White Paper:
Video System Cyber and Performance Assurance

April 16, 2018

Viakoo
1100 La Avenida Street
Bldg. B
Mountain View, CA 94043

Tel: (650) 263-8225
Web: www.viakoo.com

VIAKOO

Video System Cyber and Performance Assurance

For nearly two decades, assuring that software updates occur on a timely basis has been one of the primary concerns of IT service providers and their clients, in large part due to growing cybersecurity threats. More recently, cybersecurity has become a primary concern for electronic physical security systems. Thus, providing software and firmware updates became a stronger focus in the physical security industry, especially after the highly publicized malware infections that compromised more than a million networked surveillance cameras, routers and video recorders (DVRs, NVRs and video servers).[1]

The type of malware used in these attacks creates a botnet, a network of private computers infected with malicious software and controlled as a group without their owners' knowledge. A botnet allows the controlling attacker to perform distributed denial-of-service (DDoS) attacks on other systems, as well as steal data and disrupt systems operations. The camera owners in the publicized attacks from 2014 to 2017 were not aware that their cameras and recording devices were infected.

> Cybersecurity is now a primary concern for electronic physical security systems.

Botnet Malware

Botnets introduce a new twist to the consequences of malware infection: infected cameras that you own are likely be used to attack the systems of other organizations. The impact of such infections can have severe consequences.

For example, one such attack targeted Rutgers University during final exams and registration periods and disrupted student services for several days.[2] After the attack, the university spent $300,000 on consulting fees to upgrade their cybersecurity, and tripled their funding for IT from $1 million to $3 million.

To keep cameras out of botnets, camera vendors must fix discovered critical vulnerabilities as soon as possible and quickly provide updates (patches) for them. Security integrators, and end users who manage their own security devices, must keep their cameras and servers current with released patches.

Security Industry Wake Up Call

A decade ago, the prevalent security industry thinking was that electronic security systems should be installed on secure standalone networks, and that access to security system functionality and data should be limited to a select number of security personnel only. However, that approach to security system deployments is no longer feasible.

Mobile devices and Internet-connected WiFi networks have created expectations that work-related systems should be available anytime, anywhere and on any device. Those expectations now extend beyond security staff, for example, to corporate and business-partner personnel who want to schedule visitors or request security access changes (access control system) and check on the status of company

[1] Franceschi-Bicchierai, Lorenzo (2016, September 29). *How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet.* Retrived from: https://motherboard.vice.com/en_us/article/8q8dab/15-million-connected-cameras-ddos-botnet-brian-krebs

[2] Adely, Hannan (2017, December 13). Former Rutgers student pleads guilty in cyber attacks. Retrieved from: https://www.northjersey.com/story/news/2017/12/13/union-county-man-pleads-guilty-rutgers-cyber-attacks/949591001/

activities or customer activity (video management system). Security video analytics have become critically important for managing retail spaces and evaluating the effectiveness of marketing campaigns, and campaign stakeholders also want access to that data.

Due to security technology continuing advancement, the value of security system functionality is increasing by leaps and bounds for a growing number of organizational stakeholders. Consequently, typical end user counts for security systems are growing from dozens of users per system to hundreds or thousands of users. Current-day security systems must be connected to other networks, provide remote access via the Internet, and be available 24 hours a day, every day. This always-on connectivity increases the windows of opportunity for cybersecurity attacks.

The Challenge of Camera Updates

The increasing availability of cameras and servers to cyber attackers makes it critically important to keep security system software and camera firmware updated as patches are released. Most security system integrators and customer IT departments have tools in place for keeping standard server software up to date. Several leading video management system software vendors have server update systems in place.

However, updating cameras has always been a manual activity, and for customers with hundreds or thousands of cameras deployed, keeping camera firmware updated has been an impossible task. That leaves cameras as the cybersecurity weak point in any networked security system.

> Cameras are the cybersecurity weak point in today's physical security systems.

Cybersecurity Perspective

The Center for Internet Security, Inc. (CIS) is a 501c3 nonprofit organization whose mission is to identify, develop, validate, promote, and sustain best practices in cyber security. CIS delivers world-class cyber security solutions to prevent and rapidly respond to cyber incidents.[3] CIS develops, publishes and maintains the *CIS Controls*™, which are a prioritized set of actions that collectively form a set of field-proven defense-in-depth best practices that mitigate the most common attacks against systems and networks.

The CIS controls include people, process and technology measures for cyber defense. CIS states that of the 20 CIS Controls, "CIS Controls 1 through 6 (the Basic Controls) are essential to success and should be considered among the very first things to be done."[4] Proper management of camera firmware involves the first four of the six Basic Controls, each of which have several Sub-Controls.

The CIS Sub-Controls relevant to camera firmware management are identified below and presented with a description of their application to camera management.

[3] Center for Internet Security (2018, March 19). *CIS Controls Version 7* (PDF document), p.4. Downloaded from the page: https://www.cisecurity.org/controls/

[4] Ibid. p.5.

CIS Control 1: Inventory and Control of Hardware Assets

It is important to actively inventory and track all devices on the security network and to detect unauthorized devices, because unauthorized devices can be attacked, enrolled in botnets, and used to orchestrate cyberattacks on security system equipment and other systems. Additionally, it requires maintaining up-to-date records to keep cameras well-serviced and cybersecure.

No.	CIS Sub-Control Title	Description
1.1	Utilize an Active Discovery Tool	Use an active network discovery tool to identify network security cameras and video adapters for analog security cameras.
1.4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all networked security cameras.
1.5	Maintain Asset Inventory Information	Ensure that the camera inventory data include the network address, hardware address, camera firmware version, camera name, camera label, camera location, and whether the camera is approved be on the security network.
1.6	Address Unauthorized Assets	Ensure that unauthorized cameras are either removed from the network, quarantined or the inventory is updated in a timely manner.

CIS Control 2: Inventory and Control of Software Assets

It is important to actively inventory and track all software running on the security network, to detect outdated software versions and remove unauthorized versions. Camera firmware contains the camera's operating system and application software, including web server software. Camera firmware updates can include patches for operating systems, web servers, camera data sets and camera analytics software.

No.	CIS Sub-Control Title	Description
2.1	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized camera firmware that is required for the video surveillance system, based upon camera manufacturer recommendations, compatibility with video management system (VMS) software.
2.2	Ensure Software is Supported by Vendor	Ensure that only firmware versions obtained from the camera's vendor are added to the authorized firmware inventory.
2.5	Track Software Inventory Information	The camera and firmware inventory should be tied into the software inventory so that VMS software, video analytics software on cameras and on servers, and their compatibility are tracked from a single location.

CIS Control 3: Continuous Vulnerability Management

To minimize the windows of opportunity for attackers it is important to continuously acquire, assess, and act on new cybersecurity information to identify vulnerabilities and remediate them. This requires monitoring the product security web pages of vendors of cameras, VMS software, and video analytics software for vulnerability and patch information, and subscribing to their cybersecurity notification lists.

No.	CIS Sub-Control Title	Description
3.4	Deploy Automated Patch Management Tools	Deploy automated firmware update tools to ensure that the latest approved firmware is running on the cameras.

CIS Control 4: Controlled Use of Administrative Privileges

> Misuse of administrative user privileges is a primary cyberattack method.

To effectively control the use of camera user privileges, including administrative privileges, requires a combination of policies, processes and tools to track/control/prevent/correct the use, assignment, and configuration of administrative and other privileges on cameras. The misuse of administrative privileges is a primary method for attackers to spread across an entire network and gain unauthorized access to devices. Attackers who gain access to cameras could re-install older versions of vulnerable firmware and take advantage of security weaknesses that are thought to be remediated. Security officers monitoring cameras, and service providers maintaining them, would not know that the firmware was changed. Preventing such changes from going undetected is one reason to use an automated tool to monitor the status of camera firmware.

No.	CIS Sub-Control Title	Control Descriptions – Revised for Cameras
4.2	Change default passwords	Before deploying any new camera or an existing camera reset to factory default settings, change all default passwords to have values consistent with the password scheme for the cameras.

The security industry's lack of awareness and use of such controls – which are accepted practice in the IT world – is what keeps video surveillance systems highly vulnerable to cyberattacks. It is well past the time to begin adopting proven IT technology management practices, including the use of automated tools, for the protection of electronic physical security systems, especially video surveillance systems. Camera password checking requires a tool because there are many cameras to manage, and unlike a laptop, tablet workstation or server computer, cameras don't have a keyboard and screen interface and are accessed only via the network. In most cases, owners and managers of cameras can't see when they are being accessed. The same goes for camera firmware management, which is performed via the network.

Note that in this paper, "camera" refers to a network camera (IP camera) or an analog camera using a network adapter (media converter) to connect to the network, and "recorder" refers to a VMS recording server or an NVR (network video recorder) appliance.

Camera Password Checking

Required functionality for automated camera password checking would include:

- Discover all networked cameras across all of an organization's facilities
- From each camera retrieve the camera's IP address, hardware address, plus make, model, name or label, location information and software version of its recorder (requires integration with the VMS or NVR software)
- Check each camera for:
  - Commonly used and easily guessable passwords
  - Factory default passwords
- Provide a report of cameras whose passwords should be changed
- Check compliance again after each password change

Camera Firmware Management

Required functionality for maximally automating camera firmware management necessitates integration with the VMS or NVR recording software to eliminate manual data entry, and to reduce manual actions typically needed to perform the tasks listed below, using a "compliance" perspective for maintaining fully updated camera firmware. Management of large-scale deployments requires the capability to upgrade multiple recorders' cameras in parallel, while providing a real-time dashboard status and control display for addressing failed updates or other conditions, such as loss of network connectivity. Thus, safe and secure camera firmware management requires the following functionality.

1. **Inventory Video Surveillance System Infrastructure**
   - Discover all networked cameras and recorders across all of an organization's facilities
   - Extract camera make, model and firmware version information from each camera
   - Match discovered cameras up to their recorder
   - Extract camera information such as name and location from recorders
   - Identify "rogue" cameras − those not enrolled in a recorder
   - Build a "digital twin" model of the organization's video surveillance system infrastructure
   - Identify cameras in need of firmware updates
   - Present firmware inventory report, showing each camera's firmware version and related recorder software version for a compatibility check between the two
   - Provide a status report and/or data view that identifies cameras out of compliance (needing firmware updates)

2. **Retrieve and Test Firmware Update Files**
   - Enable retrieval of official firmware from camera manufacturers, both new versions and existing versions in use, to enable fallback in the event of update failures or problems with new versions
   - Digitally sign and store validated firmware update files
   - Provide a process to perform a test firmware upgrade on each make/model of camera before approving firmware for full distribution, including:
     - Stop recording for camera under test
     - Initiate firmware upgrade
     - If upgrade is unsuccessful reboot camera and restore previous firmware
     - Restart recording for camera under test
   - Mark successful firmware/make/model combinations as approved for use
   - Mark unsuccessful firmware/make/model combinations as unapproved for use

3. **Perform Scheduled Firmware Update Rollout**
   - Provide for defining and scheduling firmware update jobs, enabling bulk updating with:
     - Sequencing of camera updates per recorder
     - Global parallel updating of cameras (i.e. across multiple recorders, multiple facilities, and multiple geographies)
     - Automatic pause of update sequence on an update failure, with manual resumption
     - Manual pause and resume for updated sequences

- Provide status monitoring and reporting for upgrade jobs in progress
- Provide alerts for job completion and for camera update problems, checking infrastructure in real time to determine likely causes (power loss to camera, network segment outage, etc.).

4. **Monitor Firmware Compliance and Success Status**
   - Collect new firmware release data and update inventory to identify newly non-compliant cameras
   - Provide "firmware reversion job" scheduling and execution for a firmware release that turns out to be troublesome and requires fallback, applying only to applicable firmware/make/model combinations
   - Provide compliance reports for auditors
   - Provide trouble issue reports for camera and recorder vendors

The above functionality makes it possible to manage firmware updates safety and efficiently across all of an organization's video surveillance systems, regardless of the size and number of video system deployments.

Assuring Cyber Hygiene and System Performance

Service assurance is the application of policies, processes and tools to rapidly, efficiently and cost-effectively identify, isolate, troubleshoot, and repair problems with devices, computers and networks that impact security system performance. Cybersecurity vulnerabilities are now among the system problems that, once discovered, require immediate correction. Manual processes are not time-feasible or cost-feasible for maintaining video system cyber hygiene and full performance.

Note that system and device malfunctions often constitute physical and/or cybersecurity risks, especially when they require workarounds, temporary alternate protective measures, or compensating risk controls. Such measures usually create new vulnerabilities and exposures that attackers can use to their advantage. This is why near-instant detection of security system problems, coupled with proactive maintenance and service, is required to maintain system cybersecurity hygiene and full system performance.

IT service providers learned long ago that it takes clearly defined processes – combined with automated tools – to successfully manage large-scale electronic systems infrastructure, due in part to the complexities involved in software and firmware version management. Even small-scale systems can be a challenge for a service provider who has hundreds of small-scale systems to manage.

Assessing Automated Tool Solutions

What types of service assurance tools are available to provide security integrators and their customers with visibility into, and control over, the two most difficult aspects of video surveillance system management – password compliance checking and camera firmware version updates? The remainder of this paper considers the three categories of service tools that can help:

- Multi-vendor video-specific solutions
- IT industry general solutions
- Camera and video vendor-specific tools

Tools for video system *service assurance* vary greatly in function and value.

Each category's value relates to the degree to which it improves the cybersecurity profile of video systems, and the manageability of camera firmware updates and proactive system maintenance and service.

The following chart describes the nature of each solution category.

Category	Description
Multi-Vendor Video-Specific	**Video Infrastructure Cognizant.*** Built to deal with the entirety of the video technology infrastructure as a complete system with related multi-vendor component parts, and to focus on the integrity of each video data stream, throughout each stream's life-cycle from its inception at the camera through its network distribution to each video streams retention point, with insight into the performance-critical and compliance-critical functionality of the system infrastructure and its individual devices, with per-camera and aggregated performance KPIs .
IT Industry General	**Network and Computing Device Cognizant**. Built to deal with multi-vendor network and computing infrastructures to detect and report device faults, performance anomalies and performance trends.
Camera and Video Vendor-Specific	**Video Application/Device Cognizant.** Built to inform vendor technical support functions and to alert end users of current and impending application and device faults.

*Cognizant means "fully and insightfully aware."

Multi-Vendor Video-Specific Solution

The highest-value multi-vendor service assurance solution for video systems would be one that is *video infrastructure cognizant* and works with the leading brands of camera, VMS and NVR products. Such an automated multi-vendor solution must be cloud-based for central management of multi-site deployments and for secure off-site storage of infrastructure data (not video images or video metadata) including digital infrastructure model, diagnostics, compliance information and user audit trail data. It would provide both web-browser-based and mobile app-based remote access to application functions.

To be fully effective, its three areas of functionality must include:

- **Automated Service Assurance**
  - Automated Infrastructure Inventory
  - Automated Infrastructure Digital Modeling
  - Change Management Tracking
  - Global Management (Multi-Site, Multi-System)
  - Continuous Problem Detection and Automated Diagnosis
  - Service Ticket System
  - Alerting (Alerts, Warnings, Advisories)
  - Inventory and Status Reporting
  - Video Infrastructure Problem/Solution Knowledge Base
  - Video System Key Performance Indicators
  - Date-placed-in-Service Tracking and Reporting
  - User/Service Provider Authorized Secure Multi-Vendor Access to Diagnostics Data
  - Master Dashboard
  - Key performance indicators (KPIs) for video stream paths, video stream delivery, and per-camera video retention

    - Mobility App
- **Sustainable Cyber Hygiene (the above plus)**
    - Camera Password Checking (Easily Guessable, Default Passwords)
    - Camera Firmware Compliance Tracking
    - Chain-of-Trust Authentication of Firmware Versions
    - Global Schedulable Camera Firmware Updating
- **Audit Compliance**
    - Video Retention Compliance
    - SOX, PCI, SOC 2, NERC CIP, NIST Cybersecurity Framework, NIST 800-53, etc.

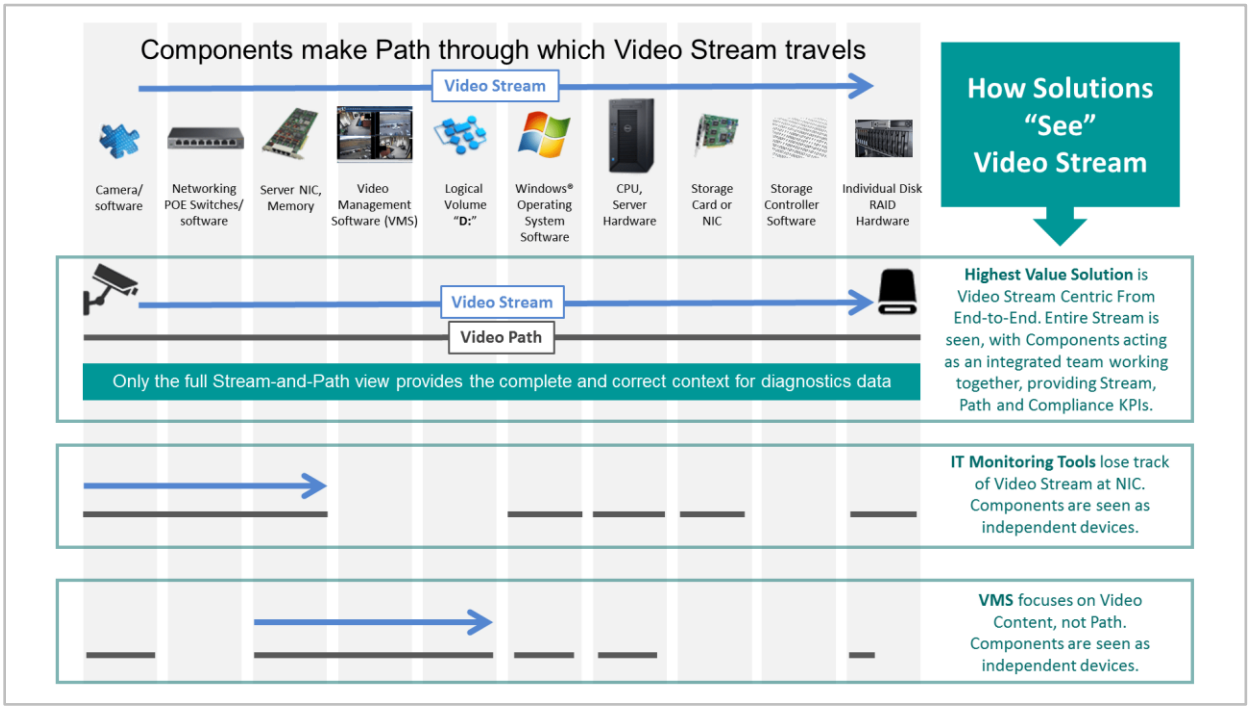
Video Infrastructure Cognizance

The reason that a solution built on IT industry general tools (such as PRTG®, SolarWinds® or WhatsUp® tools) cannot become truly *video infrastructure cognizant* is that its functionality is not designed for it. The degree of helpfulness of such tools is proportional to the degree of setup, configuration, and custom programming work done to label and present their data in video-system-relevant terms. However, such labeling does not change the nature of the data they provide. It still requires considerable work and expertise to connect the dots between the generic network and device diagnostics data and their significance for camera and video management system functionality. The larger the scale of deployment, the more effort such a solution requires.

Tools from camera and video management software vendors are limited primarily to their own products, and thus can't fully encompass the complete video technology infrastructure. They are highly useful for their specific purposes on small-scale systems, but don't scale up well, especially to large multi-site multi-system deployments.

This is illustrated in **Figure 1** below.

Figure 1. Why IT general tools and vendor-specific tools don't provide full Video Infrastructure Cognizance.



Assuring System Cybersecurity and Performance

Strong and comprehensive service assurance capabilities are required to cost-effectively maintain acceptable cybersecurity and performance profiles for security video surveillance systems. This is best done using a multi-vendor highly-scalable solution developed specifically for security video system infrastructure.

About Viakoo

Viakoo Inc. is an Industrial Internet of Things (IoT) company, located in Mountain View, California, USA.

Viakoo's cloud-based offering for service assurance is the first, and to date the only, video-infrastructure-cognizant solution built from the ground up for electronic physical security and IoT systems.

Viakoo automatically verifies performance and integrity of physical security systems and devices while delivering automated proof of their system compliance. Leveraging machine learning and purpose-built algorithms, Viakoo quickly and automatically detects physical security system failures, diagnoses problems, alerts users with repair information, and maintains historical records on operations. With Viakoo, users improve physical surveillance and security reliability and performance, gain critical insight into physical security systems, capture valuable operational performance information, eliminate lapses in security coverage and automate reporting for compliance and auditing.

Viakoo
1100 La Avenida Street
Bldg. B
Mountain View, CA 94043

Tel: (650) 263-8225
Web: www.viakoo.com