



## Protecting Critical Infrastructure

Enhancing Situational Awareness  
with Nextiva Video Analytics

A VERINT SYSTEMS EXECUTIVE BRIEF

April 2006

### AMERICAS

330 South Service Road  
Melville, NY 11747  
+1 631 962 9600

[info@verint.com](mailto:info@verint.com)  
[www.verint.com](http://www.verint.com)

### EMEA

241 Brooklands Road  
Weybridge, Surrey KT13 0RH  
+44 (0)1932 839500

[marketing.emea@verint.com](mailto:marketing.emea@verint.com)  
[www.verint.com](http://www.verint.com)

### APAC

61 Hoi Yuen Road, Kwun Tong  
Kowloon, Hong Kong  
+852 2797 5678

[marketing.apac@verint.com](mailto:marketing.apac@verint.com)  
[www.verint.com](http://www.verint.com)

## Contents

Preface: Situational Awareness in Critical Infrastructure Environments .....	1
Nextiva Critical Infrastructure: Transforming Video into Value .....	2
Verint. Powering Actionable Intelligence.® .....	2
Nextiva Video Analytics: Actionable Intelligence for a Safer World™ .....	3
The Nextiva Critical Infrastructure Analytics Portfolio.....	3
Analytics “At the Edge” for Superior Accuracy, Scalability and Efficiency.....	4
Addressing Critical Infrastructure Challenges .....	5
Actionable Intelligence — 24x7 — in Dynamic Physical Environments.....	5
Protect Tangible and Virtual Perimeters .....	5
Detect Suspicious Behaviors and Potentially Dangerous Situations.....	6
Access and Direction Analytics.....	6
Behavioral Analytics and Abandoned Object Detection .....	6
Blocked Exit Analytics .....	6
Secure Large-Scale Operations and Enhance Operational Efficiency .....	7
Automatic View Recognition .....	7
A 3-Dimensional Approach to Scene Understanding .....	7
Nextiva Mosaic Scene Stitching .....	7
Object Tracking Across Scenes .....	8
PTZ Control to Zoom in on Activity of Interest.....	8
Automatic Target Acquisition .....	8
Expedite Investigations and Make Them Highly Productive .....	9
Nextiva Investigation Management and Forensic Analyzer .....	9
Conclusion .....	9
Supplementary Materials.....	9

This document contains confidential and proprietary information of Verint Systems Inc. and is protected by copyright laws and related international treaties. Unauthorized use, duplication, disclosure or modification of this document in whole or in part without the written consent of Verint Systems Inc. is strictly prohibited.

By providing this document, Verint Systems Inc. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice.

All marks referenced herein with the ® or TM symbol are registered trademarks or trademarks of Verint Systems Inc. or its subsidiaries. All rights reserved. All other marks are trademarks of their respective owners.

© 2006 Verint Systems Inc. All rights reserved.

## Preface: Situational Awareness in Critical Infrastructure Environments

The complexity associated with protecting critical infrastructure is largely related to both the diversity of these entities and their division of ownership across public and private sectors.

The operation of critical infrastructure may be determined by public policy, or it may be shaped by strategies focused on profit and loss.

Critical infrastructure may reside in a single location, or it may span wide geographic areas that cannot be efficiently or affordably monitored.

Organizations that “own” critical infrastructure may have powerful information systems that provide visibility across their entire operations. Or they may have information silos that lack the means to rapidly share, correlate, and use the security data they collect.

But, all of the systems and facilities that critical infrastructure comprises have this in common: without keen situational awareness, these organizations are more vulnerable to attack, and an attack against one of these entities is likely to have a disruptive effect that cascades and ripples to others.

For critical infrastructure organizations, timely intelligence delivered to the right people at the right time is mission critical — a necessity and not an option.

This executive brief explores how Verint’s Nextiva™ Video Analytics help critical infrastructure organizations leverage the information in their business and security subsystems to develop greater situational awareness and actionable security intelligence.

*“America’s critical infrastructure sectors provide the foundation for our national security, governance, economic vitality and way of life.”*

- 1,800 federal reservoirs
- 1,600 municipal waste water facilities
- 80,000 dams
- 104 commercial nuclear power plants
- 2,800 electric power plants
- 300,000 oil and natural gas producing sites
- 2 billion miles of telecommunications cable
- 66,000 chemical plants
- 250,000 defense firms in 215 distinct industries
- 5,000 public airports
- 120,000 miles of major railroads
- 590,000 highway bridges
- 2 million miles of pipelines
- 300 inland/coastal ports
- 500 major urban public transit operators
- 137 million postal and shipping delivery sites
- 5,800 historic national buildings
- 3,000 government owned or operated facilities
- 460 skyscrapers
- 26,000 FDIC insured financial institutions
- 1.9 million farms
- 87,000 food processing plants
- 5,800 registered public health hospitals
- Emergency services in 87,000 localities

Source: The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, February 2003

### *Nextiva Critical Infrastructure: Transforming Video into Value*

Nextiva Critical Infrastructure is an enterprise-class video management platform designed to protect the physical systems and facilities that are integral to the well-being of the nation, its citizens, and its economy.

With network-intelligent video distribution, resilient system design, industry-leading wireless technology, and an open, IT-friendly architecture, Nextiva addresses the challenges of diverse, geographically-distributed operations — from government installations and interstate transportation networks to energy producers, power grids, and water purification, treatment, and distribution facilities.

Nextiva Critical Infrastructure transforms video into *value*, delivering actionable intelligence for deterring terrorism and crime and promoting a safe environment for people and commerce.

Nextiva integrates video with a wide variety of security subsystems and sensors to form a unified operational framework for proactive threat prevention.

- Access control
- Fire and alarm
- Incident management
- Video analytics
- Biometrics
- Perimeter fence protection
- Behavior analysis sensors
- IP and analog cameras
- Thermal imaging sensors
- Specialized immersive cameras

### *Verint. Powering Actionable Intelligence.®*

Verint® Systems Inc. (NASDAQ: VRNT) is a leading global provider of analytic software-based solutions for communications interception, networked video, and business intelligence. Verint solutions transform voice, video, and text into *actionable intelligence* — timely, mission-critical insights for achieving strategic goals.

Since 1994, Verint has been committed to developing innovative solutions that help our customers achieve their strategic objectives. Today, more than 1000 organizations in over 50 countries use Verint's actionable intelligence solutions to enhance security, boost operational efficiency, and fuel profitability.

"In the current world environment, security has taken on a more vital role for all energy and utility providers. Verint's Networked Video Solution helps us use our resources more effectively, providing secure access to vital energy supplies and a safe work environment for our employees."

Scott McCreery  
Safety Manager for BP

## Nextiva Video Analytics: Actionable Intelligence for a Safer World™

Critical infrastructure organizations collect vast amounts of information — more information than they can rapidly assess and use. Many security and emergency personnel suffer from information overload as they scan banks of monitors, unable to rapidly pinpoint and understand events of importance. And as security initiatives expand, the volume of video continues to grow, often without a corresponding increase in personnel.

Nextiva Critical Infrastructure Analytics provide security and emergency management staff with timely intelligence about events of genuine importance to their organizations, freeing them from hours of tedious, unproductive video review and positioning them to address potential exposures quickly and effectively.

Using critical information from video and incident management, emergency response, and other security systems, Nextiva Analytics automatically detect potential threats and trigger action sequences based on each organization's security policies.

For example, when an emergency occurs, Nextiva can automatically send video and data to network operations centers, emergency communications systems, security personnel, government agencies, and law enforcement for rapid response.

Nextiva can also initiate activity, such as increasing video recording frame rate or moving additional PTZ cameras into the field of view.

Nextiva Video Analytics promote rapid, effective action — even for locations with limited security or emergency management personnel on site.

### *The Nextiva Critical Infrastructure Analytics Portfolio*

The Nextiva Critical Infrastructure Analytics portfolio includes: real-time object detection, identification, and classification; tripwires and virtual perimeters; mosaic panoramic scene stitching; and detection of persons loitering, abandoned objects, blocked exits, and camera tampering or shifting.

Nextiva Critical Infrastructure Analytics are fully integrated with the Nextiva video management platform and suite of software applications, including the Nextiva IntelliFlow™ rules-based engine, Nextiva HealthCheck™ system-wide health monitoring and diagnostics, Nextiva Review and WebReview™ for anytime/anywhere video viewing, and the Nextiva Map interactive visual display of facility layouts and camera locations.



About 85 percent of the United States' critical infrastructures, telecommunications, energy, finance, and transportation systems, are owned and operated by private companies. If our critical infrastructures are targets, it is the private sector that is on the front line.

US Senator Bob Bennett  
Sept 25, 2001

This integration enables Nextiva Analytic applications to leverage Nextiva’s robust functionality “out of the box” and provides Nextiva Critical Infrastructure Analytics with a rich source of video and other information for producing highly accurate and timely intelligence. This integration, as well as Nextiva’s open, standards-based architecture, also lowers implementation costs and eliminates many of the problems associated with deploying standalone analytic applications with existing video systems.

### *Analytics “At the Edge” for Superior Accuracy, Scalability and Efficiency*

Traditional analytic solutions are server based and consequently require significant computational power. Built on a scalable, open architecture, Nextiva Critical Infrastructure Analytics offer a distributed approach for optimum device and bandwidth utilization.

Nextiva Analytics can be applied to high-quality video at the point of capture without the need to send all data to centralized servers for analysis. These analytics “at the edge” provide superior accuracy since analytic applications are applied to high-quality video. Analytics at the edge also reduce data transport and storage requirements, because only the most significant video is transmitted to centralized servers and storage devices. And analytic capabilities can be expanded (via additional edge devices) without the need for costly additional servers, for enhanced scalability and lower deployment costs.

Nextiva exploits the excess computational power of the edge device’s digital signal processors and then combines the logic and object management on the server’s CPU. This provides for more complete utilization of resources and reduces data transport and storage costs.

Verint offers a wide range of analytics-certified, wireline and wireless Nextiva Intelligent Edge Devices for indoor and outdoor use. These devices are well suited to critical infrastructure environments, capturing critical video and data virtually *anywhere* that impacts security and operational performance.



## Addressing Critical Infrastructure Challenges

### *Actionable Intelligence — 24x7 — in Dynamic Physical Environments*

**Challenge: Support 24x7 information accuracy and availability in dynamic environments often characterized by fluctuating and/or harsh weather conditions.**

Nextiva Critical Infrastructure Analytics work effectively in virtually all weather conditions, day/night applications, and complex scenes, making them especially appropriate for the geographically-distributed environments and expansive, unmanned perimeters that are characteristic of many critical infrastructure operations, such as power grids, public works, airports, seaports, and interstate transportation networks.

The Nextiva CamAlert analytic application automatically notifies the appropriate personnel of camera tampering or shifting and initiates appropriate followup action to help ensure that mission-critical video continues to be captured.

### *Protect Tangible and Virtual Perimeters*

**Challenge: Secure expansive tangible and virtual perimeters/borders that cannot be efficiently or practically patrolled.**

Nextiva Critical Infrastructure Analytics enable organizations to create custom detection rules to secure tangible and virtual perimeters or borders in virtually any environment. Nextiva Analytics enable security personnel to monitor complex or busy scenes, both indoors and outdoors, with special filters (such as a salience filter) for zeroing in on activity of interest. Nextiva Analytics can detect people and vehicles crossing virtual perimeters by enabling users to draw virtual perimeters, or *tripwires*, on their camera views, specify an alert direction, and dynamically extend or retract protection zones, as needed. Nextiva Analytics also differentiate between people and inanimate objects or vehicles, with speed filters for detecting individuals running and speeding cars. (See *Access and Direction Analytics* for more details.)



Organizations can define specific areas of interest and virtual perimeters (tripwires) in which additional detection rules can be applied; for example, people climbing over a fence or objects being thrown.

## *Detect Suspicious Behaviors and Potentially Dangerous Situations*

**Challenge: Rapidly detect potentially dangerous activity – from access to sensitive locations to suspicious objects left behind – even in areas that cannot be visually monitored or patrolled 24x7.**

### **Access and Direction Analytics**

Nextiva Critical Infrastructure Analytics can help organizations monitor the movement of people and vehicles in terms of both direction and speed. Users can specify which directional movements and speeds are approved for specific areas and which movements and speeds cause an alert to be triggered. They can also draw double tripwires on camera views, defining rules for allowed directions of travel and vehicles, as well as speed zones.

Nextiva Critical Infrastructure Analytics automatically detect activity defined by these rules, such as a truck approaching a government building at 70 miles per hour or persons entering a restricted facility through exit doors. Then, using the Nextiva IntelliFlow rules-based engine, Nextiva issues alerts to the appropriate personnel and initiates predefined actions (such as raising barriers or locking doors).



Nextiva Access and Direction Analytics can be used in flight line surveillance, recognition of watercraft, and coastal border protection.

### **Behavioral Analytics and Abandoned Object Detection**

Nextiva Critical Infrastructure Analytics enable organizations to define rules for detecting (a) people or vehicles that remain in or near sensitive areas in excess of a situation-specific threshold of time, (b) assets that are moved from their designated locations, and (c) objects (such as backpacks or briefcases) that are left behind. Once one of these situations is detected, the event is tagged as a security concern, and a real-time alarm is generated.

### **Blocked Exit Analytics**

Nextiva Critical Infrastructure Analytics are designed to recognize potential hazards associated with blocked exits and issue an alert to the appropriate personnel to eliminate the hazard. Nextiva Analytics help facilities identify blocked exits before they impact the safety of visitors and staff and comply with fire regulations.

## *Secure Large-Scale Operations and Enhance Operational Efficiency*

**Challenge: Secure large-scale operations spanning vast geographical areas, and position security and emergency management staff to act more efficiently.**

### **Automatic View Recognition**

Nextiva Analytics help security personnel quickly detect suspicious activity by storing multiple pre-set views for single cameras and the specific rules associated with each view. This Automatic View Recognition helps equip security personnel to understand the context in which events occur, moving them from single, out-of-context camera views to actually seeing the scene of the event and watching the activity unfold.

### **A 3-Dimensional Approach to Scene Understanding**

Understanding the physical relationship between objects and people in a scene is essential to reliable tracking and behavior analysis. Verint addresses this challenge with a three-dimensional approach to scene understanding, basing tracking and analysis algorithms on an automatic process of calibration to promote highly accurate video analytics-based monitoring. This automatic calibration establishes a deep understanding of the perspective structure of the scene and requires no tuning to object sizes and types. Exploiting the understanding of physical measurements of objects enables the system to be invariant to the structure of the scene, the positioning of the camera, and the alignment of its view to the tracked objects. Such invariance streamlines system installation, eliminating the tedious process of fine tuning and customization.

### **Nextiva Mosaic Scene Stitching**

It is difficult for users to have a complete understanding of all physical premises, as well as the outline and locations of all cameras connected to the system, especially for the large, distributed video security systems that are characteristic of many critical infrastructure environments. Users who observe an event captured by a specific camera must keep exact track of how this camera relates to the real world and its connections to neighboring cameras. And if the monitored event moves beyond the coverage area of the specific camera, the user needs to manually switch to other cameras.



Nextiva Mosaic is especially useful in very long or wide open areas, such as airport tarmacs, city squares, and large parking lots.

Nextiva Critical Infrastructure Analytics takes a scene-based approach so that users no longer need to manage and manipulate cameras. Instead, Nextiva Analytics support the perception that the scene is a physical location in the premises that may be covered by any number of cameras.

Nextiva Mosaic stitches scenes from many cameras in real time into a single seamless view, creating a mosaic image that allows the operator to view a full scene as the human eye was meant to see it. This virtual scene presentation helps security and emergency management personnel identify, track, and address an assortment of subjects (people, vehicles, etc.) over several camera views.

### **Object Tracking Across Scenes**

Once a scene is created, security personnel may need to view the progress of certain objects across the full stitched scene. Nextiva Mosaic enables a seamless track-line of any object, person, or vehicle from one end of the scene to the other, enhancing the security of critical infrastructure operations by keeping all objects within the line of sight.

### **PTZ Control to Zoom in on Activity of Interest**

Nextiva Mosaic enables security personnel to manually zoom in on one or more regions of interest in order to more closely observe the events taking place. This manual PTZ (Pan-Tilt-Zoom) control using existing cameras eliminates the need to invest in additional high-zoom cameras. Users can select several regions of interest and view them separately, while keeping the full scene in view for contextual placement.

### **Automatic Target Acquisition**

Nextiva Mosaic also enables security personnel to zoom in on an animate subject, such as a person or a vehicle, and track it across the full scene in a separate view, as if there were an additional PTZ camera trained on the scene. This enables security personnel to zoom in on a suspicious person or vehicle, recognize a license plate number or match a face to a database, while keeping the subject tracked throughout its stay in the scene. This readily available intelligence better equips security teams to address potential threats and other dangerous situations.



Nextiva Mosaic Automatic Target Acquisition Analytics track subjects as though there were an additional PTZ camera on the scene.

## *Expedite Investigations and Make Them Highly Productive*

**Challenge: In a critical infrastructure environment, security events must be addressed as quickly as possible.**

Nextiva Critical Infrastructure Analytics are fully integrated with the Nextiva video management platform and software applications and are designed for ready integration with other physical security subsystems. This integration promotes a high level of situational awareness by enabling critical information to be shared among security and other enterprise systems for the development of actionable security intelligence and by leveraging Nextiva functionality to ensure that this intelligence is delivered to the appropriate people, departments, and organizations in a timely way.

### **Nextiva Investigation Management and Forensic Analyzer**

Nextiva Investigation Management enables investigators to gather all case-related audio, video, and data from an array of cameras, locations, and enterprise systems in a searchable database.

The Nextiva Forensic Analyzer rapidly zeroes in on past events, unusual activity, and significant behavioral patterns in this vast amount of video.

Using a proven video authentication method to ensure video integrity, Nextiva lets users easily share video with law enforcement and other agencies for investigation and corroboration.



Nextiva Critical Infrastructure expedites investigations and facilitates cross-agency collaboration.

## **Conclusion**

Nextiva Video Analytics can significantly enhance situational awareness for critical infrastructure organizations, positioning them to more effectively deter terrorism and crime and promote a safe environment for people and commerce.

## **Supplementary Materials**

The following Verint executive briefs present useful information related to this topic. To receive the titles listed below, contact your Verint representative or call Verint at 1-631-962-9600.

- The 3 R's of IT-Friendly Solutions
- Actionable Intelligence for a Safer World and a Smarter Enterprise