

DOCUMENT* PRESENTED
BY WICK HILL

access
access
management
management
performance
performance
security
security

* © Wick Hill and the Wick Hill logo are trademarks of Wick Hill Group Plc. Registered in the UK and other countries. Other logo, brand and product names are trademarks of their respective owners. All 3rd party information contained within this document is copyright of the originator. Errors and omissions excluded.

Case Study

HMSHost Europe Secures Its Business from Web Threats with Finjan's Vital Security™ Web Appliance



Challenge

To prevent malicious web content from entering corporate network, while ensuring availability of web applications and securing sensitive data

Solution

Finjan Vital Security™ Web Appliance for proactive behavior-based security against web threats in HTTP and SSL traffic

Results

Prevention of spyware and other threats at Internet gateway, enhanced user productivity, and reduced administration efforts

Background

If you have traveled by air in Europe, chances are that you have eaten in one of HMSHost Europe's dining facilities. HMSHost is a market leader in supplying food and beverage services at airports and motorway travel plazas. HMSHost operates restaurants in 101 airports worldwide and has revenues of \$2.0 billion. Formerly known as Host Marriott Services, this company is world-renowned for creating innovative concession plans in travel venues.

HMSHost Europe is headquartered at Schiphol Airport in The Netherlands and operates more than 60 restaurants at Schiphol Airport alone, including well-known branded concepts such as Burger King, Starbucks, and Sbarro. It also operates the Mercure Schiphol Airport Terminal Hotel.

In addition to its main facility at Schiphol, HMSHost Europe maintains offices in Sweden, Ireland, Denmark, Germany and Switzerland (as of 2007). In order to ensure efficient operations across the continent, and to facilitate communications with HMSHost offices in North America, a strong and secure IT infrastructure is crucial.

Each HMSHost office in Europe is connected via VPN to IT headquarters at Schiphol. All web and email access is routed through the Schiphol Data Center, which is responsible for the entire IT infrastructure, including security, data maintenance, backup and network administration.

Business Challenge and Requirements

HMSHost Europe has always exercised caution regarding employees' Internet access, both for productivity and security reasons. However, as more of its business applications are web-based, a growing number of users required such access to carry out their daily activities. HMSHost was aware of the security threats, such as Spyware, that increased web access poses to their IT environment. Therefore, it sought a proven web security solution that blocks these types of threats in real-time at the Internet gateway, before they reach user PCs.

Availability of IT systems, such as ordering and payments, is absolutely critical for business operations. To ensure the freshness of food products for its restaurants, HMSHost supplies stock that will suffice for 24 hours of operations. This means that if the IT environment is down for any reason, orders cannot be issued to suppliers and restaurants could quickly run out of stock, instantly affecting revenues.

Payments and other business transactions are executed using web applications, and payroll for parts of Europe is also outsourced via a webapp. In addition, since HMSHost is a publicly traded company (through its parent company Autogrill S.p.A.), confidential financial information is transferred between the European and US offices for reporting purposes. Thus, securing web traffic was an absolute must for HMSHost Europe.

As much of its web communications is encrypted using SSL, HMSHost Europe required the ability to detect malicious content within SSL traffic, as well as enforcement of SSL certificates.



Decryption and scanning of SSL content with Finjan Vital Security Web and SSL Appliances



“ Finjan offers the most effective solution against Spyware, malicious code and other stealthy web-based attacks ”

Erik Wouterson, Senior Systems Engineer at HMSHost Europe

Finjan's Vital Security™ Web Appliance Solution

HMSHost Europe realized that its existing security products were not equipped to meet its growing requirements for web security. After examining several alternatives, it selected Finjan's award-winning Vital Security Web Appliance solution, which was implemented together with ISSUE Information Technology, its preferred IT partner and Finjan authorized reseller in The Netherlands. This proven and comprehensive web security solution features patented behavior-based technology to detect and block, in real time, known and unknown malicious web threats at the gateway. This includes protection from zero-day exploits and vulnerabilities using virtual patching. **"Finjan specializes in web security, with an innovative product roadmap that matches our IT security vision looking ahead,"** stated Dennis Hoogreef, Director IT and Facilities at HMSHost Europe.

All web traffic generated by offices in Europe is routed through and scanned by Finjan's Vital Security Web Appliance NG-5100, deployed at IT headquarters in Schiphol. This comprehensive appliance features Finjan's Behavior-based security, Vulnerability Anti.dote™ and Anti-Spyware engines, as well as integrating Kaspersky's Anti-Virus engine and SurfControl's URL Filtering engine. In addition, HMSHost Europe has deployed Finjan's Vital Security SSL Appliance NG-5400 for SSL inspection. The fully integrated solution is capable of detecting malicious content arriving via HTTP, HTTPS/SSL and FTP traffic.

Finjan's unique ability to detect and block malicious code that eludes traditional security solutions was proven shortly after system installation. Spyware that was trying to access some remote services, as well as an expired SSL certificate, were found on client machines at various offices. Both of these infected clients could easily have been exploited to carry out potentially damaging attacks. **"We realize that the web represents the main avenue of attack for today's new generation of professional hackers,"** stated Wouterson. **"Finjan offers the most effective solution against Spyware, malicious code and other stealthy web-based attacks."**

In order to enforce its strict Internet usage policy, HMSHost used to manually check websites in multiple languages in order to create and maintain "whitelists." With Finjan's integrated web security solution, HMSHost has full control over web content entering their network based on comprehensive URL category lists, which are maintained and updated automatically. Flexible policy management allows HMSHost to create fine-tuned security policies that leverage synergies between the various security engines.

Key Benefits and Results

Finjan's Vital Security Web Appliance enables HMSHost Europe to meet fully its business requirements:

- To detect and block both known and unknown web threats in real time, such as Spyware and encrypted malicious content, that cannot be detected by traditional security methods
- Full control over content arriving and leaving network in HTTP, HTTPS and FTP traffic
- Enhanced performance and productivity of users
- Securing the integrity of sensitive business information
- Efficient enforcement of corporate Internet access policy
- Centralized management and simplified administration

"IT systems are critical to our business operations. We required a proven web security solution that would ensure the availability of our web-based business applications."



Erik Wouterson,
Senior Systems Engineer
HMSHost Europe

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. Q4 2007.



Case Study

UK's Institute of Directors Consolidates Web Security Using Finjan's Vital Security™ Web Appliance



Challenge

Consolidate IoD's Internet security infrastructure into one solution, with a single point of management, provisioning and reporting

Solution

Vital Security Web Appliance NG-1100, providing proactive and comprehensive web security for small and medium-sized organizations

Results

Streamlined security architecture, enhanced performance and reduction in management efforts and resources

Background

Founded in 1903, the Institute of Directors (IoD) is a highly respected organization in the UK's business sector. Its membership includes over 55,000 directors of British companies, who count on the IoD to provide the information and advice they require to help their businesses succeed.

Headquartered in three London buildings, the IoD maintains ten regional offices located throughout the UK (see map). An efficient and secure information and communication infrastructure is critical for supporting its nationwide operations. Moreover, as a leader in the business community, the IoD cannot afford to compromise when it comes to Internet security. The task of keeping the IoD network secure falls on the shoulders of Richard Swann, IT Infrastructure Manager. **"Security is a business issue. The IoD is committed to informing businesses about Internet-based threats such as Spyware and Phishing, and how they can protect themselves from these hazards,"** states Swann.

The IoD regional offices are connected via a hardware-based VPN to the head office, from which all Internet access and web browsing is routed via a single point-of-presence. Over 280 users around the UK access centralized applications over the network. The IoD has historically used security solutions from Finjan and several other in-house and third-party solutions to protect its users from Internet-based threats.

Business Challenge and Requirements

The IoD security framework grew over time into three separate security infrastructures using several disparate solutions (anti-spam, anti-virus, home grown URL filtering, VPN and different proxies). In order to streamline business operations, reduce management overhead and ultimately save money, **the IoD decided to consolidate the majority of its existing infrastructure into one solution, with a single point of management, provisioning and reporting.**

The IoD needed the ability to define specific security policies for different groups of users. For instance, the Information and Advisory Service staff needed access to Internet without restrictions in order to support the IoD Business Information service, which handles members' call-in queries. The IoD used to route different groups of users through several different proxies, creating management issues and adding maintenance overhead that taxed its limited IT resources. The IoD also used to maintain its own lists of permitted and forbidden URLs. With respect to inappropriate content, the IoD has a very strict Internet usage policy and the ability to enforce this policy using a commercially available product was seen as a major advantage, not to mention the associated reductions in administration overhead.

In light of the plethora of Spyware, Phishing and other web-based attacks that can compromise personal information, **IoD required a solution that would protect its staff and members from potential identity theft.**



Vital Security™
Web Appliance NG-1100



IoD Offices



Directors Room, Pall Mall

"Finjan is the market leader with a proven system"

Richard Swann, IT Infrastructure Manager

Finjan's Vital Security™ Web Appliance Solution

With these requirements in mind, the IoD chose to implement Finjan's Vital Security Web Appliance NG-1100 as the platform upon which to consolidate its web security infrastructure. As a satisfied customer of Finjan's software-based solutions since 1999, the IoD hardly considered other options: **"Finjan is the market leader with a proven system, so why look elsewhere?"** said Swann. Moreover, Finjan was able to offer IoD an attractive migration plan so that it could continue to benefit from superior web security on a high-performance appliance.

Specially designed for small to medium-sized businesses, the NG-1100 delivers the world's best and most comprehensive web security in an all-in-one, easy to install and "self-managing" appliance. It integrates Finjan's unique security technologies (behavior-based security, zero-hour vulnerability protection, Anti-Spyware engine, Content Filtering) with leading Anti-Virus (Sophos®), and URL Filtering (SurfControl®) engines.

Finjan's patented behavior-based content inspection technology identifies and blocks known and unknown viruses and malicious code, usually before anti-virus vendors have issued an update, a fact that the IoD and Swann had come to rely upon over the last five years. **"We are very conscious of the potential dangers inherent in ActiveX and Java which can be used to exploit software vulnerabilities. Finjan's proactive solutions excel in blocking these types of sophisticated attacks,"** said Swann.

In addition to Finjan's proven security technology, the efficiencies and powerful synergies created through managing web security through a single appliance, as well as granular policy management, were key factors in the IoD's decision.

As a result of the migration, IoD was able to streamline its security architecture from several different solutions to a single NG-1100 appliance for web and proxy. The transition to Finjan's solution freed up one key IT resource, charged with supporting its various security solutions, for other important tasks. **"Finjan's proactive protection against Spyware and other malware threats has allowed us to concentrate on core business activities, without spending inordinate resources handling security incidents and cleaning infected computers,"** concludes Swann.

Key Benefits and Results

Finjan's Vital Security Web Appliance solution enabled IoD to meet fully its business requirements:

- Comprehensive "all-in-one" solution for web security in a single secure, reliable and low administration appliance
- Integrated content security including behavior-based security, vulnerability protection, anti-spyware, anti-virus, content filtering, URL filtering
- Reduction in complexity and administrative overhead by simplifying the previous architecture built upon multiple proxies and disparate solutions
- Enhanced performance and productivity of users
- Enabled the IoD to reduce security administration and management efforts by one full IT resource
- Reduced patch management overhead due to Finjan's "hardened" OS and automatic updates (fed by Finjan), with the added benefit of no 3rd party OS license fee

" Finjan's NG-1100 appliance provides the IoD with the same level of security and content management deployed by large enterprises, with a single point of administration and reporting, at an affordable price for an organization of our size. "



Richard Swann,
IT Infrastructure Manager

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



© 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.dot 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. Q4 2007.

Case Study

Max Bahr Builds Its Own Secure Network with Finjan



Challenge

To secure IT network from malicious content, enabling high availability of IT systems and continuous business operations

Solution

Finjan Vital Security™ Web Appliance to protect users from any type of malicious web content

Results

Unsurpassed web security, maximum business productivity, enhanced customer service, and reduced administrative costs

Background

The Max Bahr building store is one of the oldest home improvement chains in Germany. It was founded in 1879 in Hamburg, where the company's headquarters is still located. Today, the Max Bahr chain comprises about 80 stores and employs over 4,000 personnel. Since February 2007, Max Bahr is part of the international Praktiker Group.

With operations distributed in its stores throughout Germany, Max Bahr realizes that an efficient and secure IT infrastructure is critical to support its daily business operations. To protect its network from potential security risks, Max Bahr required a scalable and centrally managed web security solution that could be smoothly integrated within its existing network environment.

"Max Bahr is committed to providing its customers with quality products and the highest level of customer service. Our IT systems must be available and secure at all times in order to enable us to meet the needs of our customers," stated Christian Weirich, IT-Manager at Max Bahr.

Business Challenge and Requirements

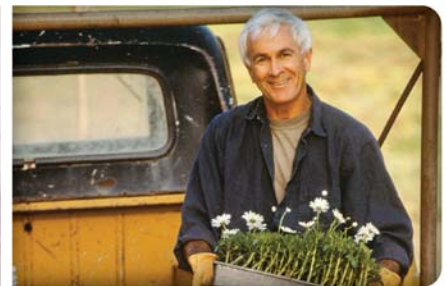
Max Bahr sought a proven solution that would provide the highest level of web security, without compromising business productivity or network performance.

Some of Max Bahr's online business applications utilize Active Content technologies (e.g., ActiveX, JavaScript, VB Script) to dynamically display and update information. Unfortunately, these same technologies are used by hackers to install Spyware and drive sophisticated web-based attacks. To allow unlimited use of Active Content without compromising its security, Max Bahr required an intelligent solution able to differentiate between legitimate and malicious Active Content. Traditional signature-based solutions were designed to block known viruses and malware; however, these types of solutions are neither sufficient nor effective in detecting unknown and stealthy attacks arriving via the web. This is why Max Bahr insisted on a proactive gateway-based web security solution that blocks web threats in real time before they infiltrate end user PCs.

Furthermore, as many users require web access to perform their work-related activities, it was important to control web browsing and prevent security breaches related to employees accessing malicious and/or inappropriate sites.



Finjan Vital Security™
 Web Appliance NG-5100



"We are pleased with the results of Finjan's unique behavior-based content security solution, which protects our users against stealthy web threats."

Christian Weirich, IT-Manager at Max Bahr

Finjan's Vital Security™ Web Appliance Solution

After a comprehensive evaluation phase involving several different vendors, Max Bahr chose to work with Finjan and its local partner, Crocodial Hamburg. Finjan's proven and comprehensive web security solution features patented behavior-based technology to detect and block known and unknown malicious web threats in real-time. **During the evaluation phase, it became clear to Max Bahr that Finjan was the only vendor with a true solution against malicious objects like Spyware and Trojan horses.**

A satisfied Finjan customer since 2003, Max Bahr migrated its initial software-based solution to the Vital Security Web Appliance NG-5100 in 2005. Subsequently, Max Bahr added NG-5100 appliances to extend its web security solution to its growing user base. These scalable and high-performance appliances feature Finjan's Real-time behavior-based security, Vulnerability Anti.dot™ and Anti-Spyware engines, as well as SurfControl's fully integrated URL Filtering engine.

Deployed at the Internet gateway behind the corporate firewall, the NG-5100 appliances provide a centrally managed solution for all of Max Bahr's users, while enabling the flexible creation of granular security policies for specific groups of users. By integrating several security engines in a single appliance, Finjan's comprehensive and integrated web security solution facilitates deployment, simplifies management, and reduces costs.

Finjan's patented behavior-based content inspection technology is uniquely capable of inspecting web content in real-time regardless of its source, breaking down the code and understanding its true intent without executing it on the end user's machine.

"We are pleased with the results of Finjan's unique behavior-based content security solution, which protects our users against stealthy web threats" said Christian Weirich.

Key Benefits and Results

Finjan's Vital Security Web Appliance enables Max Bahr to meet fully its business requirements:

- Securing its IT network from malicious and stealthy web threats, such as Spyware and Trojans, that often bypass signature-based security methods
- Enhanced performance and maximum user productivity
- Saves time and resources related to handling security incidents
- Secures private customer information
- Centralized management and implementation of security policies across its distributed network

" Finjan's Vital Security™ Web Appliance solution takes care of our web security needs, allowing IT staff to remain focused on the core business. This guarantees that our customers always get the highest levels of care and service in a secure online environment. "



Christian Weirich
IT-Manager

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



© 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.dot 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. Q4 2007.

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.

Case Study

SVB Selects Finjan to Secure Its Network from Web Threats



Challenge

To secure SVB's advanced ICT infrastructure from web-based malware threats, while simplifying management and increasing productivity

Solution

Finjan Vital Security™ Web Appliance, featuring real-time content inspection to prevent malicious web content from entering corporate network

Results

Unsurpassed real-time web security, reduction in maintenance efforts and resources, and enhanced user experience

Background

If you have lived or worked in The Netherlands, sooner or later you will come into contact with the Sociale Verzekeringsbank (SVB). With over 4.6 million clients, SVB is an independent administrative body that implements social security schemes for various government agencies. Its responsibilities include the administration of retirement pensions, child benefits, survivor benefits, care allowances for handicapped children, and remigration assistance.

SVB's operational strategy is based on extensive deployment of Information and Communications Technology (ICT). A modern, reliable and secure ICT infrastructure enables SVB to implement large-scale social security schemes. ICT is used to link SVB's headquarters, located outside of Amsterdam, with its nine branch offices (see map). This advanced infrastructure also supports integration of several customer channels, such as the website and the call centers.

Security is a key element of SVB's operational management strategy. A secure ICT infrastructure is vital to ensure efficient operations across its various offices in The Netherlands and abroad. Privacy of client information is paramount and mandated by law. Accordingly, SVB is aware of the need to safeguard its highly sensitive information assets from today's sophisticated web-based threats, such as crimeware, Trojans and other types of malicious code, which specifically target this type of information.

"Considering the sensitive nature of the information we maintain and the volume of financial transactions we handle, there is no room for compromise in the area of information security," Arjan van de Velde, IT Specialist at SVB.

Business Challenge and Requirements

Although the SVB is not a normal financial institute as the word "bank" in the name does suggest, it has to be protected effectively against cybercriminals. "We realized that our traditional anti-virus solutions had serious limitations when it came to detecting unknown malware and stealthy crimeware attacks originating from the web," stated Arjan van de Velde, IT Specialist at SVB. As a result, SVB sought a real-time solution that prevents Trojans and other malicious web content from entering its corporate network.

SVB's thousands of users are divided into three different levels, depending on their particular responsibilities and department. For example, certain personnel may require web access to perform research and other work-related activities, while others should not be allowed access at all. Thus, SVB needed the ability to define specific security policies for different groups of users.

Previously, SVB worked with trusted lists (i.e., whitelists) of URLs that were only scanned for viruses and not for malicious code in active content. However, since today's crimeware and malware often use legitimate websites as their staging ground, SVB required a solution that analyzes all web content coming into its network, regardless of the URL origin.

In order to ensure interoperability with existing network devices, SVB required a solution that was fully ICAP compliant. In addition, SVB preferred an integrated gateway solution, combining real-time web content scanning and anti-virus, with a single point of management.



Finjan Vital Security™
Web Appliance NG-5100



"Since deployment of Finjan's secure web gateway solution, maintenance of our security solution has become much easier and requires less resources"

Arjan van de Velde, IT Specialist at SVB

Finjan's Secure Web Gateway Solution

With these requirements in mind, SVB chose Finjan's secure web gateway solution, based on the award-winning Vital Security™ Web Appliance NG-5100. The solution was implemented by Pinewood, an authorized Finjan reseller in The Netherlands. Finjan's proven and comprehensive solution features patented real-time content inspection technology to detect and block known and unknown malicious web threats. During the evaluation phase, it became clear to SVB that Finjan was the preferred vendor with a true solution against dynamic malicious content like crimeware and Trojans.

Deployed at the Internet gateway, four NG-5100 appliances currently support SVB's 3500 users in a high availability configuration. These "all-in-one" appliances feature Finjan's real-time content inspection, Vulnerability Anti.dote™ and Anti-Spyware engines, as well as Kaspersky's fully integrated Anti-Virus engine.. SVB's users access the Internet via the Blue Coat proxy, which is fully interoperable with Finjan's appliances via ICAP.

Finjan's real-time content inspection technology is uniquely capable of analyzing web content in real-time regardless of its source, breaking down the code and understanding its true intent without executing it on the end user's machine. Finjan delivers the highest rate of malicious code detection and prevention, allowing organizations to safeguard their most valuable asset – their information.

By integrating several security engines in a single appliance, Finjan's comprehensive and integrated web security solution facilitates deployment, simplifies management, and reduces total cost of ownership. In addition, the appliance's flexible policy management lets SVB enforce its web browsing policy by defining specific security policies to specific groups of users. "Since deployment of Finjan's secure web gateway solution, maintenance of our security solution has become much easier and requires less resources," said Arjan van de Velde, IT Specialist at SVB.

Key Benefits and Results

Finjan's Secure Web Gateway solution enables SVB to meet fully its business requirements:

- Securing its IT network from malicious and stealthy web threats, such as crimeware and Trojans, that often bypass signature-based security methods
- Enhanced performance and maximum user productivity
- Protection of private customer information
- Reduced administration efforts and resources
- Granular security policies for specific groups of users
- Integrated security engines with single point of management, provisioning and reporting

“ Finjan's real-time web security protects our sensitive information from stealthy Trojans and crimeware ”



Arjan van de Velde,
IT Specialist at SVB

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 - 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 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 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. Q1 2008.