Solution Brief

safe•connect

Cloud-Managed Security Compliance Automation for Government

Over 707 million data records were lost or stolen in 2015; over 300 million of those were from agencies or public sector entities - a 476% increase in one year.[1]

With roughly 50% of data breaches caused by people inside of an organization[2], it's time your agency took a look at how much control and visibility you have over who's accessing data on your networks.

The IT Security Challenge

Just like their private sector counterparts, government organizations are faced with the ever increasing onslaught of unknown computing devices accessing critical network infrastructure. When it comes to network security, every employee, contractor, customer or supplier is a potential point of vulnerability.

An everyday challenge for IT managers is enforcing security compliance policies and network access privileges without impeding access by their employees, contractors and customers. Agencies are also faced with the daunting task of correlating device information and user identity for things like regulatory compliance and security forensics.

Security breaches like the ones below reinforce the need for a comprehensive NAC solution:

- A breach of Office of Personnel Management databases in 2015 compromised more than 22 million people's social security numbers and other sensitive personal information[3]
- The state of California reported a 34% increase in data breaches between 2013 and 2014[4]
- In 2015, more than 700,000 American taxpayers had their personal information compromised in a data breach of the Internal Revenue Service[5]

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.

- **Payment Card Industry Data Security Standard (PCI DSS)** Identify every user and device on all portions of your network (wired and wireless), and comply with eight specific PCI DSS requirements
- **Health Insurance Portability and Accountability Act (HIPAA)** Control access to the network, safeguard electronic protected health information (ePHI), and create and enforce information security policies

How SafeConnect Can Help

SafeConnect integrates with any LDAP structure 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.

With SafeConnect, you can create network access policies that are as granular as you need them to be. SafeConnect then provides you with automated enforcement actions tailored to meet the needs of your agency and any security violation (audit, warn or quarantine).

SafeConnect allows you to easily access detailed reports necessary during audits, such as policy compliance, policy failure, and actions taken to remediate.

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 related to on-going proactive monitoring, 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

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, staff, students and 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] Gertz, Andrew, Breach Level Index, Gemalto, https://www.gemalto.com/brochures-site/download-site/Documents/ent-Breach_Level_Index_Annual_Report_2015.pdf
[2] https://iapp.org/media/pdf/resource_center/Verizon_data-breach-investigation-report-2015.pdf
[3] Nakashima, Ellen, "Hacks of OPM Databases Compromised 22.1 Million People," www.washingtonpost.com, July 9, 2015. Accessed August 22, 2016.
[4] Author Unavailable, "2014-15 Reports." www.cio.ca.gov, Accessed August 22, 2016
[5] Schreiber, Sally. "IRS Suffers Another Data Breach," www.journnalofaccountancy.com, February 10, 2016 Web, Accessed August 22, 2016.