

DOCUMENT* PRESENTED
BY WICK HILL



Payment Card Industry (PCI) Compliance

Finjan White Paper

March 2007

THIS DOCUMENT INCLUDES PROPRIETARY AND CONFIDENTIAL INFORMATION OF FINJAN SOFTWARE INC. AND/OR ITS AFFILIATES AND SUBSIDIARIES AND MAY NOT BE USED, CIRCULATED OR QUOTED EXCEPT IN ACCORDANCE WITH EXPLICIT WRITTEN AUTHORIZATION FROM FINJAN

© Copyright 1996 - 2007. Finjan Software Inc. and its affiliates and subsidiaries (“Finjan”). 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, 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. 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.

For additional information, please visit www.finjan.com or contact one of our regional offices:

| | |
|--|--|
| <p>USA 2025 Gateway Place Suite 180 San Jose, CA 95110, USA Toll Free: 1 888 FINJAN 8 Tel: +1 408 452 9700 Fax: +1 408 452 9701 salesna@finjan.com</p> | <p>Europe Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com</p> |
| <p>Chrysler Building 405 Lexington Avenue, 35th Floor New York, NY 10174, USA Tel: +1 212 681 4410 Fax: +1 212 681 4411 salesna@finjan.com</p> | <p>Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com</p> |
| <p>Israel/APAC Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 salesint@finjan.com</p> | <p>Printerweg 56 3821 AD Amersfoort The Netherlands Tel: +31 33 4543555 Fax: +31 33 4543550 salesne@finjan.com</p> |

Email: info@finjan.com
 Internet: www.finjan.com

Contents

| | |
|--------------------------------|---|
| Background..... | 1 |
| Meeting PCI Requirements | 1 |
| About Finjan..... | 2 |

Background

The Payment Card Industry (PCI) Data Security Standard (DSS) was created by credit card companies to protect customer information. Credit card organizations like Visa, MasterCard, and American Express, recommend that merchants and service providers meet certain minimum standards of security when they store, process and transmit cardholder data.

Meeting PCI Requirements

Finjan's Vital Security™ Web Appliances have been designed, and can be configured to ensure that merchants that store, process, or transmit cardholder data, protect it properly from Web threats, in compliance with the Payment Card Industry (PCI) Data Security Standard (DSS).

Finjan enables you to be compliant with the following Web-related PCI requirements:

- **Building and Maintaining a Secure Network**
 - Establishing configuration steps that include descriptions of groups, roles, and responsibilities for logical management of network components.
 - Building a configuration that denies access to “untrusted” Web sites.
 - Restricting inbound and outbound Internet traffic.
 - Restricting outbound traffic to that which is necessary for the payment card environment.
 - Denying all other inbound and outbound traffic not specifically allowed.

- **Maintaining a Vulnerability Management Program**
 - Using and regularly updating anti-virus software to protect systems from malicious software.
 - Deploying anti-virus mechanisms on all systems commonly affected by viruses (e.g. PCs and servers). Upholding this requirement is easier when Finjan's Web security solutions are installed because they detect and block malicious code at the gateway, before it reaches the target, thus reducing the workload of client-based anti-virus mechanisms and safeguarding the throughput of peripheral resources.
 - Ensuring that all anti-virus mechanisms are current, actively running, and capable of generating audit logs
 - Developing and maintaining secure systems and applications
 - Ensuring that all system components and software have the latest vendor-supplied security patches. Finjan's Vulnerability Anti.Dote™ offers a superior security level, protecting application vulnerabilities before patches are delivered by vendors and installed and tested on merchant networks.
 - Establishing a process to identify newly discovered security vulnerabilities, including an alert service that addresses new vulnerability issues.

- **Implementing Strong Access Control Measures**
 - Limiting access to certain Internet and system resources to only those individuals whose job requires such access. Controlling Internet access for end-users and controlling Vital Security Management Console access for system administrators, can be defined on both a group level and an individual level.
 - Incorporating a mechanism with multiple users that restricts access based on a user's need to know.
 - Assigning a unique ID to each person and password authentication, ensuring that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.
 - Control the addition, deletion, and modification of user IDs, credentials, and other identifier objects.

- **Monitoring and Testing Networks on a Regular Basis**
 - Tracking all access to resources and user activities via a logging mechanism for monitoring and analysis.
 - Recording the following audit trail entries for each event (amongst others):
 - User identification
 - Type of event
 - Date and time
 - Success or failure indication
 - Origination of event
 - Identity or name of affected data, system component, or resource

- **Maintaining an Information Security Policy**
 - Establishing, publishing, maintaining, and disseminating a security policy.
 - Developing usage policies for critical employee-facing technologies, in particular for the Internet.
 - Ensuring the security policy clearly defines information security responsibilities.
 - Administering user accounts, including additions, deletions, and modifications.

About Finjan

Finjan is a global provider of best-of-breed web security solutions for businesses and organizations. Our proactive, appliance-based solutions deliver the most effective shield against web-borne threats, freeing enterprises to harness the web for maximum commercial results. Finjan's web security solutions utilize patented behavior-based technology to proactively repel all types of threats arriving via the web, such as Spyware, Phishing, Trojans and other malicious code, securing businesses against unknown and emerging threats, as well as known malware. Finjan's security solutions have received industry awards and recognition from leading analyst houses and publications, including IDC, Butler Group, SC Magazine, CRN, PCPro, ITWeek, and Information Security. With Finjan's award-winning and widely used solutions, businesses can focus on implementing web strategies to realize their full organizational and commercial potential. For more information about Finjan, please visit: www.finjan.com.