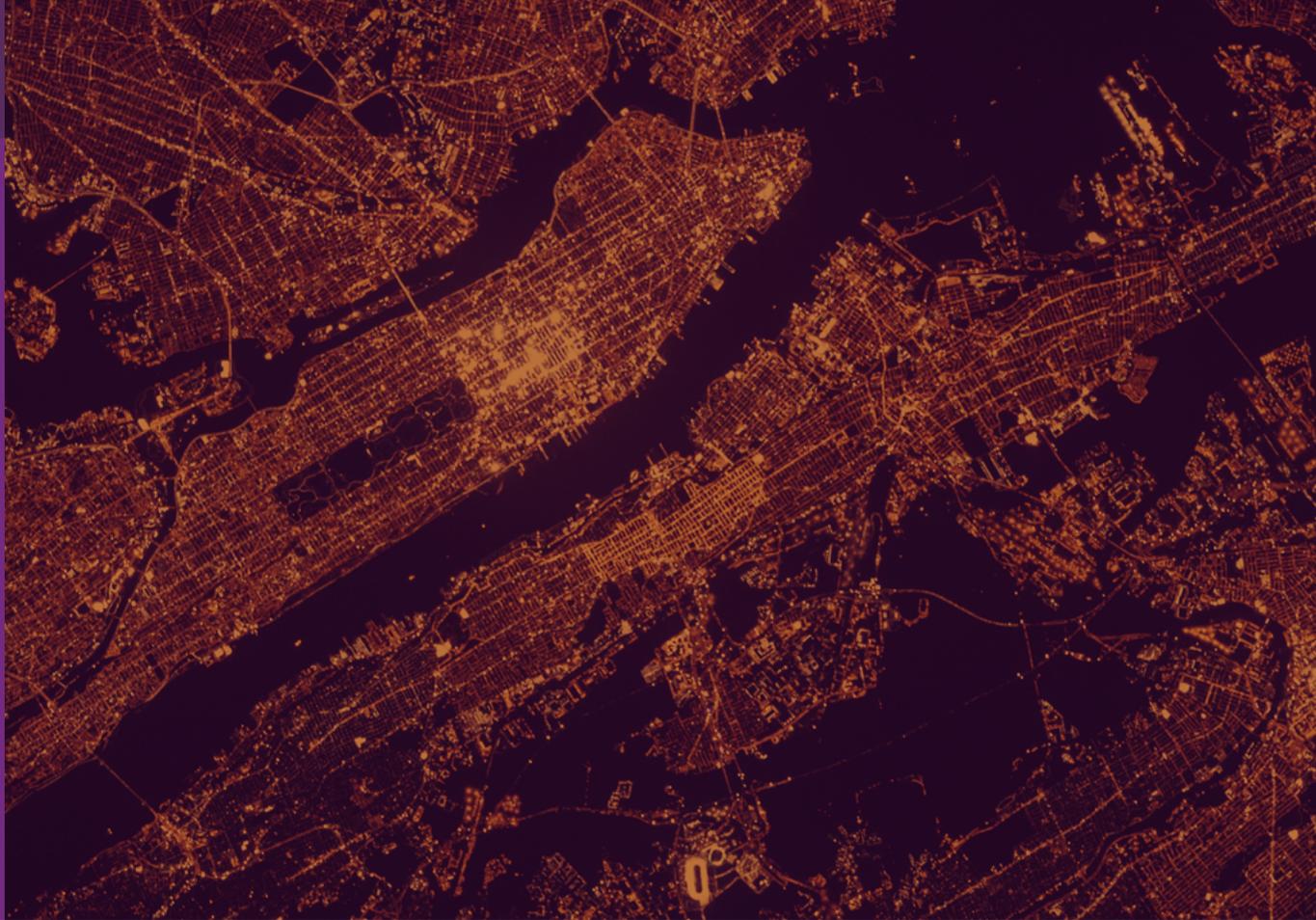


Interface Security Systems



THE CUSTOMER

Interface Security Systems is a cloud-based managed security services provider. The company integrates network and security needs into one platform, with the goal of being a single-vendor source for their customer's needs. Through its Secure Managed Broadband Service, Interface provides a PCI compliant private network to connect POS systems, credit card authorizations, inventory, security and WIFI. Interface also integrates intrusion detection, fire safety, access control and video surveillance to create one aggregate network for a more complete, secure, and economical solution.

Interface Security Systems started as a small commercial security monitoring company in 1995, and by 2001 it had grown to become one of the top 20 security companies in the country (based on industry rankings).

The company's expertise spans many different business categories including retail, restaurant, hospitality, and convenience stores. Interface's unparalleled security services bundle is deployed by many of the top brands in the country, including Dollar General, Michaels, Applebee's, and GameStop.

In 2007, the Interface team recognized that the combination of physical security (buildings) and logical security (network and computer technologies) would redefine the role of commercial security providers. As a result, they acquired Loss Prevention Management—a company that had developed a private, secure-managed, wide area broadband network. Interface then had the challenge of integrating LPM's IP infrastructure and network operations center into their secure operations center to create a unified platform.

THE NEED

Traditional physical security data (burg, fire, open/closes, etc.) was managed through the Manitou platform and the Interface team was confident in the Manitou solution; however, Interface was now managing various, non-traditional, products and services that were not monitored in Manitou. As part of the managed services bundle, Interface was monitoring multiple functions of their broadband services, including router status, primary circuit status, and VPN tunnel status, among others. As Dan Reynolds, the Senior VP of Customer Operations at Interface, explains, “These services and devices were, at the time, being monitored by dispatchers using separate tools and applications open on multiple screens. We had to streamline the process to make it more efficient.” The Interface team knew from the start that the solution was to integrate these non-traditional signals into their Manitou alarm monitoring platform.

THE SOLUTION

The teams at Interface Security Systems and Bold Technologies determined that data from the different systems and devices must be interpreted by Manitou similar to traditional alarm events. Delivering the data from multiple systems into Manitou would allow Interface to process all information through one system and provide detailed instructions to their dispatchers on how to manage each event. These discussions led to the development of Bold Technologies’ UniversalConnector, a software receiver designed to convert signals from non-traditional

transmissions into regular signals which are then processed by Manitou. The UniversalConnector can take data from a variety of sources including SMS, email, ODBC database tables, FTP, TCP, GPRS, RSS, UDP, and simple files. In the case of Interface’s broadband services, any “change of state” data was being stored on a MySQL database, so the UniversalConnector took the data from the appropriate ODBC database table and delivered that data into Manitou.

The implementation of this solution was a matter of determining how the signals would be translated into Manitou. The software had to interpret the incoming data—whether it was a primary circuit status changing from up to down, or a network latency signal presenting as an email. The data needed to be presented in way so Manitou could decipher it and create an alarm event to be actioned. Bold’s development team utilized datamaps to organize the information for Manitou to read.

A datamap is used to determine which database fields from Manitou are to be populated from the available information. Each piece of data is mapped into a specific field, such as date/time, transmitter ID, event code, etc. In the case of email notifications, the datamap organizes the data including the subject, date and time, email body, and attachments into separate database fields to be read by Manitou. Once the datamaps were completed for Interface, the data from the different types of broadband services were sent into Manitou and presented as alarm events.



THE RESULTS

Employing the solution to Interface was a seamless event. The alarms from the various devices and applications were delivered into Manitou just like the traditional burglar and fire alarms that Interface’s dispatchers were already accustomed to handling. In addition, the UniversalConnector was designed as a future-proof solution which has brought additional revenue opportunities to Interface.

Reynolds comments, “We need as many connections as we can have for all of the unique services we offer. This solution has enabled us to offer additional services to customers and promotes ease of use while providing those services. The UniversalConnector makes it possible for us to manage multiple products and services through one event monitoring platform.”

Learn how Bold Technologies can help to streamline your processes today!



800-255-BOLD
boldgroup.com
sales@boldgroup.com