SafeConnect's Privacy Policy

Maintaining the privacy of end users is a primary design consideration and long-term objective of the Impulse SafeConnect™ Network Access Control (NAC) Solution.

SafeConnect enables organizations to take more proactive measures in ensuring a secure IT infrastructure. The goal is to provide for an environment free of security threats and vulnerabilities—which promotes the exchange of ideas, information, and content to create a positive and productive network environment for all parties.

Each campus maintains full and complete control over their own policies and how, or even if, these policies are enforced. Each campus determines their strategy for allowing full access, warnings, quarantines, and remediation.

Personal Information
The software installed as part of the SafeConnect Solution (i.e., the Policy Key) does not report or log any activity other than what is required to ensure end user compliance with the endpoint security policies set forth by the organization.

No direct personal information is collected or stored. In situations where the end user device is found to be out of compliance with stated security policies, the SafeConnect system will warn or quarantine the endpoint device based on the policies defined by the organization within the SafeConnect Policy Manager.

SafeConnect collects no information until it is configured by the user's policy administrator. All queries of a user's machine must be explicitly formulated by the organization's policy administrator before they can be evaluated by SafeConnect. SafeConnect does not, and cannot, gather any personal information. Your organization's policy administrator has sole control over policy configuration, and can only create checks that result in a pass/fail result.

Additionally, SafeConnect has been designed with personal privacy in mind and can respond to a limited range of true/false questions. These questions center around the health and configuration of the endpoint and the impact it may be having on network performance. The system cannot respond to open-ended questions, or general requests for information. The system can only return a true/false answer and the transaction occurs over an encrypted communications channel. For example, "Is XYZ anti-virus software up to date and running on this device?" The answer is either true or false.

SafeConnect collects no information until it is configured by the user's policy administrator.

Impulse.com

Programs, Files, and Content
Real-time policy status metrics of endpoint devices under policy management are kept in a secure database within the SafeConnect Policy Enforcer Appliance, which remains on the organization's premises. The SafeConnect system database contains no information that can link directly back to end user personal content. The data collected is related only to the status of specific policies defined by the organization. Under certain circumstances end users may be denied network access and quarantined based on the organization's acceptable use policy enforcement rules. In such circumstances the system provides remediation guidance to the end user to become compliant with security policy.

As always, the data collected is related only to policy status and it is used solely for statistical trending and compliance auditing by the organization.

In short, Impulse will never collect or store personal information from its customer's constituents, and will never communicate directly with end users outside of a SafeConnect Managed Network environment.

24/7 Managed Support Service
Impulse's managed support service (i.e., proactive system monitoring; problem determination and resolution; software/hardware maintenance and version enhancement upgrades; and daily policy configuration backup and recovery services) is supported from an SSAE 16 compliant data center support facility.

Q: Does the SafeConnect solution collect personal information?
A: No. SafeConnect does not gather any information, or perform any checks, that are not configured by a policy administrator. SafeConnect is completely passive until it is configured by the organization's policy administrator. All queries of a user's machine must be explicitly formulated by the organization's policy administrator before they can be evaluated by SafeConnect. Impulse will never collect or store personal information from its customer's constituents.

Q: What is a Policy Key?
A: The SafeConnect Policy Key is a lightweight persistent client agent (less than 1MB in size). The SafeConnect Policy Key certifies that the endpoint device adheres to the specific endpoint security policies of the organization on a continuous/real-time basis.

Q: How do you get a Policy Key?
A: The Policy Key is downloaded to a new user as part of the device registration process. It can also be pre-distributed via the organization's software distribution mechanism of choice for managed environments, such as MS SCCM, Zenworks or through active directory group policies.

Q: Can you refuse to have a Policy Key installed on your computer?
A: Yes. However, the decision on who can, and cannot, access an organization's network remains with the organization that owns and manages the network. Many organizations require that users must read, accept, and adhere to a collection of Acceptable Use Polices (AUP) as a condition of gaining access to the network. This may include the installation of a policy key. This, of course, is the decision of the organization.

Q: Does the Policy Key stay on the computer forever?
A: No. The SafeConnect Policy Key automatically dissolves (uninstalls itself) after a pre-determined time of inactivity. Users can also uninstall the Policy Key themselves if they choose.

Q: How can I be sure that SafeConnect is not gathering personal information?
A: Impulse is committed to protecting the privacy of your organization and the end user community you support. We have established security, technology, and business processes to ensure that personal information is never collected or stored by our applications or services.

An independent examination of our privacy practices certifies that Impulse and the SafeConnect product both conform to the American Institute of CPAs (AICPA) standards. The completion of a Service Organization Controls - Type 2 (SOC 2) Privacy Report resulted in an independent CPA firm finding that Impulse's Privacy Statement is accurate.

Impulse | Experience the Freedom.
Impulse is the leading provider of Contextual Intelligence™ and access control solutions in support of BYOD-friendly enterprises. Impulse securely and efficiently automates BYOD by combining our real-time, context-aware and simplified architecture, remote managed support services and customer-centric business philosophy to enable customer freedom. Our customers know this as the Impulse Experience. The security of more than four million endpoints is entrusted to Impulse. Visit www.impulse.com