OPSWAT.

DATASHEET

SWIFT CSCF V2027

Technical Controls Supporting Secure Financial File Workflow

How OPSWAT supports financial institutions with mandatory Swift customer security controls.

The Swift Customer Security Controls Framework (CSCF) is the mandatory security baseline for every organization connected to Swift. OPSWAT provides prevention-first technologies that protect files, data flows, and connections before they reach payment systems.

Use Case	CSCF v2027 Controls	OPSWAT Capability
Malware protection	6.1 Malware Protection; 6.1; 6.5A Intrusion Detection (advisory)	Scans files with 30+ anti-malware engines (Metascan™ Multiscanning). Sanitizes and regenerates files with Deep CDR™ technology, and analyzes suspicious files in Adaptive Sandbox to help catch evasive and zero-day threats.
Secure data flows	2.4 Back-Office Data Flow Security;	Prevent malicious file transfers by inspecting content moving between back office and Swift-related systems with MFT solution
Storage and back-ups	2.5A External Transmission Data Protection	Files at rest in storage repositories, where back-ups and extracts land, are scanned and checked for sensitive content (Proactive DLP™).
Software supply chain security	2.2 Security Updates; 2.7 Vulnerability Scanning; 6.2 Software Integrity	Scans software packages and; dependencies of in-house connector software for vulnerabilities and malicious components before deployment
Web applications accepting file uploads	Customer connectors in scope (architecture A4), including customer-facing web servers	Scans and sanitizes every uploaded file before it reaches the application or the Swift flow behind it, through REST API or WAF integration via ICAP
Logging & monitoring	6.4 Logging and Monitoring	Logs every inspection event and forwards audit trails to SIEM (Security Information and Event Management) tools.
Secure removable media	3.1 Physical Security	Scans and sanitizes peripheral media and transient devices at a checkpoint before entry.

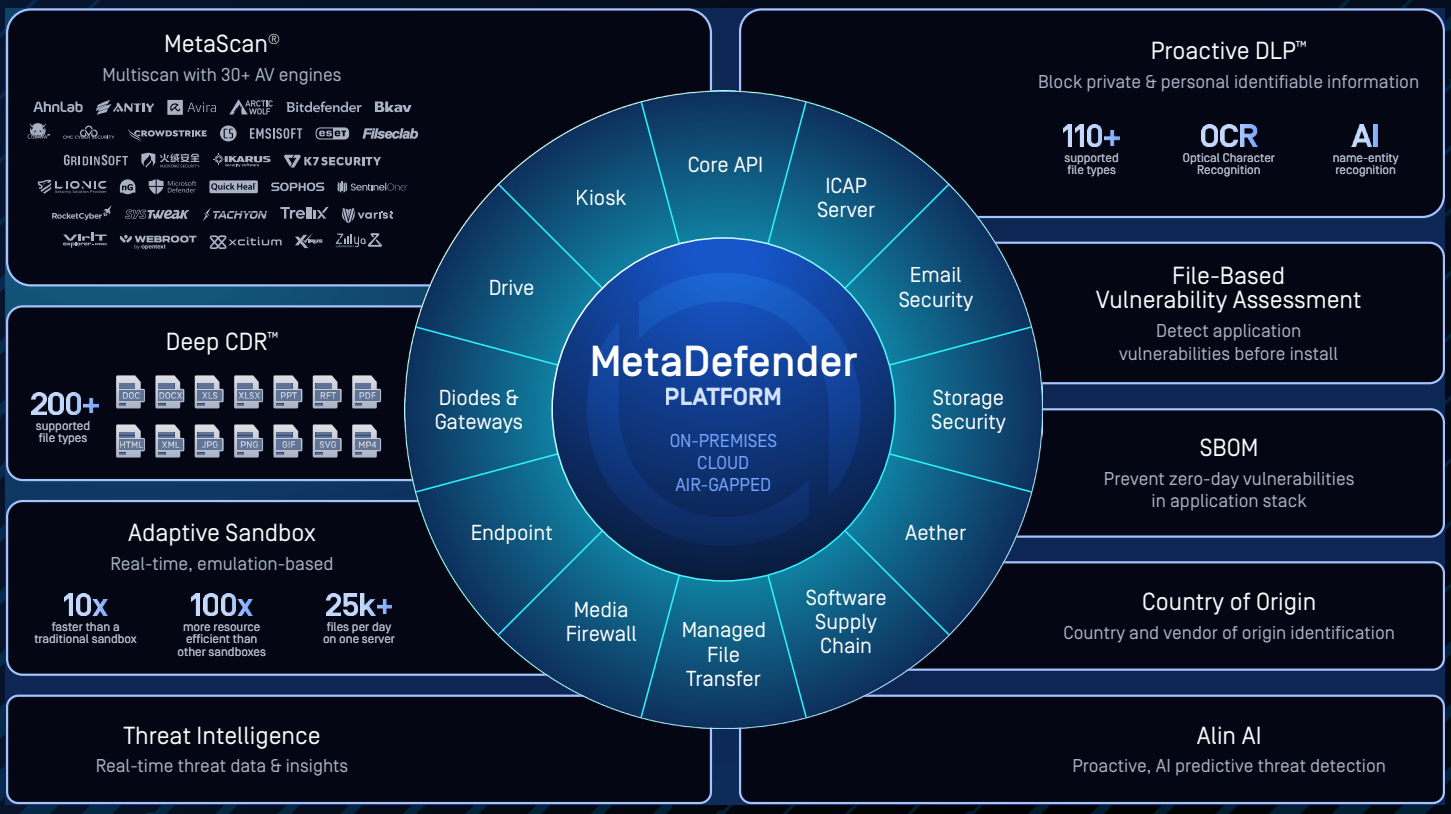
OPSWAT technologies support the implementation of these controls; compliance assessment and attestation remain the responsibility of each institution.

OPSWAT prevention layer: all file content is scanned, sanitized, and verified before it moves deeper into an environment.

Secure financial file workflows · Prevention over detection · Improved resilience · Evidence for auditors

CSCF v2027 At a Glance

32	Security controls across seven security principles
26	Mandatory controls – the baseline for all users
6	Advisory controls – recommended good practice that may become mandatory in later versions
Jul-Dec 2027	KYC attestation window against CSCF v2027, supported by independent assessment



Learn more about how OPSWAT supports your Swift CSCF v2027 requirements

Chat with an expert at:
opswat.com/get-started | sales@opswat.com

©2026 OPSWAT Inc. All rights reserved. OPSWAT, MetaScan, MetaDefender, MetaDefender Managed File Transfer (MFT), MetaAccess, Netwall, OTfuse, the OPSWAT Logo, the O Logo, Trust no file, Trust no device, and Trust no file. Trust no device. are trademarks of OPSWAT Inc.