjan's patented behavior-based content inspection technology is uniquely capable of inspecting Active Content objects in real-time (regardless of its source), breaking down the code and understanding its true intent **without executing it**. As a result, Finjan's solution can identify Active Content that is about to perform a malicious or suspicious operation, and block it at the perimeter, before it begins to run on the target computer. Moreover, Finjan offers the only solution capable of preventing unknown and targeted attacks, since it does not rely on signatures or database updates.

Finjan Vital Security Web Appliance is designed to meet the high availability needs of enterprises. Redundant scanners, as well as cached configurations and policies, ensure zero downtime of Munich Airport's critical systems.

Key Benefits and Results

Finjan's Vital Security Web Appliance enables Munich Airport to meet fully its business requirements:

- Proactively stopping web threats that utilize Active Content, such as Spyware, that cannot be detected by traditional security methods
- High availability solution with automatic failover ensures zero downtime of mission-critical systems
- Full control over content entering and leaving network via the web
- Granular security policies for specific groups of users
- Centralized management and simplified administration

“Finjan's behavior-based web security has been invaluable to us in blocking malicious code embedded in Active Content, keeping our critical information systems free from web threats.”



Marc Lindike,
 Vice President Operations
 and Services

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



© Copyright 1996 - 2007. 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 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. Kaspersky is a registered trademark of Kaspersky Lab. SurfControl is a registered trademark of SurfControl plc. Microsoft and Microsoft Office are registered trademarks of Microsoft Corporation.

All other trademarks are the trademarks of their respective owners. 04 2007.