OPSWAT.

Achieving Regulatory Compliance and Security Certification with SafeConnect Network Access Control

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

The core of regulatory compliance standards revolves around knowing who, what, when and where for devices and users on your network and controlling access to the data your company needs to keep secure. OPSWAT helps you achieve that visibility, security and control, while automating policies that validate accountability and mitigate vulnerabilities and evolving threats – ensuring your compliance come audit time.

REGULATORY COMPLIANCE

SafeConnect for Health Insurance Portability and Accountability Act (HIPAA)

While OPSWAT is neither the HIPAA Covered Entity (CE) nor the Business Associate (BA), this solution can assist CEs or BAs with HIPAA Compliance. OPSWAT's SafeConnect NAC solution delivers HIPAA compliance pertaining to visibility, the control of access to the network, protecting EPHI, and creating and enforcing information security policies specific to the following HIPAA Security Rules:

HIPAA REQUIREMENT	SAFECONNECT CAPABILITY
Identity of a person or entity seeking access to EPHI must be verified. All users should have unique identifiers or login IDs to information systems and electronic PHI	**SafeConnect integrates with directory structures** and will enforce access based upon authorized credentials.
Limit access to EPHI only to those persons or software programs that have been granted specific access rights	**SafeConnect can enforce role-based access**, ensuring only the individuals who have been authorized access will be allowed connection to restricted resources and data.
Organizations must maintain audit trails that log all access to system information	**SafeConnect 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. All information is dated and time stamped.
Organizations must identify, respond to and mitigate suspected or known security incidents and document security incidents and their outcomes	**SafeConnect can automate threat enforcement** by alerts via its integration with a customer's existing SIEM, IDS or ATD system and perform a quarantine on an endpoint that is the cause or part of a known security incident flagged by that integrated system. The quarantine of that device will be documented and logged in the SafeConnect system for auditing purposes.

SafeConnect 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. SafeConnect gives you visibility into every user and device on all portions of your network, and provides support for seven specific PCI DSS requirements:

PCI DSS REQUIREMENT	SAFECONNECT CAPABILITY
Build and Maintain a Secure Network	**SafeConnect 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, SafeConnect 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	**SafeConnect 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	**SafeConnect will enforce 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	**SafeConnect will enforce a customer's policies** around patch policy level for endpoint operating systems and can take immediate action (such as quarantine and forced user remediation) as soon as a device is found to be out of compliance.
Restrict access to cardholder data by business need to know	**SafeConnect is an automated access control system** that can restrict access rights to personnel based on their authenticated credentials, job classification, function, and responsibilities.
Assign a unique ID to each person with computer access	**SafeConnect utilizes industry standards-based authentication technologies** like 802.1x, LDAP and RADIUS 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 to allow for enforcement of the most granular of access policies.
Maintain a policy that addresses information security for employees and contractors	**SafeConnect makes it easy for your organization** to develop and maintain a policy that addresses 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 SafeConnect can facilitate compliance with this requirement.

SafeConnect for 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 SafeConnect can help. Specifically, SafeConnect addresses the following sections of the GLBA:

GLBA REQUIREMENT	SAFECONNECT CAPABILITY
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	**SafeConnect 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.	**SafeConnect provides continuous endpoint** monitoring for security compliance and integration with 3rd party threat remediation products like IDS/IPS and ATD is how SafeConnect helps your organization design and implement safeguards to control identified risks.

SafeConnect for Sarbanes Oxley (SOX)

SafeConnect helps 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 SafeConnect provides support for this compliance are:

SOX REQUIREMENT	SAFECONNECT CAPABILITY
302.4B – Establish verifiable controls to track data access	**SafeConnect satisfies this requirement** with its ability to control 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	**SafeConnect is capable of correlating 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.

SafeConnect for General Data Protection Regulation (GDPR)

SafeConnect 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 SafeConnect provides support for this compliance are:

GDPR REQUIREMENTS	**SAFECONNECT CAPABILITY**
Data Access, Article 17 – Right to Erasure	**SafeConnect satisfies this requirement** End user can request data deletion and validation it has occurred.
Data Access, Article 25 – Data Protection by Design and Default	**SafeConnect 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	**SafeConnect has real-time and historical reporting,** with ability to provide both ad-hoc and timed management reporting for audit trails.
Data Collection	**SafeConnect** does not collect any "sensitive personal data" as defined.
Data Collection	**SafeConnect** policy notification and guidance web pages do not use cookies to allow the direct identification of users.
Data Collection	**SafeConnect** does collect IP addresses and MAC addresses.
Data Transparency and Deletion	**SafeConnect captive portals** can easily communicate what data is collected and define why it is needed.

Data Transparency and Deletion	**SafeConnect Captive Portal** can include a field where an end user provides consent.
Data Transparency and Deletion	**SafeConnect Captive portal** can include a request for this information to be deleted at a personal record level.

SECURITY CERTIFICATION

SafeConnect 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 SafeConnect solutions can help satisfy:

ISO/IEC 27001 REQUIREMENTS	SAFECONNECT CAPABILITY
A.9.1.2 – Access to Networks and Network Services	**SafeConnect can enforce 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	**SafeConnect satisfies this requirement** with its ability to control 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	**SafeConnect is an automated access control system** that can restrict access rights to personnel based on their authenticated credentials, job classification, function, and responsibilities.
A.9.4.2 – Secure log-on Procedures	**SafeConnect 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. All information is dated and time stamped.
A.9.4.4 – Use of Privileged Utility Programs	**SafeConnect 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	**SafeConnect produces detailed logs** for end user events as well as administrative activities. These logs can be exported into log management tools for additional analysis. Furthermore, SafeConnect can also protect access to these log management tools.

A.14.1.2, 14.2.6., 14.3.1 – System Acquisition, Development and Maintenance	**SafeConnect 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	**SafeConnect uses a variety of avenues to collect 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.

OPSWAT SafeConnect NAC

SafeConnect NAC ensures that every network connection and endpoint device is visible and allowed or blocked appropriately in real-time. Don't risk your organization's data and reputation by exposing it – instead ensure that the security of your network, your constituents' personal information, and your intellectual property remains intact.

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.

How OPSWAT SafeConnect NAC Helps Regulatory and Certification Compliance
Compiled May 2020
All information acquired through publicly available sources or by working with the individual diode vendors.
Please report errors or updates to https://www.opswat.com/contact