safe connect
network access control

Supporting K-12 Education's Bring-Your-Own Device Policy

Security Policy Enforcement for Personally-Owned Devices

Many school systems are now incorporating personally-owned mobile devices such as laptops, iPads, tablets, and smartphones into the learning experience and as a way to address one-to-one computing mandates within tightened budgetary constraints, and enrich collaborative learning.

The Bring-Your-Own-Device (BYOD) trend is gaining momentum nationwide with much support from parents and students. *Project Tomorrow*, a national education nonprofit group, reported that 60-70 percent of parents of K-12 students would be willing to buy a mobile device to support learning. And 56 percent of high school students say that it would make it easier to learn if they were allowed to use their own mobile device at school.

While addressing key trends in education – mobile learning, online and blended learning, and e-textbooks and digital content – BYOD policies also can open the network to security vulnerabilities if not handled correctly. Safe•Connect enables schools to manage their student's personally-owned devices for enhanced learning while maintaining security across the district's wired, wireless, and remote VPN networks.

Simplify BYOD in Your District

Impulse.com

Enhancing Your Learning Environment

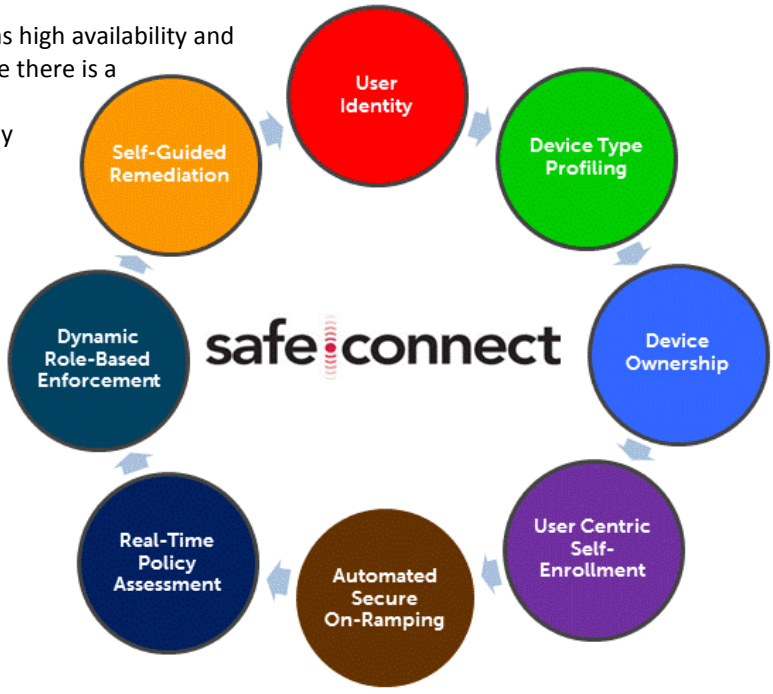
Today's learning environment is well-connected and has high availability and on-demand needs. Web access is pervasive – anywhere there is a signal, youngsters can be found accessing data from their phones and tablets. These mobile devices embody the blending of technologies (applications, tools, readers, etc.) that very easily lend themselves to education and enhanced learning. The more information students can access, the more they can learn.

Continuous Security Assessment & Enforcement

All this access, however, presents the hazard of introducing malware to the network or contact with of unwanted visitors.

Safe•Connect helps ensure that only authorized guests can access the network. The solution also automates the District's endpoint security compliance policies by continuously identifying, assessing, enforcing, and remediating computing devices before and after they gain access to the network.

The solution provides the District much needed visibility into user identities and device types, whether they are managed or unmanaged (i.e., personally-owned).



Safe•Connect automates endpoint security compliance policies by continuously identifying, assessing, enforcing, and remediating computing devices during pre- and post- network access.

Students, faculty and guests are self-guided through enrollment, and if necessary, remediation instructions to conform to district security policies. They receive individualized notifications regarding the necessity for compliance (e.g. out of date AV protection) and are guided through the process with instructions on how the appropriate software or up-do-date virus definition can be downloaded.

Experience

Bay County District Schools,
Panama City, Florida
The District required a solution to integrate with their Lightspeed Internet management, Internet filtering and Web monitoring solutions. The product also needed to scale across multiple sites and be managed from a central location. Safe•Connect is deployed across 32 schools, including more than 28,000 students and employees.

Berkeley County School District,
Moncks Corner, South Carolina
A requirement was the ability to scale across multiple sites without extensive hardware and integration requirements or prohibitive costs. Safe•Connect is deployed from one central management location across 40 schools and 4 district offices, including more than 30,000 students and employees. Berkeley uses Safe•Connect to help prevent non-county assets from accessing the network, stopping the spread of malware.

Charleston County School District,
North Charleston, South Carolina
As with most school districts, Charleston needed a cost-effective way to block devices from accessing network resources – and it needed to be centrally managed, easy to maintain, and be pre-distributed to remote locations. Safe•Connect is deployed across 79 schools, including more than 43,000 students and 5,500 employees.

Dalton Public Schools, Dalton, Georgia
Having a limited budget and IT staff to track down potential threats, DPS required a flexible solution to block certain unknown devices, while also allowing legitimate non-domain devices onto the network in a secure fashion. The solution provides the centralized management, out-of-line network architecture that they were looking for, and integrates with the systems already in place. Safe•Connect is deployed across 8 schools, including more than 7,000 students.

Lexington One School District,
Lexington, South Carolina
To help meet One-to-One Initiatives providing network access to all students, the District was allowing non-district owned devices to access the network, but wanted to be able to manage the security status of individual devices efficiently while protecting the network from malware.

Safe•Connect provides the flexibility to block or provide access to individual, non-district users at their discretion and based on security policies rather than a blanket decision. Safe•Connect is deployed across 26 schools with more than 19,000 students.

About Impulse Point

Impulse Point delivers the industry's most scalable and easiest to deploy and maintain Network Access Control (NAC) solution. Safe•Connect™ is the solution of choice for large, diverse environments – such as Education – where the "Consumerization of IT" is driving the need to provide endpoint security policy enforcement for a myriad of personally-owned, non-managed, mobile computing devices. Deployed and supported as a managed service, Safe•Connect's rapid installation, network independence, and track record of reducing help desk calls results in lower total cost of ownership and reduced risk. Customers currently entrust the security of more than a million endpoints to Impulse Point. Visit www.Impulse.com or www.SimplifyBYOD.com