

### BENEFITS

- Reduces enterprise 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
- Automates the process of registering and securing unknown guest computing devices
- Educates employees and guest users regarding acceptable use security policies

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



# Safe•Connect

## NETWORK ACCESS CONTROL

### ENTERPRISE SECURITY CHALLENGES

Enterprises have traditionally focused on network security at their perimeter to prevent potential threats from outside intrusions. While this remains a valid and essential approach, security professionals realize that the majority of threats originate from *within* their networks. In today's highly mobile and pervasive computing environment, it is increasingly likely that endpoint devices will introduce viruses, worms, or malicious threats that are capable of causing significant harm to business critical networks and systems—especially those originating from unknown sources such as guest devices.

The ability to enforce and remediate endpoint security policies at the point of network entry using Network Access Control (NAC) technology has become an essential component in addressing enterprise security concerns and regulatory compliance requirements.

### 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 organizations to address their NAC enterprise requirements in a cost-effective manner.

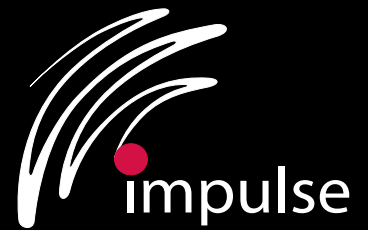
Safe•Connect delivers an OpenNAC enterprise solution that enables organizations to automate the enforcement and remediation of endpoint security acceptable use standards. Safe•Connect offers an easy to implement and support endpoint policy management alternative that seamlessly connects into an organization's 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 employees, consultants, and guests.

### POLICY MODULE KEY FEATURES

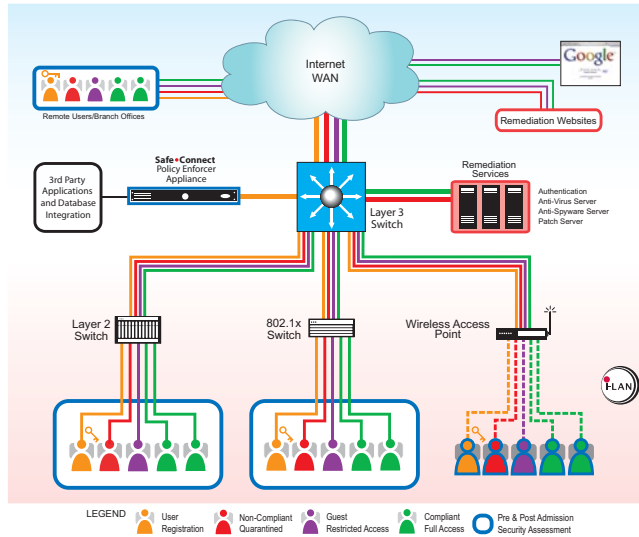
<b>Authentication and Guest Registration</b>	Prevents unauthorized user access to core network resources and Internet services. Automates the registration of end user computing devices and audits agreement to acceptable use policies. Role-based policy management integrates with enterprise AD, LDAP, IAS, or RADIUS directory services.
<b>Anti-Virus</b>	Manages compliance with anti-virus software and definitions.
<b>Anti-Spyware</b>	Manages compliance with anti-spyware software and updates.
<b>Microsoft OS Patch</b>	Ensures that users are at desired security patch maintenance levels.
<b>P2P File Sharing</b>	Prohibits the use of P2P file sharing and helps educate users on security best practices.
<b>Access Point</b>	Manages adherence to rogue access point devices that utilize Network Access Translation (NAT).
<b>Custom Policy Builder</b>	Enables organization 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 organization'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 organization 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 T 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

Organizations 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 organization'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 organization maintains full control of managing their desired end user computing policies and enforcement rules via the Impulse Policy Management Console.

## ABOUT IMPULSE POINT

Designed for highly scalable and vendor-diverse environments, 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.

Impulse Point • 6810 New Tampa Highway • Lakeland, Florida 33815 • 863.802.3738 • [www.impulse.com](http://www.impulse.com)

For more information or to arrange a demonstration, please contact us:  
[Info@Impulse.com](mailto:Info@Impulse.com) or  
[WebDemo@Impulse.com](mailto:WebDemo@Impulse.com)