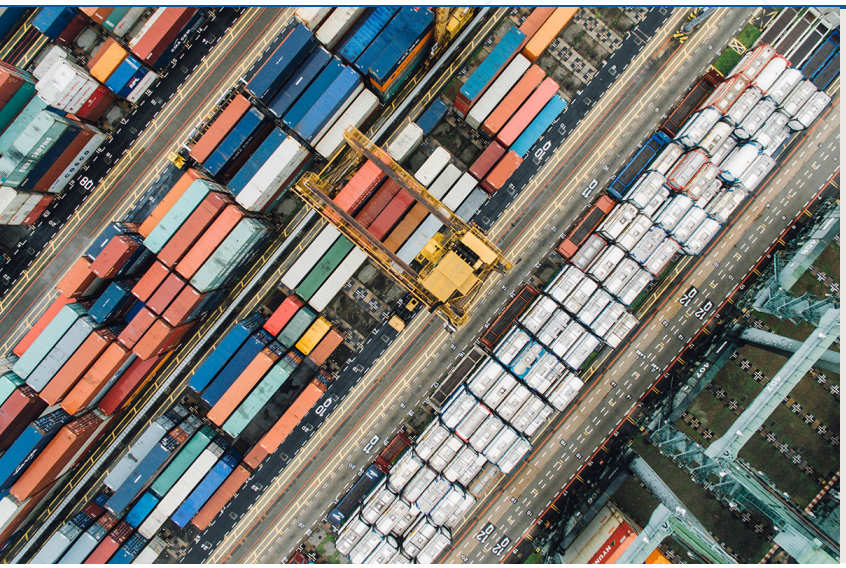
Vunetrix
Always On. Always Vigilant.

SMART Dashboard for Security Professionals
Sensor Monitoring, Alerting, and Reporting Technology



# Unattended Lots with Valuable Property

## (Auto Dealerships and Scrap Yards)

## Use Case

## Background

Client: Alarm Monitoring Company

Situation: An Alarm Monitoring Company was hired to monitor in real time unattended scrap yards and auto dealerships. They used motion detectors with built in alarms to determine when unauthorized individuals were on the property after hours. Once an alarm was tripped, monitoring attendants would access live video feeds and look for intruders in real-time in order to validate the alarm. When the presence of an intruder was confirmed, monitoring attendants would alert the police and then dial into the speakers on the lot. Intruders would verbally warn the intruders through the speakers to get off the property as police were on the way.

This company manages upwards of 15,000 cameras and 5,000 supporting devices such as audio transmitters, network connected speakers, networks switches, and NVRs within geographically dispersed areas.

Goals: Use the Vunetrix SMART dashboard and real-time notification emails to detect, troubleshoot, and respond to both device and service failures in a timely manner. Ensure live video feeds are always available when needed to verify alarms. Ensure speakers are on and available.

## Users Internal Only

Alarm Monitoring Company

- Monitoring Attendants - daily SMART dashboard users (in SOC) to assure all equipment is online and functioning as designed. Responsible for sending tickets to regional site technicians who resolve onsite issues.
- Monitoring Administrator – ad hoc to bring on new sites, daily site maintenance

# Vunetrix Deployment

On Premise Licensed

## Interactions with Vunetrix System

### Set up

1. Configure devices for SNMP community strings & WMI username/passwords.
2. Install and configure local core with appropriate license.
3. Install remote probe software locally on a Windows box and connect back to local core server through encrypted connection.
4. Discover one device on the network per device type.
5. Create a gold standard device template per device type.
6. Discover the rest of the devices based upon the gold standard templates and place into appropriate group/container.
7. Set thresholds for alerts.
8. Configure notifications.
9. Visual SMART dashboard becomes alive with color-coded graphical representation of system wide status and performance.

### Day to Day

1. SOC constantly logged into SMART dashboard to view real-time system status, alerts, and reports.
2. Monitoring attendants respond to anomaly alerts that are delivered via email.
3. Login to SMART dashboard to perform high level trouble shooting.
4. Remote into each site to perform further trouble shooting and issue investigation.
5. Unresolved issues are acknowledged and referred to regional field systems technicians to perform further onsite troubleshooting and/or device replacement.
6. Resolved issues are automatically updated to ok status on SMART dashboard.

Ad Hoc - Reoccurring issue diagnostics are handled via historical data queries.

## POTENTIAL EXCEPTIONS

Monitoring Windows Servers using WMI - When a user changes the username and password on a Windows server, that server's sensors go into an error state until they are reconfigured with the correct and updated user name and password.

Probe Disconnected - When a remote probe is disconnected, an alert occurs on the SMART dashboard and via email. Locally, the probe continues to monitor devices on site. When the probe is reconnected, cached monitoring data is uploaded to the dashboard.