CLAIMS TESTING APPLICATION FORM

FORM NUMBER: ADPC102

SECTION 1 – APPLICANT INFORMATION

Company Name: Extreme Protocol Solutions

Address: 10 River Road, Suite 101, Uxbridge, MA 01569 (USA)

General Contact

Name: Roger Gagnon

Phone: (508)278-3600 x 112

Mobile: (508)579-8370

E-Mail: rgagnon@extremeprotocol.com

SECTION 2 – APPLICANT SOFTWARE INFORMATION

Manufacturer: Extreme Protocol Solutions

Version of software: XErase – Enterprise Data Erasure V14

Version of user manual: XErase Enterprise Data Erasure V14 Manual

Algorithm to be used: NIST800-88r1 CLEAR

Please describe the means of deployment for your software/hardware product:

XErase will determine the most secure level of NIST800-88r1 Clear supported by each individual device. Options for Clear would be a SCSI Format, Secure Erase or a 1x or 3x Overwrite of the media depending on user settings. XErase will execute the selected method and perform a verification of the erasure before rendering a PASS or FAIL result for the device. Once successfully completed, all user-accessible data will be overwritten/destroyed to protect from a forensic attack equivalent to test level 1 of the ADISA threat matrix.

Please list the equipment you are intending to ship to execute the test, or the means to access/download your software tool:

EPS has varied solutions for direct connected erasure. At time of testing EPS will provide hardware and software to facilitate erasures using the various deployment methods indicated in the physical architecture claim section.

© Copyright ADISA 2019

CLAIMS TESTING APPLICATION FORM

SECTION 3 – MEDIA WHICH YOUR PRODUCT IS TO BE TESTED ON

2 x SSD and 1 x NvME SSD

ADISA Threat Matrix

RISK LEVEL	THREAT ACTOR AND COMPROMISE METHODS	TEST LEVEL
1 (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. Commercial data recovery organisation able to mount non-invasive and non-destructive software attacks and hardware attacks.	**1**
2 (Medium)	Commercial computer forensics organisation able to mount both non-invasive/non-destructive and invasive/ non-destructive software and hardware attack, utilising COTS products. 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**
3 (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**

© Copyright ADISA 2019

CLAIMS TESTING APPLICATION FORM

SECTION 4 – THE CLAIM

Extreme Protocol Solutions Inc. software/ product called XErase Enterprise Data Erasure V14.0 utilising algorithm NIST CLEAR and, when used in accordance with User Manual V14.0 will overwrite all user data on the media sample within this test to protect from a forensic attack equivalent to test level 1 of the ADISA threat matrix.

I, Roger Gagnon of Extreme Protocol Systems 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 Extreme Protocol Systems

SIGNED:

NAME: Roger Gagnon

TITLE: President/CEO

DATE: 5/20/2021

ACCEPTANCE

Claim Accepted by:

ADISA Research Centre

SIGNED:

NAME: Godfred Badu

TITLE: Forensic Analyst

DATE: 02.06.2021

© Copyright ADISA 2019