Solution Brief

safe•connect

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

SafeConnect Solution Offerings

Identity Access Control. SafeConnect automatically recognizes when devices attempt access to wired, wireless, or VPN networks and provides agentless device profiling, user authentication, browserless Internet of Things (IoT) device enrollment, self-provisioning guest access management and real-time contextual intelligence reporting. This is an ideal solution to enable context-aware device visibility (identity/role, device type profiling, location, IP/MAC Address, and ownership/liability). Network access policies can be assigned by role, for example, enabling different privileges for faculty, visiting staff, patients or guests.

Device Security. SafeConnect enhances the security posture of your network by providing real-time policy assessment, enforcement, and self-remediation for Windows & MAC OS X devices. Every user's system is checked prior to granting network access to ensure that the device adheres to your acceptable use policies (anti-virus, operating patches, personal firewalls, peer-to-peer software, etc.) as well as on a continuous basis after access is granted. Web-based, self-remediation orchestration enables users to conform to security policies without help desk involvement.

Secure BYOD On-Boarding. Welcome every new user with a captive web portal that authenticates the end user, configures the device's embedded 802.1X supplicant, and automatically transfers the device to a designated secure SSID network segment. By eliminating manual configuration, the solution delivers a more secure solution with a reduction in help desk calls and dramatically accelerates user adoption of WPA Enterprise or certificate-based secure wireless. Users are automatically associated with their secure wireless network on subsequent network connections without the need for repeated logins.

Network Security Orchestration. SafeConnect's Network Security Orchestration capabilities offer context-aware device visibility, security compliance, access control, and reporting through a single-pane-of-glass that provides enhanced cyber security defenses. Focus on blocking devices rather than making it easier to onboard devices.

- Automate policy enforcement based upon the risk levels reported by intrusion detection system (IDS) and security information and event management (SIEM) providers
- Enforce compliance with mobile device management (MDM) policies, including removing "jailbroken" devices from the network or blocking devices that have had MDM software removed
- Publish real-time Contextual Intelligence information to next-generation firewalls, web content & bandwidth managers, and SIEM providers which enable them to make more granular policies and enhanced security assessment decisions in a timely manner.

Cloud-Managed Support Services. The Impulse Experience is the result of our real-time contextual intelligence, simplified access control architecture, remote managed support services, and customer-centric business philosophy that delivers freedom from excess time, risk and negative experiences to all facets of the organization.

In addition to its simplified architecture and enhanced user experience design, a key benefit is how the SafeConnect solution is delivered and supported. SafeConnect solutions are premise-based, but come with a service that keeps the system updated regarding the latest devices, operating systems, and AV packages. In a world where users change and update their devices on a frequent basis, it is imperative that a security solution keeps ahead of these changes. SafeConnect's Cloud-Managed Support Service includes the following:

- Remote installation, training and deployment assistance
- 24x7 proactive system monitoring
- Problem determination and resolution ownership
- Daily device type, security updates and policy configuration data remote backups
- Installation of all maintenance updates and application version upgrades

Impulse | Experience the Freedom

Impulse is the leading provider of Contextual Intelligence and Network Security Orchestration in support of BYOD and IoT enabled enterprises. Impulse securely and efficiently automates BYOD by combining our real-time, context-aware and simplified access control architecture, remote cloud-managed support services, and customer-centric business philosophy to enable customer 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, May 2016