WHITE PAPER

How to Achieve Regulatory Compliance and Certification with MetaAccess

Covering HIPAA, PCI DSS, GLBA, SOX, GDPR and ISO-27001

OPSWAT.

Introduction

This document details how OPSWAT MetaAccess enables you to meet multiple specific compliance regulations and security certification.

- Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Data Security Standard (PCI DSS)
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes Oxley (SOX)
- General Data Protection Regulation (GDPR)
- ISO/IEC 27001 Security Certification

Published July, 2020

SECTION **1.0**

OPSWAT Secure Access for Health Insurance Portability and Accountability Act (HIPAA)

While OPSWAT is neither the HIPAA Covered Entity (CE) nor the Business Associate (BA), our solutions can assist CEs or BAs with HIPAA Compliance. OPSWAT's Secure Access solutions can support the HIPAA Administrative, Physical and Technical Safeguards as described below:

Administrative Safeguards	OPSWAT Capabilities
Security Management Process	Applies appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the CE (such as limiting or denying network access). Allows for review of audit logs and access reports.
Workforce Security	Enforces role-based access, ensuring only the individuals who have been authorized access will be allowed connection to restricted resources and data.
Information Access Management	Enables creation and modification of policies and procedures that restrict access to ePHI within a subgroup or among subgroups. Based upon the CE's access authorization policies, establishes and modifies a user's right of access to a workstation, transaction, program or process. Employees can be dynamically assigned access to specific resources appropriate for their roles and need to access ePHI.
Security Incident Procedures	Detects malicious activity on endpoints using a scoring system based on CVSS and OPSWAT scores. Automates threat enforcement by alerts via 3rd party integration with existing security incident utilities. Non-compliant devices can be acted on in a variety of ways (none, quarantine, fix violation). Compliance failures are logged for additional analysis post-incident, dated and time stamped.

Physical Safeguards	
Workstation Use	Enables implementation of policies to enable or disable access to specific workstations containing protected information from other systems or devices based on their roles. Can proactively manage endpoint devices on the network and their locations so that only authorized devices are given access, while unauthorized and unmanaged devices are found and prevented from gaining access.

Technical Safeguards	
Access Control	Limits access to healthcare information systems to authorized users and specified devices as well as to authenticates them prior to connection with a zero-trust model. Establishes role-based access determined by a variety of data points and requirements. Evaluates the device configuration, installed software and patch levels for compliance with security policy for devices attempting to connect remotely. Initiates vulnerability assessment of new network devices and can take action upon devices (warn, audit, quarantine or fix).
Integrity Management	Protects ePHI from improper alteration and destruction by limiting access to authorized and pre-authenticated users.

SECTION **1.0**

OPSWAT Secure Access for Payment Card Industry Data Security Standard (PCI DSS)

Achieving compliance with PCI DSS requires strict control over all the devices that use your wired and wireless networks to transmit cardholder data. OPSWAT Secure Access allows two options: restrict the scope of the PCI environment by segmenting Cardholder Data Environments (CDEs) from networks, devices and appliances unnecessary to the PCI audit with a Software Defined Perimeter, or; gain visibility into every user and device on all portions of your network with a traditional NAC solution, which supports seven specific PCI DSS requirements as outlined below:

PCI DSS Requirement	OPSWAT Capabilities
Build and Maintain a Secure Network	**Controls access to your network** based on identity and role-based policies and provides authentication verification for all users' connections on wired, wireless and VPN networks. Furthermore, MetaAccess can deny access to any device attempting to connect to the network that doesn't have personal firewall software installed and force the user to remediate before gaining access.
Do not use vendor-supplied defaults for system passwords and other security parameters	**Supports your organization's configuration standards** by verifying device posture pre- and post- connection to your network, including checking operating system patch policy levels, anti-virus status, and any other system processes for which you wish to check.
Use and regularly update anti-virus software or programs	**Enforces the presence of anti-virus software** on all network-connected devices, and additionally will also enforce that the software is current, up-to-date and actively running on those devices in accordance to the organization's Acceptable Use Policies.
Develop and maintain secure systems and applications	**Enforces organizational policies** around patch policy level for endpoint operating systems and can take immediate action (such as quarantine, forced user remediation or application removal/fix) as soon as a device is found to be out of compliance.
Restrict access to cardholder data by business need to know	**Automatically restricts access rights** to personnel based on their authenticated credentials, job classification, function, and responsibilities.
Assign a unique ID to each person with computer access	**Standards-based authentication technologies** like 802.1x, RADIUS and TACACS + to verify the identity of the person behind each device connecting to the network based not only on their credentials, but on things such as MAC address, IP address, device type, access point and time of day. For remote access, MetaAcces SDP establishes a 'Perimeter of One' for each person with authentication to only the network and applications pre-authorized.
Maintain a policy that addresses information security for employees and contractors	**Develop and maintain policies** that address strict control around access to network resources. Ensuring policy enforcement on remote access technologies, multiple IoT endpoint devices, authentication of all users accessing your network and audit trail logging of time and location-based network connections are all ways that OPSWAT can facilitate compliance with this requirement.

SECTION **1.0**

OPSWAT Secure Access Gramm-Leach-Bliley Act (GLBA)

Proving access to your data that is tightly controlled and highly secured is the key focus of GLBA compliance. Needing to know who has access to what financial records, who has access to share information, and ensuring security policies and patch levels are up to date are just a few of the ways OPSWAT can help. Specifically, OPSWAT Secure Access addresses the following sections of the GLBA:

GLBA Requirement	OPSWAT Capabilities
314 . 3 – Standards for safeguarding customer information (3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.	**Protects against unauthorized access** to information via role-based access control and port-level control, protecting your organization against unauthorized access and the subsequent inconvenience that a large-scale data breach brings along with it.
314 . 4 – Elements (c) – Design and implement information safeguards to control the risks you identify through risk assessment and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems and procedures.	**Provides continuous endpoint** monitoring for security compliance and integration with 3rd party threat remediation products like IDS/IPS and ATD is how OPSWAT helps your organization design and implement safeguards to control identified risks.

OPSWAT Secure Access for Sarbanes Oxley (SOX)

OPSWAT Secure Access solutions help organizations affirm a framework of controls that support accountability and integrity around your financial reporting, documentation and enforcement processes. The applicable sections of SOX where OPSWAT provides support for this compliance are:

SOX Requirement	OPSWAT Capabilities
302.4B – Establish verifiable controls to track data access	**Controls user access to network resources**. Our historical reporting provides your organization with a verifiable audit trail and reports that demonstrate who had what level of access to your network.
404.A.2 – Disclose security breaches to independent auditors	**Correlates user and device identity to acknowledged security events** and can then report on those events to allow for more granular analyzation and disclosure of past security events, in conjunction with SIEM or other security logging solution.

SECTION **1.0**

OPSWAT Secure Access for General Data Protection Regulation (GDPR)

OPSWAT helps organizations comply with GDPR, understanding that GDPR compliance begins with strict control and meticulously tracked access to digital data covered under this regulation. The applicable sections of GDPR where OPSWAT provides support for this compliance are:

GDPR Requirements	OPSWAT Capabilities
Data Access, Article 17 – Right to Erasure	**OPSWAT** satisfies this requirement so that an end user can request data deletion and validation the deletion occurred.
Data Access, Article 25 – Data Protection by Design and Default	**OPSWAT provides granular access** based on contextually aware attributes like a user's role, device type, network location, time of connection and device security compliance.
Data Access, Article 32: Security of Processing	**OPSWAT has real-time and historical reporting**, with ability to provide both ad-hoc and timed management reporting for audit trails.
Data Collection	**OPSWAT** does not collect any "sensitive personal data" as defined.
Data Collection	**OPSWAT** policy notification and guidance web pages do not use cookies to allow the direct identification of users.
Data Collection	**OPSWAT** does collect IP addresses and MAC addresses.
Data Transparency and Deletion	**OPSWAT Captive Portals** can easily communicate what data is collected and define why it is needed.
Data Transparency and Deletion	**OPSWAT Captive Portal** can include a field where an end user provides consent.
Data Transparency and Deletion	**OPSWAT Captive Portal** can include a request for this information to be deleted at a personal record level.

SECTION **2.0**

Security Certification

OPSWAT Secure Access for ISO/IEC 27001

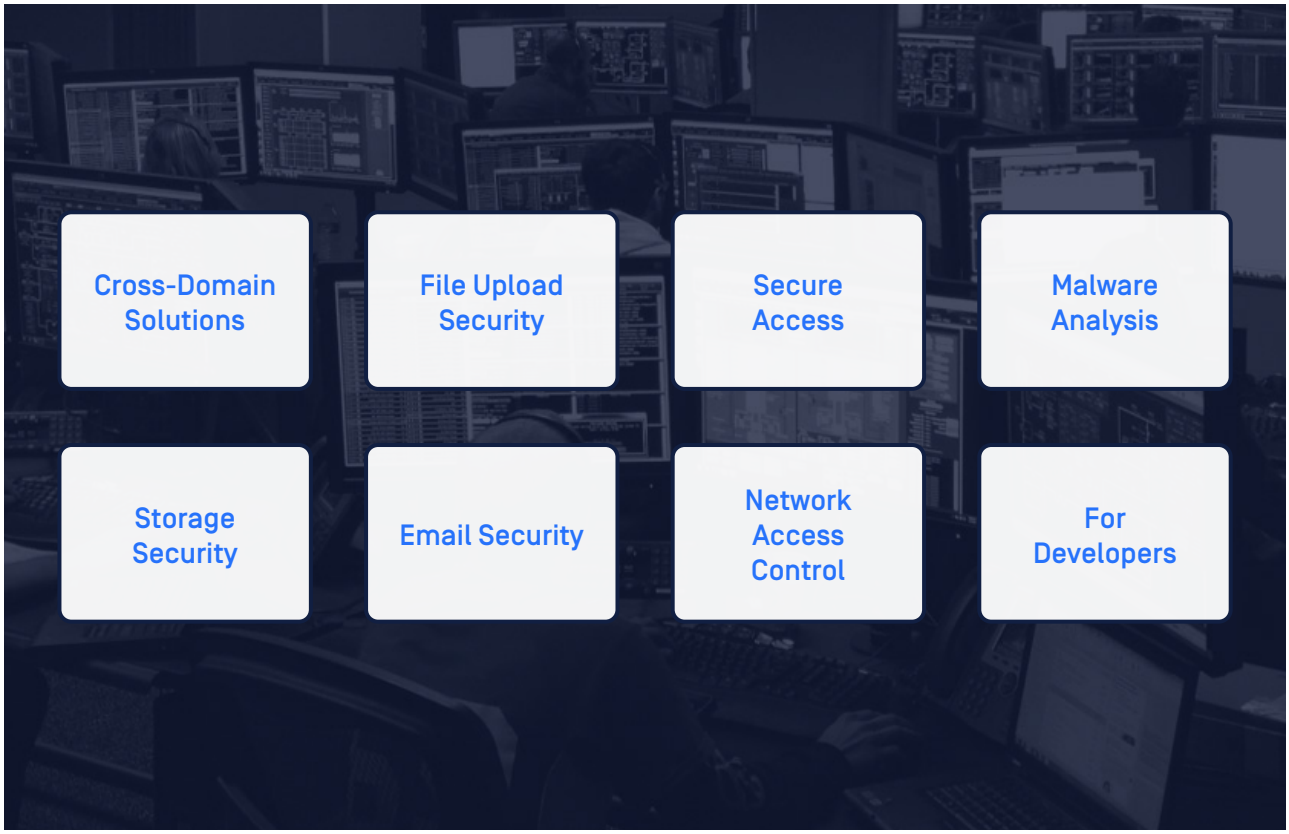
ISO/IEC 27001 helps organizations identify, assess and treat security risks to their information systems. In order to achieve compliance with this standard, organizations must provide enough evidence to auditors that they have put the necessary security controls from Annex A into place. Below are the specific security controls with which OPSWAT Secure Access solutions can help satisfy:

ISO/IEC 27001 Requirement	OPSWAT Capabilities
A.9.1.2 – Access to Networks and Network	**Enforces role-based access**, ensuring only the individuals who have been authorized access will be allowed connection to restricted resources and data.
A.9.2.1 – User registration and de-registration	**Controls user access to network resources**. Our historical reporting provides your organization with a verifiable audit trail and reports that demonstrate who had what level of access to your network.
A.9.4.1 – Information Access Restriction	**Restricts access rights** to personnel based on their authenticated credentials, job classification, function, and responsibilities.
A.9.4.2 – Secure log-on Procedures	**Logs end user connection activity** and end users' AUP compliance failures and provides both historical and real-time reporting for additional analysis to be done.
A.9.4.4 – Use of Privileged Utility Programs	**Controls access to utility programs** that are network-accessible and adds a layer of defense for systems & applications that could potentially be used to circumvent controls.
A.12.4.1 – A.12.4.3 – Logging and Monitoring	**Produces detailed logs** for end user events as well as administrative activities.
A.14.1.2, 14.2.6., 14.3.1 – System Acquisition, Development and Maintenance	**Controls access to your network** based on a variety of authentication policies such as identity, user role, user location, network and device health, and provides authentication verification for all users' connections on wired, wireless and VPN networks. This enables Administrators to create more granular access control to portions of the network that may contain intellectual property, such as development sandboxes and test environments. This assists in securing the development lifecycle of an organization's applications and services they may deliver over public networks.
A.18.1.3, A.18.1.4 - Compliance	**Collects Contextual Intelligence to verify the identity of users and the health of their device as they seek access to a network.** This protects sensitive data like Personally Identifiable Information (PII) from unauthorized access.

SECTION **3.0**

About OPSWAT

OPSWAT protects critical infrastructure. Our goal is to eliminate malware and zero-day attacks. We believe that every file and every device pose a threat. Threats must be addressed at all locations at all times—at entry, at exit, and at rest. Our products focus on threat prevention and process creation for secure data transfer and safe device access. The result is productive systems that minimize risk of compromise. That's why 98% of U.S. nuclear power facilities trust OPSWAT for cybersecurity and compliance.



Visit us on LinkedIn, Twitter, Facebook, and YouTube.

Contact us at opswat.com/contact for pricing information, evaluation accounts, technical presentations, or to request a quote.

OPSWAT.

Trust no file. Trust no device.