SafeConnect for Credit Unions

Cloud-Managed Security Automation

The IT Security Challenge and Mobility

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.

It's also difficult to keep pace with regulatory demands, estimated to cost Credit Unions $71 per member per year. The resulting negative consequences for members include higher loan rates, less competitive pricing, fewer products and services, lag times in service delivery, and lack of modernized technology upgrades. [1] Credit Unions can offset those consequences and address competitive market forces by offering an enhanced customer experience within a secure network environment.

Closing the Gap Between Your Customers' Expectations and Experience

Increasingly, financial customers are demanding an integrated, digitized experience that matches or exceeds the service they're getting from nonfinancial businesses. To attract and retain the best customers from every generation, Credit Unions need to overcome the gap between customer expectations and their day-to-day experiences with their credit union or community bank. [2]

Forrester Research talks about a "mobile mind shift" in which consumers *assume* they can access any information or service on their mobile devices at the very moment they need it—because they are able to do so most of the time. More than six in seven U.S. adults (87%) own a mobile phone, 77% of which are smartphones. The US Federal Reserve reports that more than half of these smartphone owners have used mobile banking in the previous year. [3] According to a banking survey, the number-one reason U.S. and Canadian consumers remain with their bank is a good online banking experience. Nearly 38% say that it's their top priority — even more important than low fees (28%). [4]

SafeConnect is an essential security solution that solves both security requirements and user experience conundrums. The solution protects your network by combining the real-time control of 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.

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 and/or devices with the designated role or rights to information are granted access.

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 with the ability to audit and send reports to IT, warn or immediately quarantine the device. Self-remediation steps are brought to the forefront of their screen to enable safe re-connection.

The historical and real-time reporting capabilities of SafeConnect allow you to easily access detailed information necessary for both immediate forensics and 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 and 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] CUNA Regulatory Financial Impact Study, Report of Findings, February 2016
[2] CUNA Regulatory Financial Impact Study, Report of Findings, February 2016
[3] Board of Governors of the Federal Reserve System, "Consumers and Mobile Financial Services 2016," March 2016.
[4] Accenture, 2015 North America Consumer Digital Banking Survey