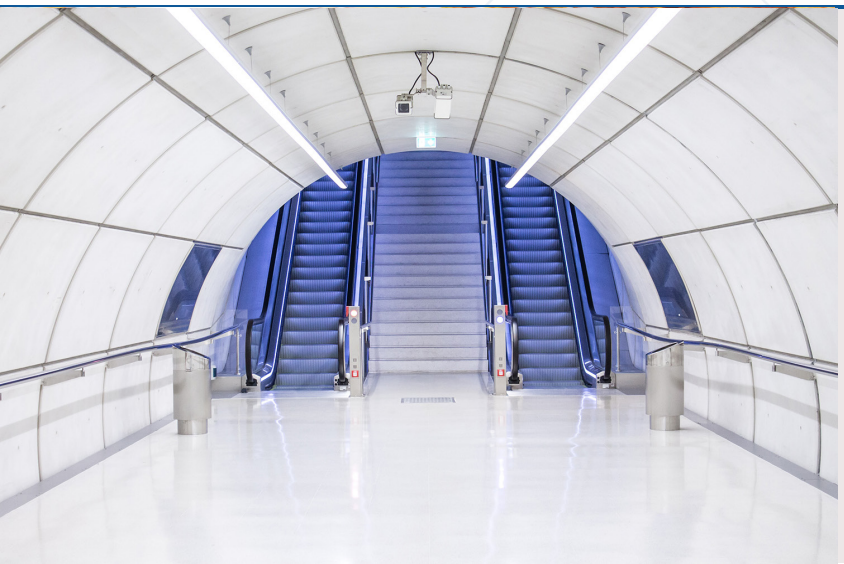
Vunetrix
Always On. Always Vigilant.

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



Maintenance Contract Enhancement

Use Case

Background

Client: Regional Integrator

Situation: A forward thinking integrator was hyper-focused on providing proactive maintenance and exceptional service to all of its customers. Several of their customers had maintenance contract that required a 4-hour SLA.

Goals: Use the Vunetrix SMART dashboard to detect, troubleshoot, and respond to both device and service failures in a timely manner. Reduce truck rolls, time to fix issues, and lower the overall cost to maintain contracts. Ultimately, they wanted to be able to know when something was wrong inside their customers' security environments even before their customers knew they had a problem.

Users Integrator Employees and Customer End Users

Integrator Employees

- Customer Care Manager - daily SMART dashboard user (in SOC)
- Integrator Systems Technicians – daily SMART dashboard users in response to security device alerts
- Integrator Field Technicians - Ad Hoc SMART dashboard users in response to specific troubleshooting cases

Customer End Users

- Customer Security Managers – Ad Hoc SMART dashboard users to view system performance and pull reports

Vunetrix Deployment

Private Hosted Secure Cloud

Interactions with Vunetrix System

Set up

1. Configure devices for SNMP community strings & WMI username/passwords.
2. Install and configure private hosted core with appropriate license and customized branding
3. Configure customized network firewall rules for external probes to connect to secure hosted core server
4. Install remote probe software locally on a Windows box and connect back to private hosted core server through encrypted connection.
5. Create user groups unique to Integrator Business Units, Regional Field Support Teams, and Customers/End Users
6. Discover one device on the network per device type.
7. Create a gold standard device template per device type.
8. Discover the rest of the devices based upon the gold standard templates and place into appropriate group/container.
9. Assign appropriate access rights for various groups to be able to view their own parts of the security network.
10. Set thresholds for alerts.
11. Configure notifications.
12. Visual SMART dashboard becomes alive with color-coded graphical representation of system wide status and performance.

Day to Day

1. Customer Care Manager constantly logged into SMART dashboard on SOC to view real-time system status, alerts, and reports.
2. Integrator Systems Technicians respond to anomaly alerts that are delivered via email.
3. Integrator Systems Technicians login to SMART dashboard to perform high level trouble shooting and issue investigation.
4. Unresolved issues are acknowledged and referred to Integrator Field technicians to perform further onsite troubleshooting and/or device replacement.
5. Resolved issues are automatically updated to ok status on SMART dashboard.

Monthly - System status reports run and shared with client for SLA verification. Internal reports run for uptime metrics to all stakeholders.

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.