UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

ASSURANCE MAINTENANCE STATUS SUMMARY (supplementing Certification Report No. P150)

CyberGuard Firewall for UnixWare / Premium Appliance Firewall

Release 4.3 Derivatives (to Release 5.2 PSU 1)

running on SCO UnixWare 2.1.3

Issue 2.0

February 2005

UK IT Security Evaluation and Certification Scheme, Certification Body,
CESG, Hubble Road, Cheltenham, Glos GL51 0EX
United Kingdom

TABLE OF CONTENTS

ABBREVIATIONS

AMA	Maintenance of Assurance Class
CCRA	Common Criteria Recognition Arrangement
CLEF	Commercial Evaluation Facility
CMS	Certificate Maintenance Scheme
DSA	Developer Security Analyst
EAL	Evaluation Assurance Level
FS	FireSTAR
HTTP	HyperText Transfer Protocol
KS	KnightSTAR
NNTP	Network News Transfer Protocol
PSU	Product Software Update
RAID	Redundant Array of Inexpensive Disks
SL	STARLord
SMTP	Simple Message Transfer Protocol
SNMP	Simple Network Management Protocol
TOE	Target of Evaluation
UKSP	United Kingdom Scheme Publication
UW	UnixWare

REFERENCES

a. Certification Report No. P150, CyberGuard Firewall for UnixWare, Release 4.3, running on SCO UnixWare 2.1.3,
UK IT Security Evaluation and Certification Scheme,
Issue 2.0, February 2003.

b. Common Criteria Security Target,
Logica UK Ltd,
CLEF.EC25402.40.1, Issue 3.0, 5 February 2003.

c. Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security,
Members of the Agreement Group,
May 2000.

d. UK Certificate Maintenance Scheme, Part I, Description of the CMS,
UK IT Security Evaluation and Certification Scheme,
UKSP 16, Issue 1.0, 31 July 1996.

e. UK Certificate Maintenance Scheme, Part II, Impact Analysis and Evaluation Methodology,
UK IT Security Evaluation and Certification Scheme,
UKSP 16, Issue 1.0, 31 July 1996.

f. UKSP 16 Addendum: Interim Guidance for CC TOEs,
UK IT Security Evaluation and Certification Scheme,
UKSP 16, Issue 1.0, January 2000.

g. Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.

h. Task LFL/T145 Certificate Maintenance Scheme, Audit Report,
Logica CLEF,
CLEF.26874.CMS/7.2/3, Issue 1.0, 22 January 2002.

i. AMS for Task LFL/T145,
Logica CLEF,
CLEF.26874.CMS/5.1/3, 18 March 2002.

j. Task LFL/T159 Combined CMS-AMS Audit Report,
Logica CLEF,
CLEF.26992.CMS/7.2/1, Issue 1.0, 5 December 2002.

k. Task LFL/T211 Combined CMS-AMS Audit Report,
LogicaCMG CLEF,
CLEF.116173.7.2/1, Issue 1.0, 23 November 2004.

l. Security Hardening in the CyberGuard Firewall for UnixWare,
CyberGuard Corporation,
EV032-001, Issue 1.0, 13 February 2003.

(This page is intentionally left blank)

I. INTRODUCTION

Introduction

1. This summary outlines the current status of the UK assurance maintenance process for the CyberGuard Firewall for UnixWare (UW) / Premium Appliance Firewall Release 4.3 derivatives, and is intended to assist prospective consumers when judging the suitability of the IT security of the derivatives for their particular requirements.

2. The baseline for assurance maintenance was the Common Criteria (CC) evaluation, to the EAL4 Evaluation Assurance Level, of product Release 4.3. The Developer's flaw remediation procedures were also evaluated in accordance with the CC ALC_FLR.1 evaluation requirements.

3. Prospective consumers are advised to read this document in conjunction with both:

- the Certification Report [Reference a] for the EAL4 and ALC_FLR.1 evaluation; and
- the Security Target [b] which specifies the functional, environmental and assurance requirements for the evaluation and assurance maintenance.

Assurance Maintained Derivatives

4. The version of the product originally evaluated was:

- CyberGuard Firewall for UnixWare / Premium Appliance Firewall Release 4.3.

5. The most recent version of the product for which assurance has been maintained is:

- CyberGuard Firewall for UnixWare / Premium Appliance Firewall Release 5.2 PSU 1.

6. Assurance has also been maintained for the intermediate releases and Product Software Updates (PSUs) detailed in this summary. (Only Releases 4.3 PSU 6 and 5.0 PSU 3 have not been assurance maintained.)

7. Similarly to the evaluation of product Release 4.3, all assurance maintained derivatives include the pre-configured, pre-packaged Premium Appliance Firewall products[1]:

- FireSTAR (FS)
- KnightSTAR (KS)
- STARLord (SL)

8. Note that for all of the assurance maintained derivatives, the scope of the Target of Evaluation (TOE) functionality remains unchanged from that defined in the Security Target, even though the product features have been enhanced.

[1] The LX product is no longer supported and has therefore been removed from this report.

Status of Maintenance Results

9. Assurance maintenance involves a process whereby a Developer Security Analyst (DSA) performs an analysis of the security impact of changes to the product, affirms that these changes do not undermine the security of the product, affirms that the changes are not of sufficient significance to warrant a Commercial Evaluation Facility (CLEF) re-evaluation and maintains product and process documentation. The work of the DSA is periodically audited by the CLEF.

10. The evaluation of product Release 4.3 was conducted in accordance with the terms of the CC Recognition Arrangement (CCRA) [c], and the evaluation of flaw remediation procedures was conducted in accordance with a working agreement amongst the parties to the arrangement (pending formal extension of CCRA). These agreements are based on evaluation by a CLEF using common evaluation methodology agreed by the CCRA parties.

11. A common methodology for assurance maintenance had not been agreed at the start of the activities covered by this summary, and CCRA did not extend to assurance maintenance. The UK assurance maintenance process is thus based on an interim UK methodology comprising UKSP 16 [d, e] and the UKSP 16 Addendum for CC TOEs [f]. The UK IT Security Evaluation and Certification Scheme considers this methodology appropriate for use with the CC Part 3 [g] AMA criteria.

AMA Audit Schedule

12. The schedule of completed AMA Audits is detailed in the table below.

Schedule	Date	Auditors
AMA Audit No 1 [h, i]	August 2001	Logica CLEF
AMA Audit No 2 [j]	November 2002	Logica CLEF
AMA Audit No 3 [k]	August 2004	LogicaCMG CLEF

AMA Audit Schedule

AMA Audit Results

13. After due consideration of the Audit Reports [h-k] produced by the LogicaCMG CLEF (formerly the Logica CLEF) and other visibility of the assurance maintenance process given to the Certifier, the Certification Body has determined that EAL4 assurance has been maintained for all derivatives of CyberGuard Firewall for UnixWare (UW) / Premium Appliance Firewall Release 4.3 listed in this summary.

14. The ALC_FLR evaluation was conducted concurrently with AMA Audit No 1, and maintenance of this assurance augmentation was confirmed during AMA Audit No 2 and Audit No 3.

General Points

15. Assurance maintenance addresses the security functionality claimed in the Security Target with reference to the assumed operating environment specified by the Security Target. The assurance-maintained derivative configurations are as specified in the Certification Report and the derivative modifications specified in the following chapters. Prospective consumers are advised to check that this matches their identified requirements.

16. The assurance maintenance process is not a guarantee of freedom from security vulnerabilities; there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after an AMA Audit has been completed. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this document was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether such patches have been:

- applied in accordance with the evaluated flaw remediation procedures,
- incorporated into a later assurance maintained derivative, or
- evaluated and certified.

Assurance-maintained Derivative Changes

17. The following chapters give information of relevance to consumers for the assurance maintained derivatives, particularly where this differs from that supplied in the Certification Report for CyberGuard Firewall Release 4.3 [a].

18. The Installation and Guidance documentation for the original TOE (Release 4.3) is detailed in the Certification Report [a]. For each TOE derivative, a summary of the updated Installation and Guidance documentation and CD-ROM media, including a summary of the security-related changes, is provided in the following chapters.

19. The consumer-relevant items that have changed since the original evaluation of Release 4.3 are summarised in the table below.

Item	Modified	Description
Security Target	Yes	Issue 2.0 has been updated to Issue 3.0 to include augmentation by ALC_FLR.1. (There have been no changes to the assurance or functionality requirements under assurance maintenance.)
Product Identifiers	Yes	Identifiers of derivatives, associated guidance documents and hardware specified for the evaluation environment are as specified in the following chapters.

Item	Modified	Description
Delivery Procedures	Yes	MD5 checksum procedure evaluated as a delivery procedure under Flaw Remediation (see Certification Report [a]. In addition to the software release (including PSU) number, the model number (or enhancement status) and CD-ROM reference number are marked on the software CD and included on the packing slip and in the e-mail sent to the customer prior to shipment. (Also the site identifier and a hardware serial number can be used by Customer Support to identify a derivative previously supplied to a customer). There have been no other changes under assurance maintenance.
Installation and Guidance Documentation	Yes	Delivery and Configuration document: There have been no changes to this document under assurance maintenance. Installation Guide: Changes in each major release have been reflected in a new version of this document. Release Notes: Changes in each major release have been reflected in a new version of this document. CyberGuard Firewall Manual: Changes in each major release have been reflected in a new version of this document. Security Hardening document: Minor changes (eg revised reference to the Firewall Manual) have been included in an updated version [l]. README files: Changes in each PSU have been reflected in a README file (available on the relevant CD-ROM media and the CyberGuard website). Answer Book: Updated on CyberGuard website to reflect changes in each major release and PSU. On-line help and manual pages: Updated in product to reflect changes in each major release and PSU.

Item	Modified	Description
UnixWare 2.1.3	No	No vulnerabilities found within the scope of the TOE derivatives.
Security tests	Yes	Each new release or PSU is subjected to the full set of automated firewall security tests on each current Premium Appliance Firewall hardware platform. (See Annex A for further information.). Additional tests have been created and added to the existing suite as required to check the impact of the TOE changes.

Maintenance of Consumer-Relevant Items

20. In the following chapters, the reference to "UW" relates to the original CyberGuard Firewall for UnixWare Release 4.3 software, indicating a software-only update, i.e. no pre-packaged hardware was supplied by CyberGuard (note that this option is no longer marketed by CyberGuard). In addition, the references to "FS", "KS" and "SL" relate to the original pre-configured, pre-packaged TOE derivatives detailed in the Certification Report [a]. Within CyberGuard, subsequent TOE derivatives are referenced either by specific Model Number (eg FS 500), or by specific enhancement (eg KS raid (see below) – these predate the introduction of Model Numbers).

21. The TOE derivatives that include specific pre-configured, pre-packaged enhancements, but no Model Number, are indicated as follows:

- KS raid: KnightSTAR containing a specific RAID subsystem
- KS tu: KnightSTAR containing an Intel Tupelo processor with 9GB hard drive
- KS tu18: KnightSTAR containing an Intel Tupelo processor with 18GB hard drive
- FS b: FireSTAR containing a specific memory upgrade.

II. 4.3 PSU 1 (P4x3p1)

22. There were some security-supporting changes to the source code of this TOE derivative to improve messages and to support performance enhancements, together with some updates to the NNTP and FTP proxies.

23. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
README File on CD-ROM and CyberGuard website.	N/A

Updated Installation and Guidance Documentation

24. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
UW	1905	12/18/00
KS	1905	12/18/00
SL	1905	12/18/00
FS	1906	01/04/01

Updated Product CD-ROM Media

III. 4.3 PSU 2 (P4x3p2)

25. There were some security-supporting changes to the source code of this TOE derivative to support corrections and improvements to the FTP, SMTP and HTTP proxies.

26. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
README File on CD-ROM and CyberGuard website.	N/A

Updated Installation and Guidance Documentation

27. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
UW	1907	04/18/01
KS	1908	04/18/01
SL	1909	04/18/01
KS raid	1909	04/18/01
FS	1910	04/18/01
SL 500	1911	04/20/01
KS tu	1912 (superseded by 1913 with IPMI fix)	04/20/01
KS tu	1913	05/15/01

Updated Product CD-ROM Media

IV. 4.3 PSU 3 (P4x3p3)

28. There were some security-critical changes to the source code of this TOE derivative to support SMTP filtering.

29. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
README File on CD-ROM and CyberGuard website.	N/A

Updated Installation and Guidance Documentation

30. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
UW	1920	07/25/01
KS	1921	07/25/01
KS tu	1922	07/25/01
SL	1923	07/25/01
SL 500	1924	07/25/01
KS raid	1924	07/25/01
FS	1925	07/25/01
KS tu18	1926	12/13/01

Updated Product CD-ROM Media

V. 4.3 PSU 4 (P4x3p4)

31. There were no security-critical or security-supporting changes to the source code of this TOE derivative.

32. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
README File on CD-ROM and CyberGuard website.	N/A

Updated Installation and Guidance Documentation

33. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
KS tu18	1927	12/19/01
KS tu	1928	12/19/01
KS	1929	12/19/01
SL	1930	12/19/01
SL 500	1931	12/19/01
KS raid	1932	12/19/01
FS	1933	12/19/01
UW	1934	01/18/02

Updated Product CD-ROM Media

VI. 4.3 PSU 5 (P4x3p5)

34. There were no security-critical or security-supporting changes to the source code of this TOE derivative.

35. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
README File on CD-ROM and CyberGuard website.	N/A

Updated Installation and Guidance Documentation

36. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
UW	1935	04/11/02
KS	1936	05/07/02
KS tu	1937	04/17/02
KS tu18	1938	06/03/02
FS	1940	04/17/02
FS b	1941	04/30/02
SL	1942	05/23/02
SL 500	1943	05/17/02
KS raid	1943	05/17/02

Updated Product CD-ROM Media

VII. 5.0

37. There were some security-supporting changes to the source code of this TOE derivative to support synflood defence and to support VPN. (VPN is not included within the scope of the TOE.)

38. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
CyberGuard Firewall Manual (Vols 1, 2, 3)	FW001-061, November 2001
CyberGuard 5.0 Installation Guide	IN001-050, November 2001
CyberGuard Firewall Release Notes Version 5.0	RN001-5.0, 28 November 2001

Updated Installation and Guidance Documentation

39. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
KS	2510	11/28/01
KS tu	2512	11/28/01
KS tu18	2513	11/28/01
FS	2514	11/28/01
SL	2515	11/28/01
SL 500	2516	11/28/01
KS raid	2516	11/28/01

Updated Product CD-ROM Media

VIII. 5.0 PSU 1 (P5x0p1)

40. There were no security-critical or security-supporting changes to the source code of this TOE derivative.

41. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
README File on CD-ROM and CyberGuard website.	N/A

Updated Installation and Guidance Documentation

42. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
KS	2518	02/25/02
FS	2521	02/25/02
FS b	2522	02/25/02
SL	2523	02/25/02
SL 500	2524	02/25/02
KS raid	2524	02/25/02
KS tu	2526	03/15/02
KS tu18	2527	03/15/02

Updated Product CD-ROM Media

IX. 5.0 PSU 2 (P5x0p2)

43. There were no security-critical or security-supporting changes to the source code of this TOE derivative.

44. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
README File on CD-ROM and CyberGuard website.	N/A

Updated Installation and Guidance Documentation

45. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
KS	2529	05/22/02
KS tu	2530	06/13/02
FS	2533	05/24/02
SL	2535	05/24/02
KS tu18	2538	05/21/02
FS b	2539	06/13/02
KS 1000/1500	2543	09/11/02
SL 2000	2545	10/03/02

Updated Product CD-ROM Media

X. 5.1

46. There were no security-critical or security-supporting changes to the source code of this TOE derivative.

47. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
CyberGuard Firewall Manual (Vols 1, 2, 3)	FW001-070, October 2002
CyberGuard 5.1 Installation Guide	IN001-060, October 2002
CyberGuard Firewall Release Notes Version 5.1	RN001-5.1, 29 October 2002

Updated Installation and Guidance Documentation

48. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
KS	2602	10/29/02
KS tu	2603	10/29/02
KS tu18	2604	10/29/02
KS 1000/1500	2605	10/29/02
FS	2606	10/29/02
FS b	2607	10/29/02
FS 250/500	2608	10/29/02
SL	2609	10/29/02
SL 2000	2611	10/29/02

Updated Product CD-ROM Media

XI. 5.1 PSU 1 (P5x1p1)

49. There were some security relevant and some security enforcing changes to the source code of this TOE derivative.

50. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
README File on CD-ROM and CyberGuard website.	N/A

Updated Installation and Guidance Documentation

51. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
KS	2616	05/15/03
KS tu	2617	05/15/03
KS tu18	2618	05/14/03
KS 1000/1500	2619	05/14/03
FS	2620	05/16/03
FS b	2621	05/14/03
FS 250/500	2622	05/14/03
SL	2623	05/15/03
SL 500 KS RAID	2624	05/16/03
SL 2000 SL 3200 KS1500R	2625	05/14/03
KS ide	2626	07/21/03
KS 1000/1500 u320	2628	09/12/03

Updated Product CD-ROM Media

XII. 5.1 PSU 2 (P5x1p2)

52. There were some security relevant and security enforcing changes to the source code of this TOE derivative.

53. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
README File on CD-ROM and CyberGuard website.	N/A

Updated Installation and Guidance Documentation

54. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
KS	2651	06/08/04
KS ide	2652	06/10/04
KS tu	2653	06/08/04
KS tu18	2654	06/08/04
KS 1000/1500	2655	06/08/04
KS 1000/1500 u320	2656	06/08/04
FS	2657	06/08/04
FS b	2658	06/08/04
FS 250/500 FS 300/600	2659	06/08/04
SL	2660	06/08/04
SL 500 KS RAID	2661	06/08/04
SL 2000 SL 3200 KS 1500R	2662	06/08/04

Updated Product CD-ROM Media

XIII. 5.2

55. There were some security enforcing and some security relevant changes to the source code of this TOE derivative.

56. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
CyberGuard Firewall Manual (Vols 1, 2, 3)	FW001-080, November 2003
CyberGuard 5.2 Installation Guide	IN001-070, December 2003
CyberGuard Firewall Release Notes Version 5.2	RN001-5.2, December 2003

Updated Installation and Guidance Documentation

57. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
KS	2706	01/09/03
KS ide	2707	01/09/03
KS tu	2708	01/09/03
KS tu18	2709	01/09/03
KS 1000/1500	2710	01/09/03
KS 1000/1500 u320	2711	01/09/03
FS	2712	01/09/03
FS b	2713	01/09/03
FS 250/500	2714	01/09/03
SL	2715	01/09/03
SL 500 KS RAID	2716	01/09/03
SL 2000 SL 3200 KS 1500R	2717	01/09/03
KS 1500R	2611	10/29/02
FS 250/500	2718	01/26/03

Updated Product CD-ROM Media

XIV.5.2 PSU 1 (P5x2p1)

58. There were some security relevant changes to the source code of this TOE derivative.

59. The updated Installation and Guidance documentation relevant to this TOE derivative is detailed in the table below.

Document	Reference and Date
README File on CD-ROM and CyberGuard website.	N/A

Updated Installation and Guidance Documentation

60. The CD-ROM media and hardware relevant to this TOE derivative are detailed in the table below.

Hardware	CD-ROM Reference	Date
KS	2721	09/10/04
KS ide	2722	09/16/04
KS tu	2723	09/10/04
KS tu18	2724	09/10/04
KS 1000/1500	2725	09/10/04
KS 1000/1500 u320	2726	09/10/04
FS	2727	09/10/04
FS b	2728	09/10/04
FS 250/500 FS 300/600	2729	09/10/04
SL	2730	09/10/04
SL 500 KS RAID	2731	09/10/04
SL 2000 SL 3200 KS 1500R	2732	09/10/04
FS 300/600 nfd	2733	12/10/04

Updated Product CD-ROM Media

ANNEX A: NOTES ON TOE DERIVATIVE TESTS

1. This annex summarises the TOE derivative testing.

2. The CyberGuard Firewall test suite is fully automated and includes all security tests from the original evaluation, but updated as appropriate to cater for new product functionality, new potential vulnerabilities and more recent versions of the appropriate test tools.

3. Each new software release or PSU has been tested on the various appliance models (or enhancements) marketed at the time. In each case the firewall was subjected to the full set of firewall security tests, which include auto regression and repetitive tests that exercise all the Security Functions, all TOE components and all TOE changes. The repetitive tests include testing for vulnerabilities using tools such as Internet Security Scanner (Version 6.2.1), Nessus (Version 2.0.12), NMAP (Version 3.0) and Jolt 3 (Version 2.0).

4. During the AMA Audits, the Evaluators examined the test records for the TOE derivatives and confirmed that there was suitable evidence of security testing for all TOE derivatives.

5. During AMA Audit No 2, the Evaluators requested that the automated test suite be re-run against 2 sample TOE derivatives, Release 4.3 PSU 4 (on a Premium Appliance Firewall FS500) and Release 5.1 (on a Premium Appliance Firewall KS1500). The Evaluators confirmed that the test results were satisfactory.

6. During AMA Audit No 3, the Evaluators requested that the automated test suite be re-run against 2 sample TOE derivatives, Release 5.1 PSU 2 (on a Premium Appliance Firewall FS500) and the most recent Release 5.2 PSU 1 (on a Premium Appliance Firewall KS1500). The Evaluators reviewed the test results and checked that a sample of changes, which they had previously examined in the on-line tracking database, had been correctly tested by the updated test suite. The Evaluators confirmed that the regression and change test results were satisfactory.

(This page is intentionally left blank)