

## BENEFITS

- Reduces IT security risks by ensuring adherence to endpoint security policies
- Prevents unauthorized user network access
- Limits exposure and risks associated with P2P file sharing
- Isolates non-compliant users using I-LAN quarantine technology and offers individualized remediation guidance
- Reduces personnel costs associated with registering and securing student-owned and guest computing devices
- Complements security awareness campaigns by educating users on security best practices

[www.impulse.com](http://www.impulse.com)



# Safe•Connect

## NETWORK ACCESS CONTROL

### HIGHER EDUCATION SECURITY CHALLENGES

Educational institutions face a multitude of escalating challenges to secure and maintain their critical information technology assets while continuing to support the open computing philosophies that are the hallmark of higher education.

Higher education requires a sophisticated, yet flexible, approach to address the unique and evolving concerns posed by a highly mobile computing population. Because of the escalating number of unknown, personally-managed devices on college campuses, it is especially important to be able to enforce and remediate endpoint security policies at the point of network entry using Network Access Control (NAC) technology.

### THE SOLUTION

The Impulse Safe•Connect™ system provides an open network access control (OpenNAC™) solution that easily integrates into vendor-diverse network environments. The inherent scalability advantages of Safe•Connect's distributed software architecture and managed support approach enables institutions to address their NAC enterprise requirements in a cost-effective manner.

Originally designed for the Higher Education Industry, Safe•Connect delivers an OpenNAC enterprise solution that enables institutions to automate the enforcement and remediation of endpoint security acceptable use standards. Safe•Connect offers an easy to implement and support endpoint policy management alternative that seamlessly connects into an institution's existing multi-vendor infrastructure, and provides an evolutionary path to maturing NAC industry standards like IEEE 802.1x.

By focusing on endpoint policy management, Safe•Connect provides the following capabilities:

- Prevents unauthorized user access to wired, wireless, and VPN networks.
- Ensures users maintain compliance with anti-virus, anti-spyware, Microsoft security patches, P2P file sharing software, and custom endpoint security policies.
- Automates the isolation of non-compliant devices at Layer 2 using I-LAN quarantine technology and provides individualized remediation guidance.
- Flexible role-based policy management for students, faculty, staff, and guests.

### POLICY MODULE KEY FEATURES

#### Authentication and Guest Registration

Prevents unauthorized user access to core network resources and Internet services. Automates the registration of end user computing devices and audits agreement to acceptable use policies. Role-based policy management integrates with enterprise AD, LDAP, IAS, or RADIUS directory services.

#### Anti-Virus

Manages compliance with anti-virus software and definitions.

#### Anti-Spyware

Manages compliance with anti-spyware software and updates.

#### Microsoft OS Patch

Ensures that users are at desired security patch maintenance levels.

#### P2P File Sharing

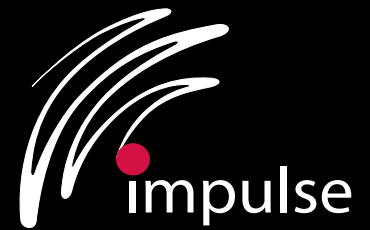
Prohibits the use of P2P file sharing and helps educate students on security best practices.

#### Access Point

Manages adherence to rogue access point devices that utilize Network Access Translation (NAT).

#### Custom Policy Builder

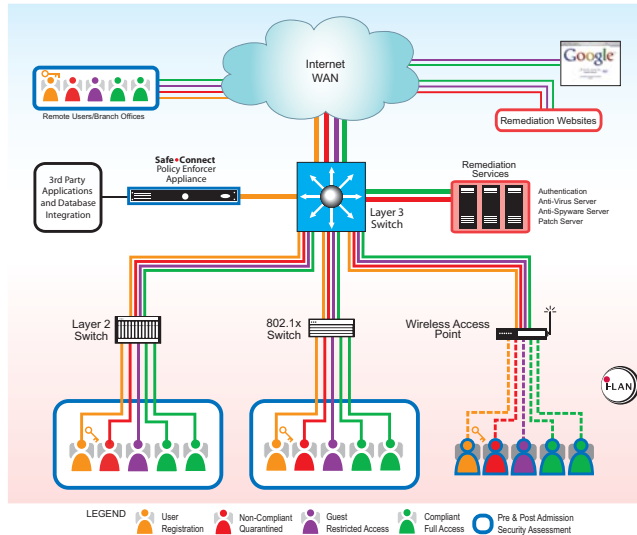
Enables institution to build custom policies and messaging to address their unique endpoint security standards and enforcement rules.



## HOW DOES IT WORK?

1. The Safe•Connect Policy Enforcer Appliance is installed on the institution's premises and is connected "out of line" to an existing customer router.
2. The organization configures their desired policies and enforcement rules using the Safe•Connect Policy Management Console by network segment or directory services group.
3. Endpoint devices connecting to the institution network will be intercepted, authenticated, presented with the organization's acceptable use policies, and issued a Safe•Connect Policy Key.
4. The Safe•Connect Policy Key certifies that the endpoint device adheres to endpoint security policies on a continuous/real-time basis. It reports non-compliance to the Safe•Connect Policy Enforcer and delivers individualized remediation guidance. The endpoint devices can remain completely isolated using I-LAN quarantine technology until the policy breach is resolved.
5. Safe•Connect offers consistent endpoint device support for wired, wireless, and VPN networks.

## Safe•Connect Solution Overview



## WHY SAFE•CONNECT?

- Scalable, distributed architectural design
- Non-intrusive IT infrastructure implementation approach
- Out-of-line network integration design
- I-LAN Layer 2 quarantine technology is independent of switch hardware
- No single-point-of failure or performance bottleneck
- Turnkey implementation and training services
- 24/7 managed support and service

## POLICY MANAGEMENT CONSOLE

Institutions can define and change endpoint computing policies and enforcement rules by network segment or directory services policy group from a centralized policy management portal interface. The Safe•Connect Policy Management Console also displays real-time status reporting that provides valuable insight into group or individual policy compliance.

## QUARANTINE TECHNOLOGY



Impulse Point's I-LAN quarantine technology isolates non-compliant endpoint devices from accessing Layer 2 and Layer 3 network resources. I-LAN also limits end user access to designated internal or Internet remediation domains, where it communicates the actions required to become compliant with an institution's endpoint security policies and regain network access privileges.

## 24/7 SOLUTION SUPPORT

Safe•Connect is delivered as an operationally managed service. The health of the system is monitored from the Impulse Support Center on a 24/7 basis. Impulse Point is responsible for delivering all necessary hardware and software maintenance, problem determination/resolution, and ongoing feature enhancements, while the institution maintains full control of managing their desired end user computing policies and enforcement rules via the Impulse Policy Management Console.

## ABOUT IMPULSE POINT

Originally designed for higher education's highly scalable and vendor-diverse environment, Impulse Point's Safe•Connect™ Open Network Access Control (OpenNAC™) solution enables organizations to automate and enforce end user authentication, anti-virus, anti-spyware, Microsoft security patches, P2P file sharing, and custom endpoint security policies. The result is a more secure, reliable, and predictable IT network infrastructure. Impulse Point ([www.impulse.com](http://www.impulse.com)) is headquartered in Lakeland, Florida and is one of Tampa Bay's premier technology innovators.

For more information or to arrange a demonstration, please contact us:

[Info@Impulse.com](mailto:Info@Impulse.com) or  
[WebDemo@Impulse.com](http://WebDemo@Impulse.com)