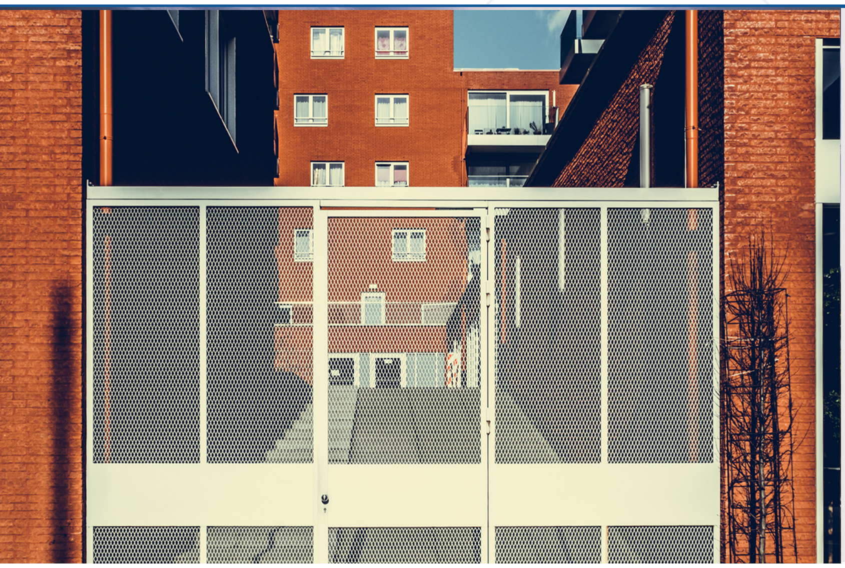
Vunetrix

Always On. Always Vigilant.

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



Property Management

Use Case

Background

Client: A regional integrator supporting a property management firm with multiple locations across the country.

Situation: A property management firm was concerned with liability issues surrounding the loss of recorded video at multiple locations across the country. Liability factors were compounded by the high risk of camera device tampering. They engaged with an integrator who could remotely manage their geographically disparate surveillance systems and detect issues as well as provide proactive alerts to assure camera uptime and system health.

Goals: Use the Vunetrix SMART Dashboard to detect when cameras are tampered with or have failed. Provide notification when video storage devices are approaching capacity, are in pre-failure state and need replacing, or have issues recording video to the NVR.

Users Internal & External

System Integrator

- Security Systems Technicians: SMART dashboard user in response to security device alerts; responsible for overall health and performance of all VMS systems at all sites
- Customer Service Manager: Intermittent SMART dashboard user; reports and quality assurance metrics
- Security Field Technicians: Ad Hoc SMART dashboard users in response to specific troubleshooting cases

Property Management Firm

- Community and/or Facility Manager by location: Intermittent SMART dashboard users

Vunetrix Deployment

Secure Hosted Cloud

Interactions with Vunetrix System

Set up

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

Day to Day

1. Users respond to anomaly alerts that come via email from the SMART Dashboard.
2. Login to SMART Dashboard to perform high level trouble shooting.
3. Remote into each site to perform further trouble shooting and issue investigation.
4. Unresolved issues are acknowledged and referred to local or subcontracted security field technicians to perform further onsite troubleshooting and/or device replacement.
5. Resolved issues are automatically updated to ok status on the SMART Dashboard.

Monthly

System status reports run and shared with client for SLA verification.

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 SMART Dashboard.