Solution Brief

safe•connect

K-12 Districts Simplify Network Security

Many K-12 school districts are recognizing that implementing a BYOD (Bring Your Own Device) policy is an effective approach to enhance the education process by leveraging 21st century technology already owned by their staff and students.
However, it can represent a big cultural change for the learning environment as well as a challenge to IT professionals. How can a district implement a BYOD initiative and still maintain security and control over its computing environment? How can the district's IT department allow personal devices on the network without acquiring additional technical and support resources?

The IT Security Challenge

How do school IT managers take advantage of a BYOD policy without adding complexity and straining support resources? How do districts allow both school-owned and personal device, and ensure that they are used for academic purposes? And how can IT managers allow personal devices access to network resources and protect them at the same time?

Districts need a proven solution that not only automates the authentication, identification and onboarding process for faculty, staff, students and guests, but one that offers context-aware device visibility, security compliance, access control and reporting.

> *It has been a pleasure working with Impulse. They've been supportive every step of the way during our implementation, and even found solutions for us when we encountered road-blocks within our own network infrastructure.*
>
> -Deana Sabala-Aborne
> Bellflower Unified School District

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 Benefits for K12:

- Real-time visibility into all managed and unmanaged devices on the network
- Network access privileges based on a wide variety of contextual intelligence attributes (device type, role, location, time of day, ownership, etc.)
- Automated policy enforcement reduces IT help desk
- Centrally deployed solution scales easily to support the highly distributed environment of school districts
- Vendor agnostic, seamlessly integrates into your existing environment

SafeConnect Solution Offerings

Identify and Authenticate. 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 employees, guests or vendors.

Posture Assessment. 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 adoptionof 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. With this approach, the focus is on blocking unauthorized devices.

- Automate policy enforcement based upon the risk levels reported by threat detection systems such as intrusion detection system (IDS) and Advanced Threat Protection (ATP)
- Publish real-time Contextual Intelligence information to next-generation firewalls, web content & bandwidth managers to enable much more granular policies
- Integrate with SIEM providers which enables much more detailed reporting for enhanced security assessment decisions in a timely manner.

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 and 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 Remote- 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

Impulse | A SafeConnect Network is a Secure Network Impulse is the leading provider of Secure Access for traditional networks as well as remote and cloud access. Impulse securely and efficiently automates this access for organizations of all sizes and needs by combining our simplified access control architecture, remote managed support services, and customer-centric business philosophy to enable customer and IT security freedom. Our customers know this as the Impulse Experience. Visit www.impulse.com