The Trust You Need in a BYOD World

Contextual Intelligence™ and Network Access Management

The explosion of mobile devices, coupled with advances in wireless technologies and readily available mobile apps has driven the adoption of Bring Your Own Device (BYOD). Today, nearly everyone owns a smartphone, 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 mobile devices accessing sensitive internal applications and data resources.

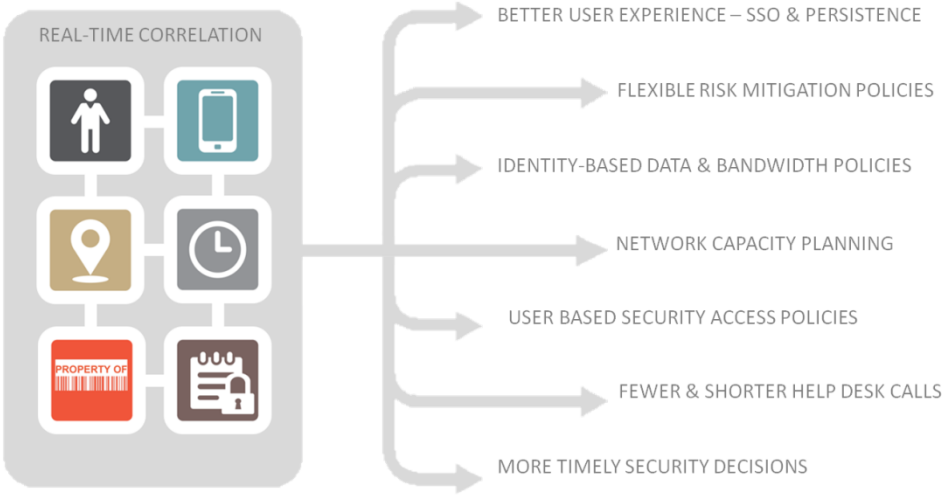
An everyday challenge for IT managers is enforcing security compliance policies and network access privileges while maintaining a positive user experience and reducing help desk support calls.

Organizations are also faced with the daunting task of correlating mobile device information and user identity (over time and across their networks) for regulatory compliance; security forensics; and enabling identity-based firewall, web content and bandwidth management policies.

SafeConnect provides the ability to automate the enforcement of security compliance and network access control policies (based on identity, device type, location, and ownership), and gathers a wealth of real-time and historical context-aware device data so you can make more informed and intelligent decisions.

Contextual Intelligence™

Impulse's Contextual Intelligence™ technology delivers real-time device information that correlates identity/role, device type, and location (along with other attributes such as ownership and compliance status) over time to power its SafeConnect solution.



Information gleaned "in context" regarding mobile devices on the network (both real time and historically) allow IT managers to make better decisions on network capacity, risk mitigation, and forensic analysis required for addressing compliance. The ability to leverage real-time contextual data for identity persistence also reduces the number and length of help desk calls by improving the end user experience.

SafeConnect

SafeConnect delivers a range of capabilities that provides a comprehensive enterprise- wide management solution to address the flexibility and security needed to support today's mobile device environments.

Identity Access Control recognizes when devices attempt access to wired, wireless, or VPN networks and provides agentless device profiling, user authentication, non-browser device registration, self-provisioning guest access management and real-time contextual intelligence reporting. This is an ideal solution for customers seeking to replace "home-grown" device registration systems (i.e. NetReg), as well as for those organizations that desire context-aware network access control assignment and visibility for mobile devices based on identity/role, device type profiling, location, IP-MAC Address, and ownership/liability.

Identity Access Control (IAC) includes an easy-to-configure, standards-based RADIUS server that integrates with an organization's AD-LDAP directory services infrastrucsture to deliver 802.1X authentication services that support both Open and Secure WPA2 Enterprise wireless networks, as well as 802.1X based wired and VPN environments. IAC can optionally integrate with an organization's existing RADIUS server platform.

Secure BYOD On-Boarding solves a complicated problem for end users by automating the process required to provision devices onto secure 802.1X-WPA2 Enterprise wired and wireless network environments. By eliminating end user manual configuration, the solution delivers a reduction in help desk support calls and dramatically accelerates user adoption of secure wireless. When combined with Identity Access Control this feature enables you to welcome every new user with a captive web portal that authenticates the end user, configures the device's embedded 802.1X supplicant, and automatically assigns (moves) the device to a designated secure SSID network segment. Users are automatically associated with their secure wireless network on subsequent network connections without the need for repeated logins.

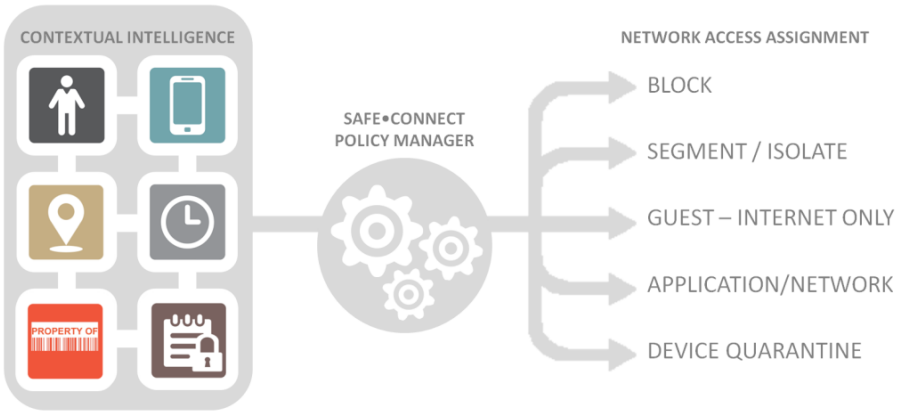
Device Security enhances the security posture of your network by providing real-time policy assessment, enforcement, and self-remediation for Windows and MAC OS X devices. A user's system is checked prior to granting network access to ensure that the device adheres to the organization's acceptable use policies (anti-virus, operating patches, personal firewalls, P2P, etc.) as well as on a continuous basis after access is granted. Web-based self-remediation guidance enables users to conform to security policies without help desk support involvement.

Mobile Device Management delivers integrated premise- or cloud-based MDM solution offerings to provide a comprehensive policy enforcement framework for mobile devices that enable the following benefits:

- Automate MDM provisioning by detecting, blocking and redirecting all unknown mobile devices to the MDM registration portal to ensure compliance
- Apply network-level quarantine to all mobile devices that are either not registered or are non-compliant with MDM policies as well as provide web-based self-remediation guidance
- Assign application and network access privileges based on identity/role (i.e., employee, faculty, staff, guest, vendor, etc.), device type, location, ownership and policy status.

RADIUS Based Enforcement

RADIUS Based Enforcement (RBE) delivers dramatic scalability and granular network access control for Secure 802.1X -WPA2 Enterprise and Open wireless networks based on contextual intelligence driven policies.

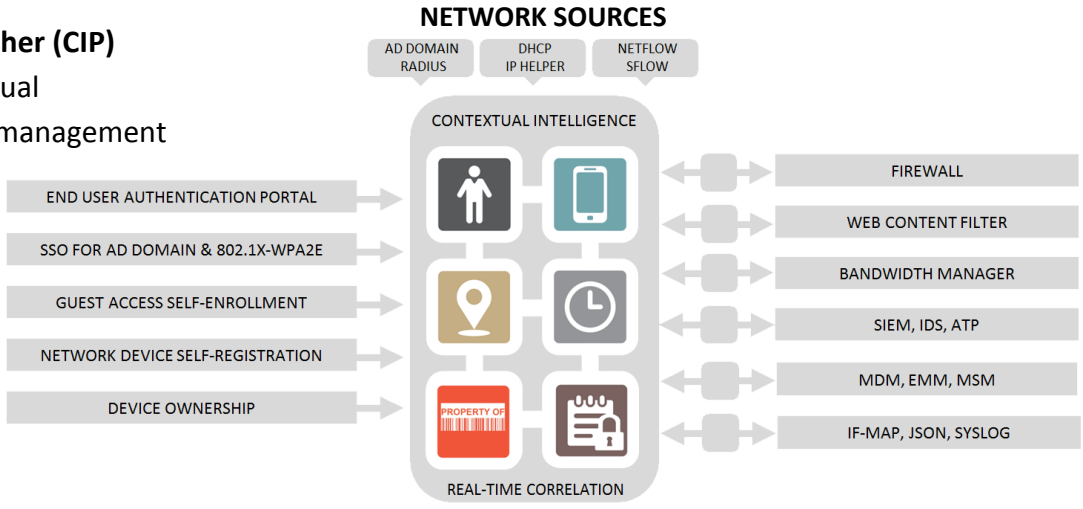


A key benefit of Impulse's RBE is its non-reliance on VLAN Steering. RBE assigns network access privileges to a specific device versus moving a device to a shared VLAN. RBE's non-VLAN approach for wireless environments offers the following benefits:

- Easier to design, deploy, and support – Fewer technical resources required
- Real-time post-admission network access assignment – No need to remove or re-authenticate a device to conduct a security posture check or change network access status
- A better end user experience – No IP address/VLAN changes
- Higher level of device quarantine/segmentation – Devices are restricted/isolated directly, not placed into a shared/dirty/common VLAN

Contextual Intelligence Publisher (CIP)

CIP provides real-time contextual intelligence to other network management and security systems that enable single-sign-on, one-time user authentication, granular policy assignment, and enhanced analytics to provide more informed and timely security decisions.



24 x 7 x 365 Maintenance and Managed Support Services

All Impulse products come with an industry exclusive and comprehensive hardware and software maintenance program. This includes 24x7 system monitoring; problem determination and resolution technical support; daily remote backups, device type profiling, operating systems, and remediation software updates; overnight hardware replacement; and no-charge software version and hardware upgrades.

SafeConnect BYOD Security Management	
Identity Access Control	
RADIUS Authentication Server	Provides RADIUS to AD/LDAP Authentication Services in support of Open and Secure 802.1X-WPA2 Enterprise wireless networks, as well as 802.1X based wired and VPN environments.
User Identity Authentication	Prevents unauthorized users from accessing network resources and participates in 802.1X-RADIUS and AD Domain Single Sign-On (SSO).
Agentless Device Profiling	Provides visibility into device types and ownership (whether a device is company-owned and liable or personally-owned - i.e. BYOD).
Guest User Self-Enrollment	Automates the process of provisioning Internet-only network access for guests without help desk involvement.
Network Device Registration	Allows end users to self-enroll non-browser devices such as printers, e-readers, media, or gaming systems using their identity credentials.
Real-Time & Historical Reporting	Provides real-time reporting views and historical policy event data that depict authentication, compliance, and remediation status.
Contextual Intelligence Publishing (CIP)	Delivers real-time correlated user identity/role, device type, ownership, and compliance information to third-party firewalls, web content filters, SIEMs, and bandwidth managers that allows for more granular identity-based policies for BYOD mobile devices and enhances the user experience via authentication persistence.
Secure BYOD On-Boarding	
WPA2 Enterprise / Auto-Provisioning	Automates the user experience of "on-boarding" devices onto WPA2 Enterprise/802.1X secure wireless and wired networks.
Device Security	
Acceptable Use Policy Enforcement	Flexible real-time AUP enforcement for devices including audit-only, periodic grace-period, warnings and network quarantine.
Real-Time Security Compliance	Manages compliance with Anti-Virus, Anti-Malware, OS Patch and Personal Firewall policies for Windows and MAC OS X devices.
Application Usage Policies	Prohibits the use of peer-to-peer (P2P) file sharing and other non-approved applications and addresses DMCA compliance.
Custom Policy Builder	Enables customers to easily build policies based on the existence or non-existence of file types, services, processes, or registry settings.
Mobile Device Management	
MDM On-Ramping & Policy Enforcement	Ensures that end users install the organization's preferred MDM Solution on their mobile devices and adhere to policy.

impulse

Experience the Freedom

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 one thing, it's everything. Visit impulse.com