ASSET DISPOSAL & INFORMATION SECURITY ALLIANCE

Claims Testing Application Form

Form Number ADPC00036

Section 1 – Applicant Information

Company Name: White Canyon
Address: 947 South 500 East American Fork UT, 84003

General Contact
Name: Nathan Jones
Phone: 801.224.2955
Mobile: 801.472.8770
E-Mail: Nathan.jones@whitecanyon.com

Section 2 – Applicant Software Information

Manufacturer: WhiteCanyon Software Inc.
Version of software: WipeDrive Enterprise 8.1.4

Background (Explanation of the company and software)

WhiteCanyon is the leading provider of secure data destruction software to the Fortune 100 an is the only tool to be certified to the Common Criteria EAL4+ standard.

Technical / physical architecture of claims test applicant software.

WipeDrive is run from a live Linux OS which loads on the client at startup.

Best practice usage guide for usage of software being tested. (Please enclose any manuals)

User Guide is attached

Host Information for claims test applicant software to run on. To be shipped by test claimant.

The drives to be tested can be wiped on any x86 server, laptop or desktop provided that a wipe pattern with a hardware level overwrite pass is used.

Section 3 – Test Hardware Information

Device 1

Solid State Storage Device chip set of device.

Manufacturer: Micron

Model: Micron MSOO SATA SSD

Capacity: 480Gb

Controller: n/a

NAND Chipset n/a

Drive serial no. 1338095284C7

Device 2

Solid State Storage Device chip set of device.

Manufacturer: Micron

Model: Micron C400 SATA SSD

Capacity: 512Gb

Controller: n/a

NAND Chipset n/a

Drive serial no. 1310092E5739

ADISA Threat Matrix

Risk Level	Threat Actor and Compromise Methods	Test Level
1 (Very Low)	Casual or opportunistic threat actor only able to mount high-level non-invasive and non-destructive software attacks utilising freeware, OS tools and COTS products.	1
2 (Low)	Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	1
3 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising COTS products.	2
4 (High)	Commercial data recovery and computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising both COTS and bespoke utilities.	2
5 (Very High)	Government-sponsored organisations or an organisation with unlimited resources and unlimited time capable of using advanced techniques to mount all types of software and hardware attacks to recover sanitised data.	3

Section 4 – The Claim

White Canyon's software called Wipedrive Enterprise 8.1.4, when used in accordance with User Manel "WipeDrive 8 Enterprise Manual" and using NIST 800.88 wipe pattern, will overwrite all available data on the hardware sample within this test to protect to a forensic attach equivalent to test level 2 of the ADISA threat matrix.

Claim Technical Contact at applicant.

Name: Todd Manning
Phone:
Mobile: 801.440.0415
E-Mail: todd.manning @whitecanyon.com

Acceptance

I, Nathan Jones of WhiteCanyon Software Inc. confirm that the information outlined in this document is an accurate and true reflection of the claims made by our product wishing to undergo the ADISA testing method.

Signed on behalf of WhiteCanyon Software Inc.

SIGNED: Nathan Jones
NAME: Nathan Jones
TITLE: VP of Sales
DATE: 11.29.2017

Claim Accepted by:

Signed on behalf of University of South Wales

SIGNED:
NAME: Andrew Blyth
TITLE: Professor
DATE: 1st December 2017

Signed on behalf of ADISA

SIGNED:
NAME: Steve Mellings
TITLE: Director
DATE: 1st December 2017