

K-12 Districts Simplify Security with Cloud Managed Network Access Control

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 through a *single-pane-of-glass*.

Identify, Secure, Orchestrate

SafeConnect is an essential network security solution for any school district looking to identify the growing number and type of personally-owned devices on their networks without sacrificing ease of use for their students, staff and guests. SafeConnect is delivered as a Cloud-Managed Service that relieves the district of costly technical support related to deployment, proactive monitoring, maintenance, and upgrades.

SafeConnect automates your device security policies— from assigning network access privileges based on identity/role, device type, location, and ownership to providing network-based enforcement and automated remediation user guidance for non-compliant devices.

SafeConnect Benefits for K-12:

- 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

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.

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

1 http://www.pewinternet.org/2015/04/09/teens-social-media-technology-2015/pi_2015-04-09_teensandtech_06/

4 https://thejournal.com/Articles/2017/06/08/K12-Cyber-Incidents-Have-Been-Increasing-in-2017.aspx?s=the_nu_140617&mkt_tok=eyJpjiTnpNd016WXdPREpsTjJMClslNlQlOjMmNnhkKzBTXC9SvnrkzJlM3hVWUJOYXdlL2w4QlkyNW5kZmRlZDRiZlQ4bHVJZXdNdE5lbn2xNlkaEw4TDdTZE0zME80VmtCbXhiQnFRaWJnT0FNQ2daTGxm0d1NNGp4MnFGN05hYm5GT3VclzJlRWRST1hkQ2hFRWJ1U2JWQ5J9&Page=1



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

Internet of Things and the Need to Secure It

- 73% of American teenagers have access to a smartphone¹



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