Solution Brief

SafeConnect for the Healthcare Industry

The average cost of a data breach for healthcare organizations is estimated to be more than $2.2 million. Despite this, about half of covered entities have little to no confidence that they can detect all patient data loss or theft that may occur on their networks.[1]

SafeConnect gives healthcare organizations the visibility and control they need to ensure electronic protected health information (ePHI) is kept secured.

The IT Security Challenge

Mobility is paramount not only for doctors, nurses and other medical facility professionals, but for those working for any covered entity in the industry. From retrieving patient records to ordering lab tests or medications, on-demand access is needed from a growing number of device types. Add in the challenge of integrated HIPAA regulations, and the requirement for network access control becomes more urgent than ever to ensure HIPAA compliance as well as the safety of your patient data.

How SafeConnect Helps

By verifying the identity of anyone seeking access to your network resources, limiting access to only those who need it, and maintaining event information for audit time, SafeConnect plays an integral part in securing your ePHI.

SafeConnect integrates with any LDAP structure such as Active Directory to create role-based access for your most sensitive data. This ensures that only those people with the designated role or rights to information are granted access.

Crafting an enforcement policy to ensure you are preventing and correcting any security violations is a key rule under HIPAA regulations. With SafeConnect, you can create network access policies that are as granular as you need them to be - whether it's controlling a single device to enforcing a policy facility-wide. SafeConnect then provides you with automated enforcement actions tailored to meet the needs of your organization based on the security violation.

The historical and real-time reporting capabilities of SafeConnect allow you to easily access detailed information necessary during audits, such as policy compliance, policy failure, and actions taken to remediate. All reports are kept for one year and can be exported easily for extended periods thereafter.

HIPAA Security Rule	How SafeConnect Helps
Identity of a person or entity seeking access to ePHI must be verified.	SafeConnect integrates with directory structures and will enforce access based upon authorized credentials.
Limit ePHI access only to those persons or software programs with 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 failures at compliance to an organization's AUPs and provides both historical and real-time data and time-stamped reporting.
Organizations must identify, respond to and mitigate suspected or known security incidents and document security incidents and their outcomes.	SafeConnect can immediately receive security incident information from an existing ATD, SIEM or IDS solution and take quarantine action on devices that are suspected or known to be part of said incident. Furthermore, SafeConnect's historical reporting stores documentation of these incidents for audit.

SafeConnect automates your security policies – from assessing compliance with security policies to determining if a specific application is running on a device while it is on the network. Other features include the following:

- Real-time agentless device identification of endpoints and user authentication prevents unauthorized devices and users from accessing critical network resources
- Dynamic identity-based network and application access assignment based on the role a user plays at your organization
- Guest self-enrollment and automated verification, including multiple guest access profile options and approval policies
- Self-guided remediation allows users to conform to security policies without help desk support

Experience Service Like Never Before

The *Impulse Experience* is the result of our real-time contextual intelligence, simplified access control architecture, US based remote managed deployment and support services, and customer-centric business philosophy that delivers freedom to all facets of the organization. It's not just one thing we do, it's everything.

In addition to its simplified network access control architecture and enhanced user experience design, a key unique customer benefit is how the SafeConnect solution is delivered and supported as compared with other NAC vendor alternatives.

Installation: The SafeConnect solution is premise based and delivered to the customer commonly as a VMware or Hyper-V virtual appliance, but hardware is also available for an additional cost. A single SafeConnect instance supports up to 30,000 concurrent endpoints but the system can be scaled with additional nodes to over 150,000 concurrent endpoints.

Integration: The installation of SafeConnect requires minimal technical resources. In short, the system simply needs to be downloaded and deployed within your VMware or Hyper-V environment, or the hardware needs to be installed in a rack and powered on. Once that is completed, an Impulse Engineer will work remotely with the customer through our 5-step implementation process. This includes integrating with your network infrastructure, establishing communications with your directory services with self-service scripts and guides, and any other security integrations for Contextual Intelligence like a SIEM or NGFW.

Implementation: An Impulse Engineer will work with you remotely on policy creation and implementation. You will be guided through the deployment process with recommendations and direction. This includes branding, hands-on and video training, and best practices so that you will have a fully functional solution including a communication plan to your users.

Support: SafeConnect is supported by the industry's only comprehensive managed support services offering. Impulse will provide continuous, around-the-clock (24x7x365) proactive monitoring and support. The Impulse Support team owns the responsibility of determining the problem including owning any updates, configuration changes or actions required for resolution.
Impulse will also provide consultative "how to" support services.

Update: Daily system updates for device profiles and OS/AV fingerprints, as well as policy configuration backups are included. In a world where users change and update their devices on a frequent basis, it is imperative that the security solution keeps ahead of these changes. When new versions are available, or maintenance updates are required, Impulse will proactively notify you and will perform the update, for as long as you remain under an annual maintenance agreement.

impulse

Impulse | A SafeConnect Network is a Secure Network Impulse is the leading provider of Secure Access for traditional networks as well as remote and cloud access. Impulse securely and efficiently automates this access for organizations of all sizes and needs by combining our simplified access control architecture, remote managed support services, and customer-centric business philosophy to enable customer and IT security freedom. Our customers know this as the Impulse Experience. Visit www.impulse.com

1 Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute