12600 Fair Lakes Dr., Suite 210
Fairfax, VA 22033
703.267.6050
corsec.com

November 5, 2025

**RE: OPSWAT FIPS 140-3 Publication**

OPSWAT
11111 Street
San Francisco, CA 99999
USA

To Whom It May Concern:

Corsec Security, Inc. has conducted an analysis of the OPSWAT MetaDefender NDR product, assessing product operations for the Federal Information Processing Standard Publication 140-3 (FIPS 140-3).

As issued by the National Institute of Standards and Technology (NIST), FIPS 140-3 specifies the security requirements that must be satisfied by a cryptographic module used in a security system protecting sensitive but unclassified (SBU) information. Corsec has reviewed the architecture, features, operations, and cryptographic components in OPSWAT's product and provides the following conclusions:

- OPSWAT has implemented the use of several embedded validated cryptographic modules
- FIPS mode has been explicitly enabled where applicable
- Cryptographic algorithms utilized are FIPS 140-3 approved algorithms
- Communication to MetaDefender NDR is secured using Transport Layer Security (TLS) utilizing FIPS 140-3 validated components
- OPSWAT's utilization of these cryptographic components is in accordance with the requirements of FIPS 140-3

Corsec attests that the MetaDefender NDR incorporated FIPS-Approved cryptographic services provided by FIPS-validated Cryptographic Libraries and **PASSED** Corsec's **FIPS Verified** process.

For any additional information I can provide on this matter, please do not hesitate to call me at (703) 267-6050.

Sincerely,

Matthew Appler
CEO, Corsec Security, Inc.

12600 Fair Lakes Dr., Suite 210
Fairfax, VA 22033
703.267.6050
corsec.com

Companies are routinely asked to provide “proof” that their products are compliant to the FIPS 140 standard. Corsec is a trusted third-party advisor to the FIPS validation program having worked directly with NIST over the past 27 years to help review and develop security requirements. Corsec’s unique understanding of the ins-and-outs of certification requirements specific to product architecture allows for a wholistic approach to answering questions and requests from governments and product vendors around the globe.

Corsec has reviewed MetaDefender NDR architectural design and documentation to verify the product satisfies government and regulated industries requests for FIPS 140-3 compliance.

Corsec’s evaluation included block diagram analysis of the OPSWAT NDR product and its components, as well as thorough review of the cryptographic utilization.

**Utilized FIPS 140-3 Validated Modules**

| FIPS 140 Provider | Certificate Number |
|---|---|
| Oracle Linux 8 OpenSSL Cryptographic Module | #4215 |
| Oracle Linux 8 libgcrypt Cryptographic Module | #4232 |
| Oracle Linux 8 NSS Cryptographic Module | #4226 |
| Oracle Linux 8 GnuTLS Cryptographic Module | #4229 |