Solution Brief

safe•connect

Automated Visibility and Control for Higher Education

Gartner, Inc. forecasts that by 2020 there will be more than 20 billion "things" connected to the Internet.[1] Today alone, over 5.5 million new things will connect. And with the early adopter personalities of higher education, a higher percentage of those devices are already on your campus.

Being able to identify, classify and secure these devices without inconveniencing your students and faculty is the foundation of a comprehensive network security strategy. And automating the process to reduce the burden on your IT Help Desk is the most essential component of a well-run network access management system.

The IT Security Challenge

Nearly everyone owns a smart phone, laptop, and/or tablet—which has created the need for security policies and network access controls to support the escalating volume and diversity of personally-owned devices that are accessing sensitive internal applications and data resources. As the Internet of Things (IoT) continues to grow at an exponential rate, so do the risks to your network's security.

An everyday challenge for network administrators in higher education is enforcing security compliance policies and network access privileges while maintaining a positive user experience for ***everyone*** on campus - students, faculty, staff and guests. The larger the student population, the more magnified this challenge becomes, as the need to reduce help desk support calls becomes just as important.

SafeConnect automates device security compliance and network access assignment policies based on identity/role, device type, location, and ownership, and gathers this information in real-time. It is centrally deployed and incredibly scalable, making it the perfect solution for higher education institutions of all sizes.

Featured SafeConnect Customers

- **University of Florida:** *52,286 students*
  92% reduction of security events on unmanaged devices; improved speed and simplicity for 802.1X onboarding
- **University of California at Los Angeles:** *43,301 students*
  93% reduction in help desk calls during move-in; centrally deployed solution across wired and wireless networks
- **Lynchburg College:** *2141 students*
  Single pane of glass to address DCMA violation notifications quickly; self-remediation for students has streamlined trouble ticket resolution procedures
- **Ouachita Baptist University:** *1538 students*
  Automated device self-registration eliminates manual input by IT department; guest self-enrollment provides automatic guest onboarding and management

[1] Gartner, Inc., http://www.gartner.com/newsroom/id/3165317

Experience Service Like Never Before

The *Impulse Experience* is the result of our real-time contextual intelligence, simplified access control architecture, US based remote managed deployment and 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.

In addition to its simplified network access control architecture and enhanced user experience design, a key unique customer benefit is how the SafeConnect solution is delivered and supported as compared with other NAC vendor alternatives.

Installation: The SafeConnect solution is premise based and delivered to the customer commonly as a VMware or Hyper-V virtual appliance, but hardware is also available for an additional cost. A single SafeConnect instance supports up to 30,000 concurrent endpoints but the system can be scaled with additional nodes to over 150,000 concurrent endpoints.

Integration: The installation of SafeConnect requires minimal technical resources. In short, the system simply needs to be downloaded and deployed within your VMware or Hyper-V environment, or the hardware needs to be installed in a rack and powered on. Once that is completed, an Impulse Engineer will work remotely with the customer through our 5-step implementation process. This includes integrating with your network infrastructure, establishing communications with your directory services with self- service scripts and guides, and any other security integrations for Contextual Intelligence like a SIEM or NGFW.

Implementation: An Impulse Engineer will work with you remotely on policy creation and implementation. You will be guided through the deployment process with recommendations and direction. This includes branding, hands-on and video training, and best practices so that you will have a fully functional solution including a communication plan to your users.

Support: SafeConnect is supported by the industry's only comprehensive managed support services offering. Impulse will provide continuous, around-the-clock (24x7x365) proactive monitoring and support. The Impulse Support team owns the responsibility of determining the problem including owning any updates, configuration changes or actions required for resolution. Impulse will also provide consultative "how to" support services.

Update: Daily system updates for device profiles and OS/AV fingerprints, as well as policy configuration backups are included. In a world where users change and update their devices on a frequent basis, it is imperative that the security solution keeps ahead of these changes. When new versions are available, or maintenance updates are required, Impulse will proactively notify you and will perform the update, for as long as you remain under an annual maintenance agreement.

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