# Network Security Orchestration

*Cloud-Managed Security Compliance Automation*



## 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.

It is widely recognized that the majority of incidents are deemed avoidable (97%)[1], although many may be extremely difficult in practice.  What's interesting to note is that while many of solutions in place today are focused on external attacks, 70% of all incidents are actually internally sourced.[2]

Business-critical resources are at their most vulnerable—more than 37 percent of data breaches are the result of unauthorized network access.[3] Several recent high-profile retail industry security events were attributed to compromised vendors or lack of automated policy enforcement of untrusted devices.  Each unknown personal or Internet of Things (IoT) device attempting access to your network represents yet another opportunity for invasion, compromise, and business news headlines.

## 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 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 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.
- **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.
- **Gramm-Leach-Bliley Act (GLBA).**  Prove access to your data is tightly controlled and highly secured.

## 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 access policies can be assigned by role, for example, enabling different privileges for executive management, staff, 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 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:



**SAFECONNECT**

**CONTEXTUAL INTELLIGENCE**

- Automate policy enforcement based upon the risk level 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 constituents' 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 BYOD by combining our real-time, context-aware and simplified architecture, remote managed support services and customer-centric business philosophy to enable IT peace of mind and customer freedom. Our customers know this as the Impulse Experience.
Visit www.impulse.com

[1] 2016 OTA Data Protection & Breach Readiness Guide, otalliance.org/resources/data-breach-protection
[2] 2016 Ponemon Cost of Data Breach Study, www-03.ibm.com/
[3] 2016 Ponemon Cost of Data Breach Study, www-03.ibm.com/