SCMP
SECURITY CLOUD & MOBILE PARTNERS

Service Automation For Security Systems

Detect Physical & Logical Failures
Reduce Repair Costs & Downtime
Auto-Deploy Camera Firmware Upgrades
Generate Regulatory Compliance Reports

Powered by Viakoo

What are the consequences to your organization if security video is lost or not recorded?

Solutions Overview

Security Cloud & Mobile Partners is the first company focused exclusively on Service Improvement of Electronic Security Systems. We enable Security, IT and Facility Management teams to detect and mitigate the operating risks associated with networked video and access control systems, as well as IoT connected devices. Our solutions monitor and analyze those devices and processes that your security systems and IT management tools can't, because they are not designed to. This is the only Global Service Assurance application on the market for physical electronic security systems.

Our solutions are powered by Viakoo's patented technology. The application scans the relevant network infrastructure gathering meta-data (performance and health data) from every logical and physical device, process and application critical to your security systems. The next autonomous step identifies and analyzes the behavior of all devices and their applications and alerts you to all failures, anomalies and behaviors that can predict failures. And then you are provided with a recommended fix to the problem as a result of our root cause analysis. Our solution options also enable remote camera firmware upgrades, compliance reporting and detection of cyber vulnerabilities. All this from within a single application.

The Issues: Multiple Points of Failure

For your video security system to work properly, it has to be designed, installed and programmed correctly. And, all of its components need to work in perfect harmony with all of the network applications and devices. This includes cameras and their firmware, network switches, VMS application software, server electronics, the operating system, network interface cards, storage servers and their drives. There are at least 10 different physical or logical components a video stream passes through in order to successfully be stored on a disk drive for replay at a later date.

So there is no longer a single point of failure, there are hundreds, if not thousands. And the causes can be due to power or current fluctuations from the POE switch. IT can download a security upgrade to a server, reboot the server, but neglect to restart the capture service in the VMS application. A connector problem can be undetected and grow worse over time until it fails. And if these failures or the degraded operation go undetected, they can suddenly and without warning negatively impact storage retention goals, cause corrupt video, and even cause video to not be recorded or to not be retrievable.

There are also additional risks to reporting required to meet regulatory requirements, including documentation proving system uptime and documentation relating to maintenance. There are also cyber vulnerability risks associated with not changing the default passwords that come with cameras.

Doesn't my VMS or IT monitor this?

The primary reason this is a problem is that the majority of Video Management Systems (VMS's) on the market are not designed to fully protect themselves or diagnose their own service vulnerabilities or the IT infrastructure on which they reside. And the tools your IT department owns are not designed to diagnose and troubleshoot your electronic security systems nor the software managing those devices, let alone analyze your system behavior. Combined, neither are capable of documenting performance trends and predicting potential failures without additional human analysis involvement. Our Viakoo solution is the only purpose-built, single solution, granular enough to determine whether an individual camera stream is recording, or not, and, the only solution capable of automatically performing storage layer and camera/network problem root cause analysis and providing a recommended fix.
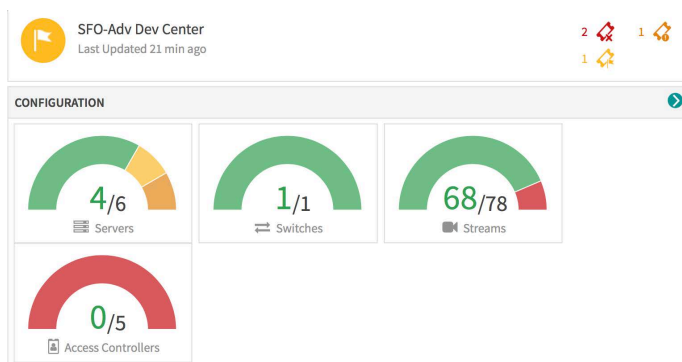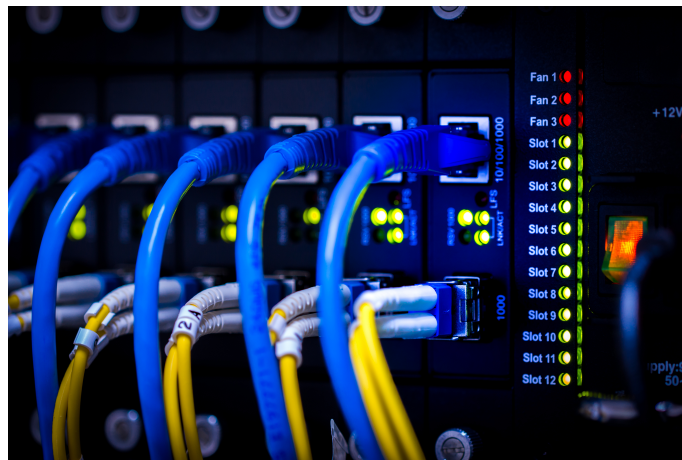
WE HELP ORGANIZATIONS LIKE YOURS TO:

Reduce Service Expenses and Increase Uptime by alerting you to previously undetectable failures and providing Root Cause Analysis and recommending the most likely problem fix before calling your service provider - thus eliminating multiple truck rolls and reducing troubleshooting and diagnostic times, which account for 80% of all service costs.

Eliminate Lost Video by alerting you when storage volumes fail or individual camera streams become unstable and are likely to cause corrupt video.
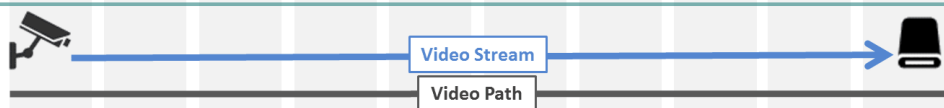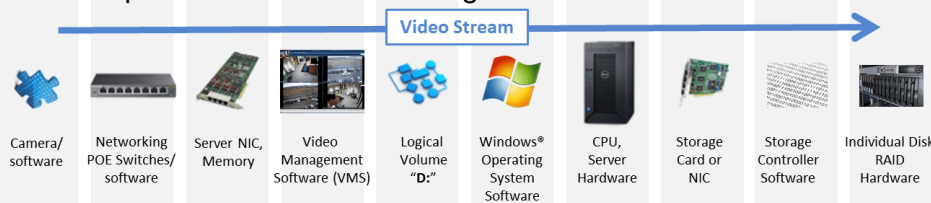
Document Regulatory Compliance by automatically documenting system uptime, retention goal confirmations and service history - saving your organization from lengthy audits. Our solutions also notify you of malicious or intentional file deletions. A complete service ticketing system is included.

Defend Against Cyber Vulnerabilities by alerting you if and when default camera passwords and firmware have been changed or updated, whether foreign connections have been made to your cameras and by keeping all diagnostic data on a digital twin instead of production servers.

Auto-Deploy Camera Firmware Updates - Viakoo's Camera Firmware Update Manager (CFUM) provides the capability to automatically update firmware on camera devices from multiple manufacturers, and performs these updates with a chain-of-trust method that ensures integrity of the firmware.

SFO-Adv Dev Center
Last Updated 21 min ago

CONFIGURATION

4/6 Servers
1/1 Switches
68/78 Streams
0/5 Access Controllers

Components make Path through which Video Stream travels

Video Stream

Camera/ software	Networking POE Switches/ software	Server NIC, Memory	Video Management Software (VMS)	Logical Volume "D:"	Windows® Operating System Software	CPU, Server Hardware	Storage Card or NIC	Storage Controller Software	Individual Disk RAID Hardware

How Solutions "See" Video Stream

Video Stream
Video Path

Only the full Stream-and-Path view provides the complete and correct context for diagnostics data

Highest Value Solution is Video Stream Centric From End-to-End. Entire Stream is seen, with Components acting as an integrated team working together, providing Stream, Path and Compliance KPIs.

IT Monitoring Tools lose track of Video Stream at NIC. Components are seen as independent devices.

VMS focuses on Video Content, not Path. Components are seen as independent devices.

Try us free and let us show you how we're changing service - it's on us. Call or email us today.