

Security & Defense Solutions

Intelligent Convergence with EdgeFrontier®

Contents

1. Introduction	2
2. The Need for Intelligent Convergence.....	3
2.1 Security Convergence with EdgeFrontier	3
2.2 EdgeFrontier in Action	4
2.3 Technical Requirements.....	5
3. Solutions for Defense, Borders, & Ports.....	6
4. Solutions for Public Safety & Security	8

1. Introduction

The distributed and evolving nature of threats has limited the utility of single, standalone systems as the sole method for monitoring facilities, personnel, and situations. More comprehensive protection requires a variety of sensors and devices, including cameras, access control systems, motion detection devices, chemical and biological threat detection sensors, biometrics, and other systems. Moreover, these security and defense systems should link to information technology (IT) systems, visualization systems, geographic information systems (GIS), notification systems, and intelligent analytics to provide holistic security.

2. The Need for Intelligent Convergence

The trend toward diverse device and system deployments has led to the need for convergence of data from these assets in order to maximize the opportunities for real-time monitoring and response. Yet, convergence can be a stumbling block for many organizations as they struggle to overcome the challenges of system integration, data management, and policy management.

A single platform for data integration and policy management – middleware that sits between the various systems – can enable efficient and effective solutions for security and defense. With features that include integration, protocol/format encoding and decoding, notification management, complex event processing, and policy management, EdgeFrontier provides such a platform, overcoming integration hurdles and powering the convergence of diverse security assets for enhanced situational awareness and response.

2.1 Security Convergence with EdgeFrontier

EdgeFrontier is remotely configurable middleware that resides on servers and other computing systems, providing a platform for security and defense solutions. EdgeFrontier supports integration and normalization of data, events, and control functions from diverse devices, systems, and networks, regardless of manufacturer or communications protocol. These include sensors, wireless sensor networks, RFID systems, video devices and systems, access control systems, metering and measurement devices, actuators, databases and file repositories, and other assets. In addition, rules and policies can be configured through EdgeFrontier, enabling notifications, alerts, complex event processing, and automated control. See Figure 1 for an illustration of these capabilities.

For security and defense solutions, EdgeFrontier is commonly used to support integration and normalization of data, events, and control functions between devices, systems, and applications where no pre-existing interfaces exist. EdgeFrontier is also used to support centralized or remote event or policy-based processing that pushes intelligence and logic beyond the data center and throughout the network infrastructure on a distributed basis.

This flexibility is important for customized security and defense solutions. Different security organizations may have different requirements based upon specific security practices, assets, personnel, or other considerations. Moreover, within these organizations, there are often layers of customized policies based upon the needs of specific facilities and personnel.

Security and defense solutions built upon EdgeFrontier facilitate the intelligent capture and correlation of events, as well as the rapid creation of robust, customized policies based upon those events, which are specific to the security assets and requirements of the organization or facility. With user-friendly graphical components and methods that easily can be configured and related, EdgeFrontier provides the versatility to automate the many in-house procedures required by security and defense organizations, whatever the specific need or circumstance.

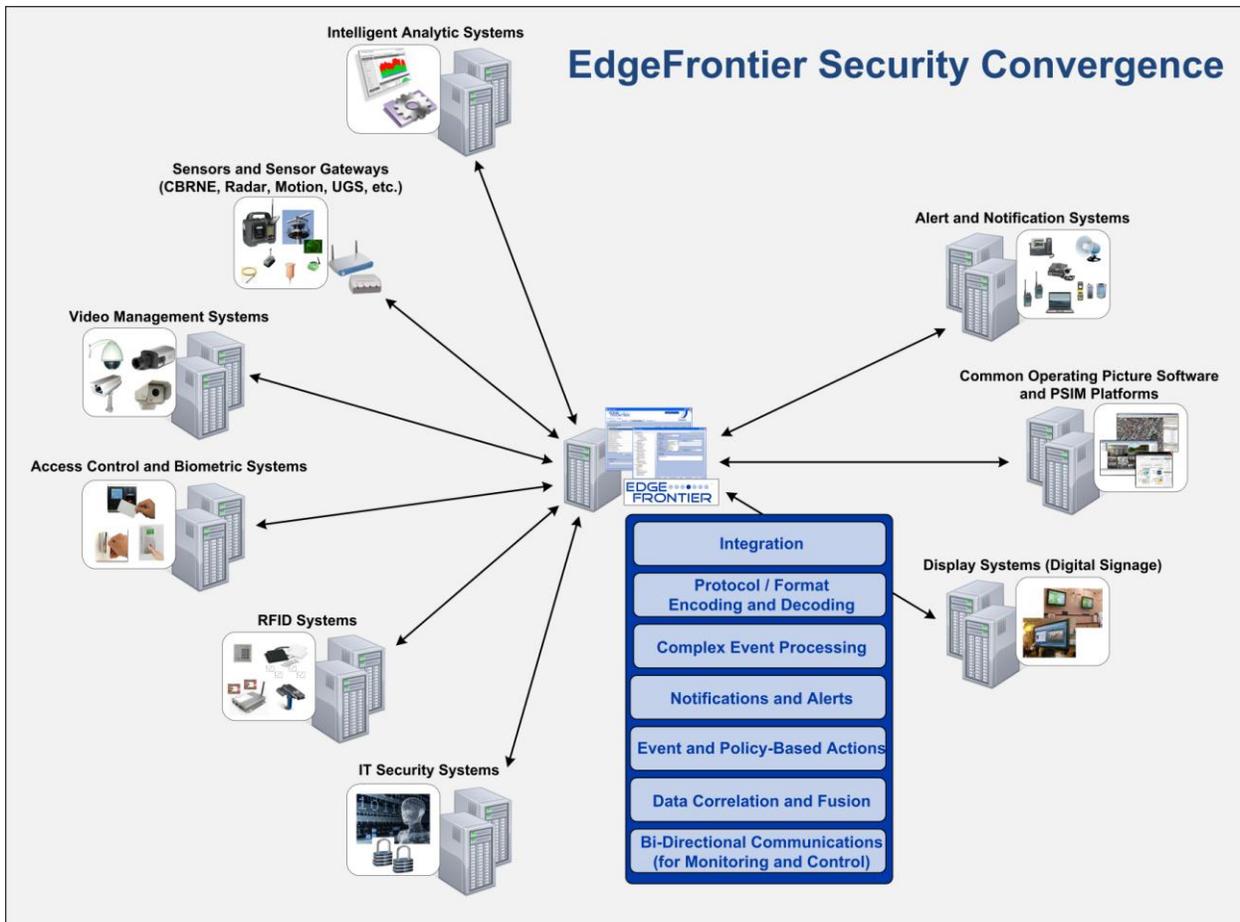


Figure 1: EdgeFrontier Convergence

2.2 EdgeFrontier in Action

As an example, a security policy built within EdgeFrontier may consist of monitoring events from an access control system. The policy could be configured so that three consecutive unauthorized badge read attempts would trigger the following actions:

- Slew a camera to the badge reader area through communication with a video management system
- Start a video archive for the camera within the video management system
- Instruct the video management system to change to a full-screen display of the camera feed
- Retrieve a camera image from the video management system
- Retrieve an image matching the employee badge number from the client employee directory
- Stitch the two images together, convert them to an appropriate file type, and then display the image upon the IP phone at the front desk
- Play an audible alert on the phone and display soft key options to 'Grant Access,' 'Deny Access,' or 'Alert Security'

The soft key options would then have their own sets of policy-based actions. Pressing the 'Grant Access' soft key would:

- Raise a video management system event that access was granted by the front desk
- Stop the video archiving within the video management system
- Announce over an IP speaker that access is granted by the front desk
- Instruct the access control system to unlock the door for ten seconds, then re-secure the door

Pressing the 'Deny Access' soft key would:

- Raise a video management system event that access was denied by the front desk
- Announce over an IP speaker that access is denied
- After one minute, stop the video archiving within the video management system

Pressing the 'Alert Security' soft key would:

- Invoke an emergency notification system phone call to the security center notifying personnel of the event with a request for acknowledgment
- Enable power to a warning light in the security center
- Instruct a digital media manager platform to display a map of the location of the event on digital signage
- Email images from the client directory and camera feed to handheld devices and mobile phones of security personnel
- Start video archives within the video management system for other camera feeds within the area

Policies such as these could be dynamically configured and continually extended and enhanced as organization or facility security systems or requirements are changed. See the following pages for further examples of how organizations may utilize EdgeFrontier for security and defense solutions.

2.3 Technical Requirements

EdgeFrontier includes an EdgeFrontier Engine™ application, which provides the field-level power for the software, and an EdgeFrontier Client™ application, which enables enterprises and integrators to configure the EdgeFrontier Engine application remotely. With the installation of EdgeFrontier Engine on servers or other computing platforms, and EdgeFrontier Client on remote workstations and PCs, users are provided with a complete, remotely configurable middleware platform for intelligent convergence solutions.

EdgeFrontier Engine can be implemented on network devices, including servers and other computing systems, which are capable of supporting the Microsoft® .NET Framework (versions 3.5 and higher) or the Mono framework. The software acts as an edge application server and can be configured as an edge enterprise service bus, providing an abstraction layer to support processing and distribution of data, events, and control commands without writing code.

3. Solutions for Defense, Borders, & Ports



Since military and border and port security deployments differ based on the missions and mandates of different government agencies, opportunities abound for diverse and dynamic security and defense solutions via EdgeFrontier. For example, a security solution built upon EdgeFrontier could be configured to monitor and filter alerts and events from ground-based radar systems and unattended ground sensor (UGS) systems, send triggers to video surveillance assets to provide video captures and streams into the network infrastructure, distribute notifications to emergency response communications systems, and provide alerts to common operating picture software, physical security information management (PSIM) visualization systems, and other enterprise applications.

Under such a scenario, EdgeFrontier could be configured to support system-wide and localized event linking. System-wide events could be managed by policy-based components that perform advanced logical

evaluations to determine if a linked action should occur. Logical operations and comparisons could be performed on any number of devices, states, and schedules. These capabilities would allow the user to define event links based on complex conditions, including requirements for both radar and UGS system events prior to the posting of alerts.

The resulting impact of this intelligent convergence solution is dramatic, enabling the automation of security activities based upon organizational policies. For example, under this scenario, if radar or UGS systems were to sense activity, the solution could be configured to:

- Coordinate and filter event information to minimize false positives
- Automatically trigger and control PTZ cameras to allow for coordinated events and imagery displays
- Automatically display event and alert information to command and control personnel
- Provide notifications of events and video captures via text, email, or IP phone notifications to mobile and field personnel

Notably, these applications are not limited to single deployments, but can be linked for comprehensive security and defense solutions, as depicted in Figure 2. These are only two examples of the possibilities for defense and port and border solutions built with EdgeFrontier.



EdgeFrontier Border and Port Security Example

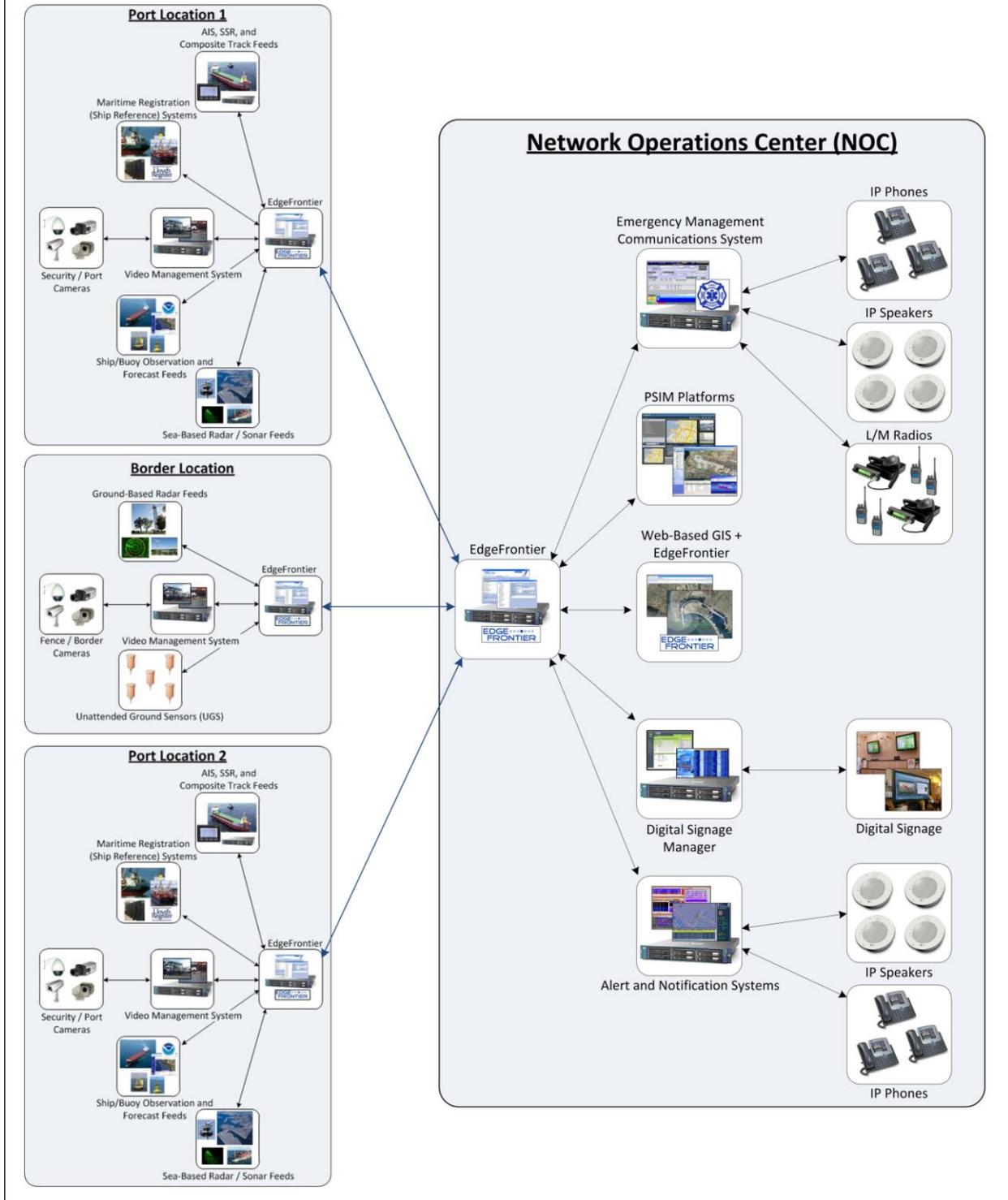


Figure 2: EdgeFrontier for Border and Port Security

4. Solutions for Public Safety & Security

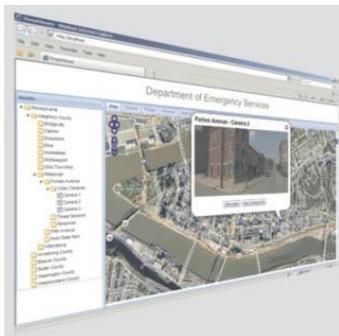


Public safety and security solutions will also differ based on the missions and mandates of particular government agencies. As with defense solutions, many opportunities exist for dynamic public safety and security solutions built upon EdgeFrontier.

Leveraging new and legacy security assets, for example, a public safety and security solution built upon EdgeFrontier could be configured to monitor and filter alerts and events from motion detection systems or access control systems, send triggers to video surveillance assets to provide video captures and streams into the network infrastructure, distribute notifications to emergency response communications systems, and provide alerts to PSIM systems, geospatial management systems, and other enterprise applications.

EdgeFrontier could be configured to define policies based on complex conditions, thus automating public safety and security activities based upon unique organizational needs. For instance, in an emergency management deployment built upon EdgeFrontier, which could tie together a variety of surveillance, facility, and notification systems, a centralized weather agency's RSS feeds could signal a potentially harmful weather event. This would in turn trigger the EdgeFrontier-built system to:

- Automatically display information on the weather alert to users
- Assess and display power outages for government and private facilities
- Automatically display video and provide control of PTZ cameras
- Enable text-based dissemination of weather alerts and power system information through emergency management systems
- Provide notifications of events with video captures via text, email, or IP phone systems to emergency management, command center, mobile, and field personnel
- Display evacuation plans on digital signage



Other scenarios could include the use of gunshot location detection systems or CBRNE sensors as triggers for alerts, notifications, and actions and the integration of additional federal, state, municipal, or private video systems; unified communications systems; and emergency management interoperability/notification systems. All told, the possibilities for custom public safety and security solutions built upon EdgeFrontier are vast.

Intergraph is a wholly owned subsidiary of Hexagon AB (Nordic exchange: HEXA B) and (Swiss exchange: HEXN). For more information, visit www.intergraph.com and www.hexagon.se

Intergraph and the Intergraph logo are registered trademarks of Intergraph Corporation or its subsidiaries in the United States and in other countries. Microsoft is a registered trademark of Microsoft Corporation. Other brands and product names are trademarks of their respective owners. ©2011 Intergraph Corporation. All Rights Reserved. 10/11 SGI-US-0043A-ENG