

*VIGILENT*TM

Critical Incident Management

Compressus Inc.
101 Constitution Avenue, N.W., Suite 800
Washington, DC 20001
tel : +1 202.742.4307
fax : +1 202.742.4286
www.compressus.com

Table of Contents

- Executive Summary 4**
- Overview 6**
 - CommandSight™ 7
 - MedSight™ 8
 - Critical Care Tracking 8
 - Bed Counts 9
 - Staff Tracking..... 9
 - Other Resource Tracking..... 9
 - Hospital Bypass..... 9
 - Ambulance Bypass 10
 - Equipment Tracking 10
 - Initiation of Care Patient ID Tracking..... 10
 - Notification..... 10
- Technical Framework..... 12**
 - Healthcare IT Standards 12
 - Communications Architecture..... 12
 - Interoperability Standards 13
 - Authentication and Authorization 13
 - Messaging..... 14
- About Compressus 16**
 - Company Overview..... 16
 - Products 16
 - Management 17

Executive Summary

EXECUTIVE SUMMARY

VIGILENT™ provides comprehensive access to critical, real-time information to support the identification of community health problems and facilitate rapid, effective response.

VIGILENT™ is designed to be interoperable with and shared by multiple users, leveraging secure connections to a wide assortment of health information systems and devices to create a wide variety of surveillance and response capacities.

The VIGILENT™ suite is comprised of browser-based, state-of-the-art applications and scalable platform technologies. Compressus brings years of experience, building upon accepted industry standards, creating an open architecture and end-to-end scalability so that VIGILENT™ technology will interoperate with all existing and emerging applications and information systems. For example, XML and HL7 interfaces to existing medical information systems are used to interoperate with a wide range of data sources.

The VIGILENT™ architecture has been developed over the last 11 years with input and guidance from the Centers for Disease Control (CDC) Bioterrorism Planning and Emergency Response Team, various state and local public health officials, the Defense Advanced Research and Projects Agency (DARPA), and the United States Air Force.

The VIGILENT™ application modules can be deployed independently or in combination to provide First Responders and health and public safety officials with the flexibility to react to a wide range of emergencies. Since VIGILENT™ is used 24/7 and not deployed just during a crisis situation, it also supports rapid and effective response to any large-scale natural disease outbreak, disaster, or terrorist event.

The VIGILENT™ modules include:

- **CommandSight™** is an interactive incident management tool designed to provide emergency responders and other local, state, and federal officials with a common operational picture, facilitating an effective response to an outbreak or emergency incident.
- **MedSight™** provides ongoing surveillance to identify an epidemiological and/or hazmat event early in the outbreak cycle. Rapid identification of the threat and effective ongoing communications among the Public Health, Medical and First Responder communities are essential to minimizing loss of life.
- **Critical Care Tracking (CCT)** provides shared information to facilitate ambulance diversion and medical resource management, whether the challenge is responding to an emergency or handling the everyday stresses of emergency medicine. CCT also monitors the status of various medical resources in case a response plan needs to be developed quickly.
- **Notification** provides rules-based exchange of information to all relevant agencies via existing communications networks.

Overview

OVERVIEW

Naturally occurring disease outbreaks and health problems such as West Nile virus, influenza, and SARS are significant, long-standing concerns of health officials. Detecting, identifying, and mitigating such outbreaks are among their primary responsibilities.

In the aftermath of September 11th and the anthrax attacks of 2001, bioterrorism surveillance became another prominent responsibility.

In October and November of 2001, the anthrax attacks sent 11 patients to the hospital with anthrax infections. Five of these patients died, and six lived. The average time from symptom onset to treatment for those that lived was 4.7 days. For those that died, the interval was 5.8 days. In other words, life or death was largely determined by reducing identification and response time by just 24 hours.



The VIGILENT™ system is comprised of modules that can be deployed independently or in combination to provide any of the following capabilities:

- Incident-management command-and-control tools enabling a wide range of organizations to communicate efficiently, supporting a rapid and coordinated response;
- Assurance that the tools and pertinent data are securely available in real time to the appropriate personnel;

<p>MedSight™</p> <ul style="list-style-type: none"> • Event Based Syndromics • Continuous Data Ingest • Facility Census • Reports • Mapping 	<p>CommandSight™</p> <ul style="list-style-type: none"> • Common Operating View • Plan Manager • Checklist Manager • Statewide Notification • Reports • Causality Tracking 	<p>Critical Care Tracking</p> <ul style="list-style-type: none"> • Facility Status • Ambulance Diversion • Reports • Resource Tracking • Mapping
<p>Notification</p> <ul style="list-style-type: none"> • Paging • Voice to Text • Wireless • SMTP • LDAP • Alerts 		
<p>Administration Module</p> <ul style="list-style-type: none"> • Module Setup • Reporting • Reference Code Maintenance • User Admin • Organization Admin • Group/Role Admin 		
<p>Platform Services</p> <ul style="list-style-type: none"> • HTTP/S Server • J2EE Application Server • Portal Framework • NEDSS Integration 		
<p>Integrated Data Repository</p> <ul style="list-style-type: none"> • SQL RDBMS • OLTP & OLAP • Redundancy • Local to National View • Civilian & Military Support • Affiliate Integration 		

Modules and capabilities of the VIGILENT™ system.

- Large-scale data collection from the Public Health Information Network (PHIN) and/or any other national standards-based data sources;
- Analysis tools to identify disease outbreaks and covert attacks;
- Visualization tools such as GIS maps to graphically represent information and the location of incidents, secondary assessment centers, hospitals, and treatment centers; and
- Portable bio-agent identification devices that can identify bio-agents and diseases in the field within minutes.

The forerunner of Compressus' VIGILENT™ product line was the LEADERS system, developed beginning in 1993 by a consortium that included Oracle and Ernst & Young Technologies, along with support from the United States Air Force Surgeon General's Office, Defense Advanced Research Projects Agency (DARPA), and the Centers for Disease Control (CDC). Compressus' former Executive Vice President, Dr. Klaus Schafer (Brigadier General, USAF, Retired), spearheaded this development in response to the need for a uniform system to effectively detect, track, and respond to biological attacks, widespread outbreaks of disease, and natural or man-made disasters.

CommandSight™

CommandSight™ provides on-site responders and remotely located command personnel with the ability to quickly and easily:

- Display resource/responder locations within the context of a geo-referenced map;
- Track and monitor response activities in real time;
- Visually define areas of interest such as perimeter locations, hot zones, staging, etc;
- Share a common operational picture with remotely located personnel and/or supporting organizations and agencies;
- Automatically collect and store time-stamped incident information for playback and after action review; and
- Visually playback the sequence of response activities in order to facilitate investigation and training, including time sequenced events.

Simple drag-and-drop functionality allows users to place customized icons onto the map display and move them to new locations as an incident unfolds. Each element, or icon, is automatically geo-referenced and recorded into the VIGILENT™ database as it is dropped onto the map interface or when it is relocated within the map window. The custom properties feature of CommandSight™ allows users to pre-enter specific information or key characteristics associated with responding personnel and units, supporting agencies or organizations, or other on-site resources as defined by the user.

MedSight™

MedSight™ is at the core of the VIGILENT™ surveillance component, which provides the rapid collection, storage, analysis, and distribution of critical sets of data. These tools and algorithms help public health officials, emergency response personnel, and medical support organizations provide rapid, effective response to outbreaks of natural disease or overt/covert biological warfare attacks on civilian populations.

MedSight™ integrates and continually monitors data from a wide variety of sources and systems, such as hospitals, labs, pharmacies, school districts, clinics, and 911 call centers, providing early identification of an epidemiological event and thus isolating and containing the outbreak early in the cycle.

The mapping feature of MedSight™ provides a view for a defined public health network. This network can include locations and status data of key resources, such as civilian hospitals, medical treatment facilities, military and VA hospitals, local emergency clinics, or drug dispensaries. MedSight™ provides users with an “at-a-glance” picture of ongoing syndromic monitoring results and the real-time status of locations as selected by the user. In short, the MedSight™ application provides approved users with the ability to:

- View the locations and characteristics of key healthcare facilities within the context of a geo-referenced map, including medical treatment facilities, deployed testing unit locations, and areas containing supplemental resource stores;
- Visually monitor and track real-time syndromic and disease monitoring data over time and by location;
- View alerts as defined syndromic thresholds are met or exceeded;
- Share a common operational picture with remotely located command staff, public health organizations, and emergency response personnel; and
- Automatically access and store syndromic indicators and outbreak escalation data over time for after-action review and training.

Critical Care Tracking

Critical Care Tracking (CCT) is a Web-based module of VIGILENT™ providing the immediate exchange of information among hospitals and public safety organizations concerning the status of a hospital's emergency facilities and related critical care departments. Using CCT will give the current capacity and surge capacity of the relevant healthcare community. The application automatically refreshes relevant data every minute, and when the status of a department in a participating hospital changes, a notice is broadcast to other participants, updating them with the most current information available.

The national average wait in a typical emergency room facility is 45 minutes. However, the reality is that the wait can range anywhere from two to six hours. In Los Angeles County, California, seriously ill patients can experience ER waiting periods as long as nine hours. Astonishingly, the record waiting period in the same county is 84 hours. Ambulances are frequently unable to unload patients for long periods of time because there are no available beds

or monitors. When the patient is finally admitted, they sometimes spend 18 hours or more in a triage cube designed for one bed but holding two because there are no hospital beds available. Unfortunately, this is becoming the rule — not the exception.

CCT features include:

Bed Counts

Provides ER and inpatient bed count capacity and availability of each hospital. The user-defined bed types can include such categories as Med/Surgery, ICU, PICU, O/R, Isolation, Negative Pressure, Burn, Pediatric and Psychiatric.

Staff Tracking

Provides staff tracking for each hospital. The user defines the staff categories, such as:

- Physicians
- Nurses
- Respiratory Therapy
- Other Healthcare Staff

Resource types can be defined more specifically under each category. For example, under the Nurse category the resource list could include Pediatric, Burn, Med/Surg, Critical Care, Operating Room, Anesthesiology, and Emergency Room.

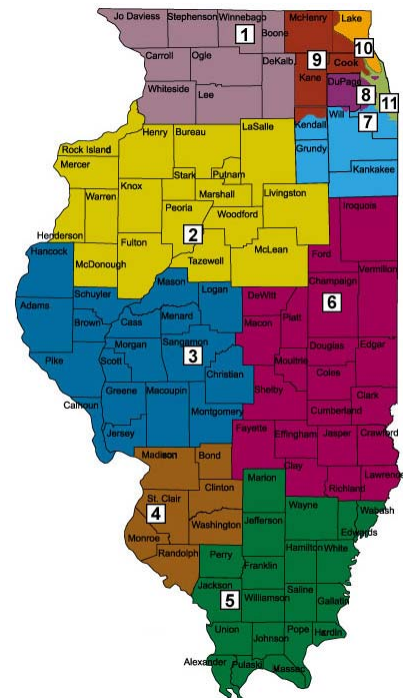
Other Resource Tracking

Because of the flexibility within the program, Compressus can create tabs within CCT to assist with other critical capacity issues, such as medical supplies and pharmaceuticals.

Hospital Bypass

Provides hospital bypass management and publishes the current status of the critical care departments of each participating hospital. Again, the user defines the bypass status options, such as “Open,” “Bypass,” and “Special Bypass.”

The user group also defines the departments that are tracked for bypass, such as ER/ED, ICU, PICU, CCU. This list can be expanded to include any critical resource that is currently being tracked by the user group.



VIGILENT™ tracks medical resources in Illinois' 11 EMS regions.



Ambulance Bypass

Provides ambulance bypass management and publishes current status of the available number of ambulances in each facility. When all of the ambulances in a facility are engaged, they will report a bypass status. The status will reflect the numerical availability of ALS, BLS, and HazMat with facility and system wide totals.

Equipment Tracking

Provides counts for tracking specific equipment and other various hospital resources. This includes the capability to label desired general equipment specific to the hospital as well as standard equipment of interest, such as respirators, blood units, or emergency medicines.

Initiation of Care Patient ID Tracking

Provides the capability to collect and maintain proprietary patient IDs acquired at initiation of care and link them to a unique identifier in VIGILENT™. This unique identifier can then be mapped to the hospital HIS systems through permitted interoperability. This system includes rugged wireless devices that collect patient information in the field and communicate with the hospitals.



Equipment in first responder vehicles is one source of the patient tracking process at the initiation of patient care. The information is imported into VIGILENT™ via XML. Walk-in patient information can be imported into VIGILENT™ via an XML interface from the HIS admissions application. Doctor's Office admissions can be sent to VIGILENT™ from either the doctor's information system or from the HIS admission system via XML interface.

VIGILENT™ can even sort out and keep track of the various patient IDs that are created by the initiation of care in different systems.

Notification

After integrating and analyzing the health data, MedSight™ will automatically open an event and send out a suitable alert via any configured electronic communications network to notify the appropriate individuals or groups. Notification provides messaging services for all of the VIGILENT™ modules. It allows authorized users to define and manage predetermined and ad hoc messages and alerts within all the modules of VIGILENT™. The communications are managed and tracked through the Message Board tab. The Message Board is fully customizable for alerts by the end user and provides real-time communication across agencies, groups, and individuals.

Technical Framework

TECHNICAL FRAMEWORK

The VIGILENT™ framework is built upon standards-based interoperability and modular design architecture. One of the principles driving our work is designing the industry's latest standards and best practices into our software. In fact, members of our team have participated in the actual development of standards those governing XML, wireless communications, and imaging.

Healthcare IT Standards

All of our team's development efforts embrace and extend developing relevant healthcare processes and technology standards, such as HL7, IHE, NEMESIS, HIPAA, NEDSS, HAN, PHIN, and others maturing in the medical and broader business world under the auspices of the Organization for the Advancement of Structured Information Standards (OASIS).

Compressus continues to follow, and in some cases helps drive, the standards that are contributing to efficient interoperability in the medical world. The ultimate goal and value of these principles are that a properly designed architecture should provide the flexibility to replace any component of the system solely based upon required functionality or added value, not technical compatibility.

Bringing together the systems that support these areas builds an effective set of tools to respond to daily events as well as mass casualty events. It also allows discrete regional systems to interoperate with state and federal response systems. The ability to share cross-jurisdictional information is critical to effectively responding to large-scale events.

Communications Architecture

VIGILENT™ is designed to use any physical layer network that supports the TCP/IP protocol suite, including broadband networks. VIGILENT™ also supports, and Compressus recommends, that other physical layer networks, such as cellular, satellite, and POTS, be considered for out-of-band use in times of wide area network brownouts or failure.

VIGILENT™ is built upon a centralized data store that supports a distributed computing environment. The modular applications that comprise VIGILENT™ can be deployed to the initial locations and to satellite facilities by simply adding authentication and authorization information to the LDAP directory that provides this function for VIGILENT™. Since the client is a standard Web browser that can be run on existing workstations, there will not be any equipment costs to extend this communication system.

Interoperability Standards

The information contained in the VIGILENT™ data store can be granularly exposed via XML for use by other applications on the network. Applications can either share an XML interface or use a specific DTD to present a schema for that application. Compressus prefers that all XML interfaces use approved XML standards interfaces as a starting point for interoperability. By incorporating accepted schemas and minimizing overlaps, there will be less reworking of the interoperable data feeds as these standards evolve. VIGILENT™ data and functions can also be exposed as Web services when required for system interoperability.

Compressus is dedicated to interoperability standards in all of its development activities. This dedication is centered on XML and its manifestations such as CAP, VEDS, and other recognized standards that are developed in partnership with the National Incident Management System (NIMS). Interoperability with the broader systems as they are developed means that all the various standard development efforts must be taken into consideration even if they are not applicable to the immediate project.

Compressus is also dedicated to other enterprise application standards, such as LDAP, DSML, X.509, and DICOM, so applications can leverage existing network services and facilitate greater interoperability with other standards-based applications. For example, Universal Description Discovery and Integration (UDDI) is a standard being viewed by NIMS because it provides the ability to build secure electronic white pages for contact information, yellow pages for department and business function categorization, and green pages for locating and publishing available Web services.

VIGILENT™ will accept CAP messages from registered agencies and then forward or trigger a related message to other registered agencies, individuals, and other applications. For example, if several hospitals go on bypass, a policy may be in place that specifies several people and organizations are notified. The CCT notification module will send hospital-specific messages to the appropriate people within the VIGILENT™ module and could also send a CAP message to groups outside the CCT purview. This same approach provides the capability to send messages to federal systems such as the DOJ via the Amber Alert XML. As these standards continue to be accepted, their value will grow exponentially.

Authentication and Authorization

VIGILENT™ uses a standards-based LDAP directory to provide enterprise interoperable authentication information for the system. An LDAP directory provides a scalable centralized administrative service with a distributed data store for identity-specific information, such as X.509 certificates, user roles, establishment of inter-organizational groups, and the transparent integration of meta-directory services necessary for the secure interoperability required for HIPAA.

The addition of users can also be managed by hospitals that have an LDAP directory, such as NDS, Active Directory, or any UNIX LDAP directory in place. Compressus will present the authorization attributes used in VIGILENT™. When they are added to the hospital directory, that

user will then have access to the VIGILENT™ system. This reduces the need for multiple points of administration. As the appropriate users in the hospital directory are moved within groups or otherwise have attributes modified, their access can immediately be altered within VIGILENT™. Another benefit of an LDAP authentication and authorization store is that X.509 certificates can be used for stronger authentication. This allows entities in cross-jurisdictional situations to have temporary authentication and granular authorization to the appropriate system by simply having the hospital or EOC trust an outside individual's X.509 certificate during a mass casualty event or other emergency via the DSML XML authorization standard.

Messaging

VIGILENT™ has a sophisticated Notification service module that manages the communication of internal events and alerts to the participants of the Hospital Bypass system and other VIGILENT™ modules such as MedSight™. The recipients are notified via e-mail, phone, pager, fax, or other communications network and are triggered by customizable events that occur within the system. In addition, alerts can be displayed on any authorized workstation connected to the VIGILENT™ system. Among these recipients are external entities or individuals.

About Compressus

ABOUT COMPRESSUS

Company Overview

Compressus, Inc. is a software development company serving the medical and public health communities with comprehensive, cutting-edge solutions in medical imaging, telemedicine, biosurveillance, and critical incident management. The company's patented data-compression technology, developed by the U.S. military and leading technology companies, enables the rapid collection, storage, and secure transmission of large data sets, such as medical images and hospital system status reports, over any information technology and telecom system. The company is headquartered in Washington, DC, and staffed by experts in medicine, public health, the Internet, defense, and anti-terrorism.

The name "Compressus" refers to our core technology, which compresses enormous data sets and makes it possible to collect them, store them, and transmit them securely over limited bandwidth connections across the Internet. We literally compress the time, staffing and computing resources needed to obtain critical information and make life-saving decisions.

Compressus' clients include the U.S. Department of Homeland Security; U.S. Air Force; U.S. Defense Threat Reduction Agency/NCR Teradata; Illinois Department of Public Health; Northern Virginia Hospital Alliance; Valley Health System in the Northern Shenandoah Valley of Virginia; and Hillsborough County Hospitals in Florida.

Products

Compressus offers three inter-related product lines:

- **VIGILENT™** is the most comprehensive, interoperable suite of IT applications enabling health and safety officials to detect and manage health emergencies.
- **RadSight™** enables healthcare professionals to store, retrieve and transmit large medical-image data files, rapidly and securely, working interoperably with any kind of IT and telecommunications system.
- **ImageI/O™** is Compressus' core data-compression technology, providing optimized data handling for many image types including large geospatial data sets, multi-component color images, and single component medical images (8-bit per pixel and greater).

Management

Compressus is a team of extraordinary professionals from backgrounds including medicine, law enforcement, military, information systems, Internet, software development, anti-terrorism, and public service:

- Chairman and Co-Founder **Tom Campbell** is a former Fortune 100 company executive and head of a Washington-based public affairs firm.
- Co-Founder **Reynaldo Martinez** has a long and distinguished career as a leader in the Democratic Party and in the Hispanic community, including service as Chief of Staff to Senator Harry Reid of Nevada for two terms.
- Chief Executive Officer **John Macfarlane** has more than 30 years of corporate experience including managing an integrated marketing and sales organization for IBM.
- Chief Technology Officer **Laszlo Gasztonyi** has nearly 15 years of technical and managerial experience in the telecommunications and geo-spatial markets. He was one of the experts who invented the “jpeg” compression standard technology and wireless communication protocols.

For more information:

www.compressus.com

202-742-4307