

SafeConnect for Finance

Cloud-Managed Security Compliance Automation

safeconnect
by impulse



The IT Security Challenge

Today's networks are dynamic, changing with each device accessing it. As endpoints enter and leave the network, the threat landscape changes – and IT departments face the challenge of keeping pace.

Compliance requirements such as the Graham-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), and other industry-specific obligations ushered in a regulatory era that demands stringent IT security compliance. Factor in the mobility demands of customers, employees, and guests; along with the increased rate of cyber-theft - and the mix turns into a risk-management nightmare.

Data security breaches are increasing at an alarming rate in the finance industry – in 2015, the number of breaches doubled from the previous year.¹ SafeConnect is an essential security solution for protecting your network, combining the real-time visibility of controlling the users and devices accessing your network resources with the flexibility to assign different policies by role. This is not a “one size fits all” solution, but one tailored for your different user communities.

Identify, Secure, Orchestrate

SafeConnect is an essential network security solution for protecting your critical data and intellectual property, combining the real-time visibility, security and orchestration required to address regulatory compliance and security policy automation. SafeConnect is delivered as a Cloud-Managed Service that relieves the organization of costly technical support, on-going proactive maintenance, and upgrades.

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

Regulatory Compliance

All core IT regulatory compliance standards revolve around understanding who and what is on your network, where and when they have access, and the ability to automate and control access to sensitive data. SafeConnect helps you achieve that control, create frameworks of accountability and mitigate vulnerabilities – ensuring your compliance at audit time.

- **Sarbanes Oxley (SOX).** Affirm a framework of controls to support accountability and integrity around financial reporting, documentation and enforcement processes, especially concerning Sections 302 and 404
- **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 eight specific PCI DSS requirements
- **Gramm-Leach-Bliley Act (GLBA).** Proving that access to your data 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, ensuring security policies and patch levels are up to date are just a few of the ways SafeConnect can help

How SafeConnect Helps

SafeConnect integrates with any LDAP structure (such as Active Directory) to create role-based access to 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 GBLA and SOX 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 and any security violation (audit, warn and quarantine).

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 on the appliance for one year and can be exported easily for extended periods thereafter.

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, non-browser 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 security policies can be assigned by role, for example, enabling different privileges for executive management, staff and guest.

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 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.

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:

- 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 to all facets of the organization. It's not just one thing we do, it's everything we do.

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

Experience Simplified Security

Simplify the automation and orchestration of your essential security policies, manage the compliance integrity of your network, and enhance the capabilities of your existing security solutions with SafeConnect.

The value of SafeConnect is simply this—by ensuring that the security posture of every endpoint device is monitored and enforced in real-time, the threat associated with security incidents can be reduced substantially. Don't risk your company's data and reputation by exposing it – instead ensure that the security of your network, your customers' personal information, and your intellectual property remains intact.

Impulse | Experience the Freedom

Impulse is the leading provider of Contextual Intelligence™ and access control solutions in support of mobile-friendly enterprises. Impulse securely and efficiently automates managed devices 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. Visit www.impulse.com



¹ : idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches