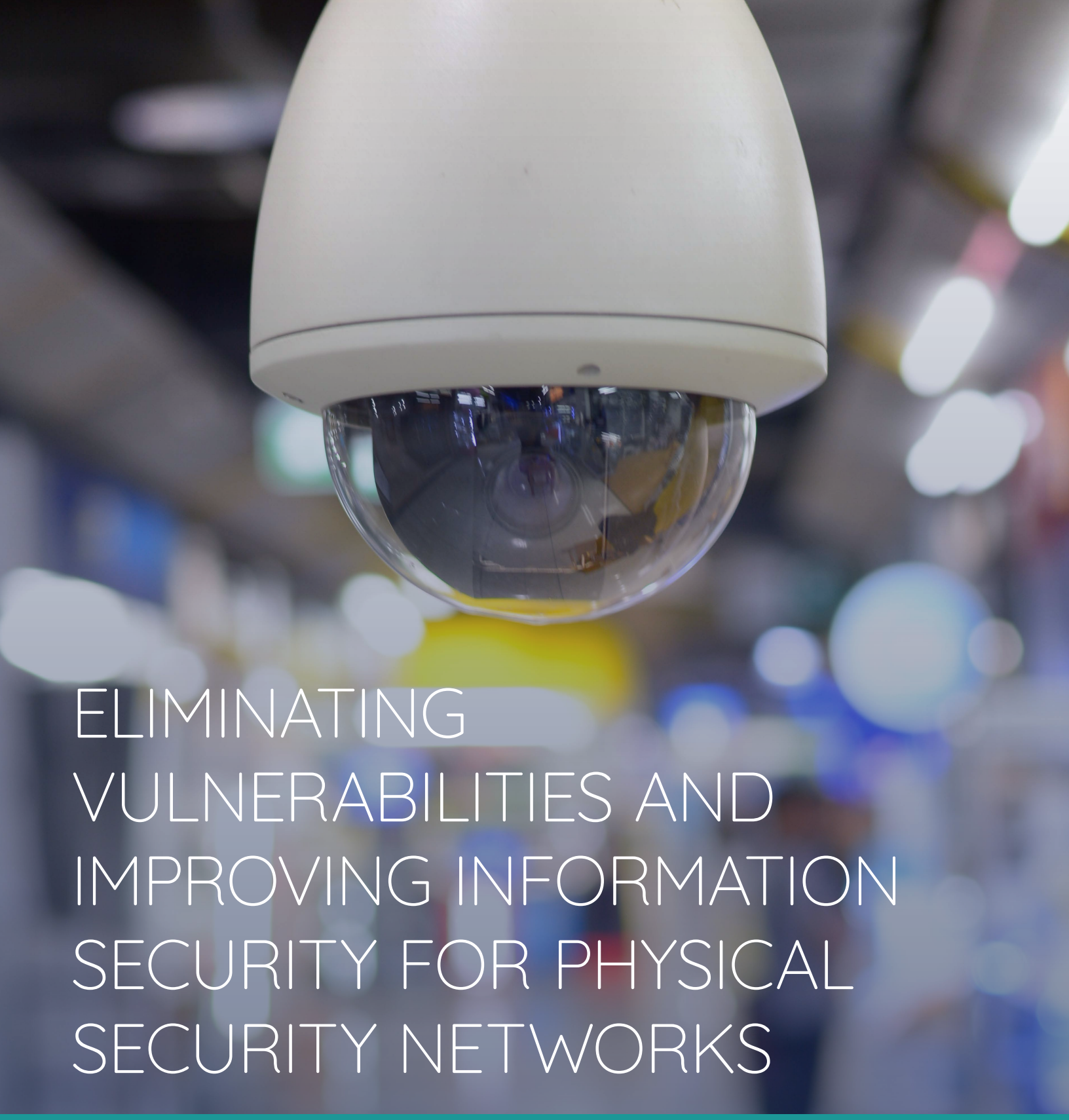


ELIMINATING VULNERABILITIES AND IMPROVING INFORMATION SECURITY FOR PHYSICAL SECURITY NETWORKS

Viakoo

(650) 263-8225 | sales@viakoo.com | viakoo.com

Introduction

Viakoo reduces significant information security vulnerabilities that are unnecessarily created from the common methods of supporting physical security IoT systems.

Viakoo offers customers the first Quality of Service (QoS) metrics for physical security IoT applications, and uniform automated diagnostic methods.

Today, there are few, if any, controls over the system management & diagnostic process, common physical security industry practices are littered with trial-and-error, needle-in-a haystack, and linear troubleshooting that leads to seemingly limitless vendor finger- pointing.

Other specific vulnerabilities that are created include:

- Non-uniform diagnostic data collection leads to misdiagnosis, and costly unnecessary system changes along with prolonged video downtime
- Inefficient diagnostic methods mean extended video downtime and increased enterprise risk
- Lack of purpose-built tools to identify problems with certainty, creates risk
- Ad-hoc use of non standard tools creates security vulnerabilities

THE MYTH OF THE SEPARATE OR "ISOLATED" NETWORK

Today some users think that an "isolated" physical security network means a "protected" network. There was also a time when people mistakenly thought putting money under their mattress was safer than putting it in a bank. Of course that changed when people recognized that a proven, reliable, uniform system was the safer choice.

In fact, isolation can cause behavior that actually increases the risk profile. Isolated networks require contracted service personnel to come onsite:

- Travel-time to the site means increased video downtime; when video is down, enterprise risk is up.
- Access to video networks increases access to video content and related risks of downloading or deletion.
- Repair people can introduce malware on laptops/USB sticks
- Contractors and/or Technicians establishing a VPN for remote electronic access increases the opportunity for a breach.
- No control over who, on the contractor/vendor end, uses the VPN

Isolation isn't really a solution because users let people into their isolated network ultimately, and create information security vulnerability.

NO AUDIT TRAIL IS POSSIBLE TODAY

Ad-hoc, non-standardized methods of diagnosing security video problems are difficult to measure, regulate, and ultimately audit.

- Non-repetitive process cannot be measured or improved over time
- Variables created by the trial-and-error diagnostic method obscure visibility into procedural effectiveness
- Linear problem solving (one vendor after another) increases the number of outsiders with access to sensitive video content

THE VIAKOO SOLUTION

A diagnostic solution that is controlled, consistent, protected, and auditable.

- Eliminates informational truck rolls and the need for production network access
- No VPNs required
- Reduces trouble shooting time and finger pointing among vendors

Viakoo provides a diagnostic representation of your video infrastructure for Collaborative Problem Resolution, without network or video content exposure.

Data Collection and Diagnostics

As shown in Figure 1 Viakoo automatically collects diagnostic metadata from existing IP infrastructures and sends the data to the cloud-based Viakoo service center (or on-premise if desired), via a secure, outbound-only connection.

Once uploaded the diagnostic data is analyzed, looking for anomalies, making correlations, and doing predictive analysis. (Figure 2)

The results of the analysis are delivered to the stakeholder's phone or desktop, using a phone app (Apple and Android and a standard desktop browser. Alerts are sent by an automatic Ticket generation capability that tracks activity and corrective actions.

With Viakoo, users can get reports, charts, and graphs of performance status and trends.

To speed problem resolution, Team Viakoo experts can provide additional live, in-depth diagnostic analysis beyond that provided automatically.

Figure 1. Viakoo Overview

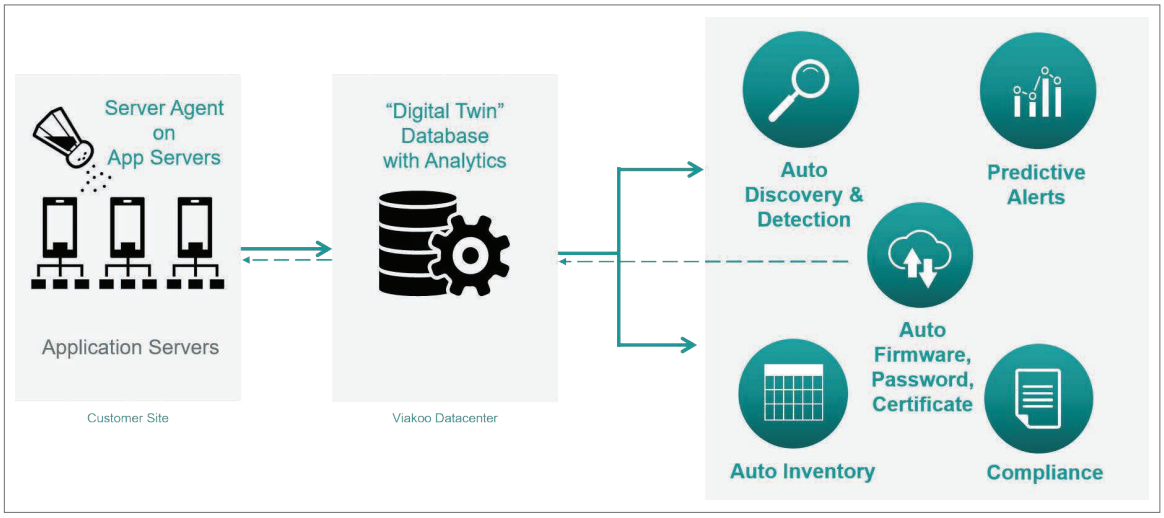
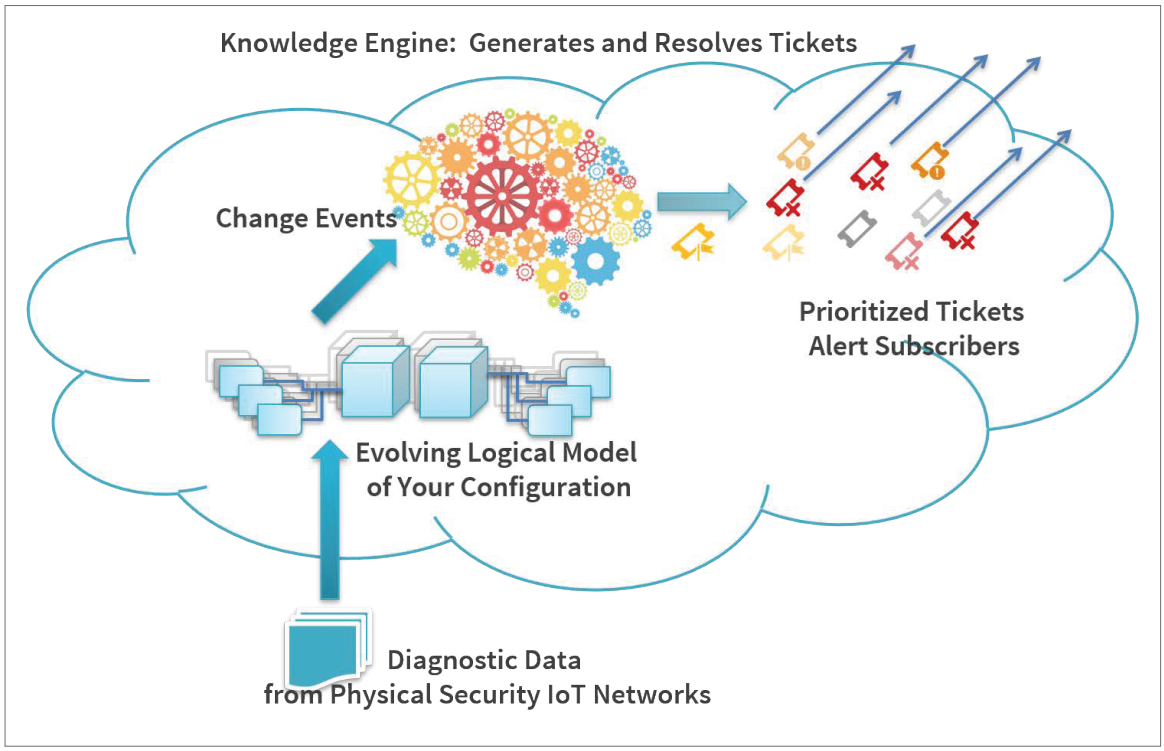


Figure 2. Viakoo Cloud/On-Premises Architecture



Key Security Measures

Table 1 presents the key elements that make Viakoo implementations a safe & secure way to provide a unique set of capabilities that help your physical security IoT infrastructure work properly, fulfilling its mission to provide situational awareness and maintain the video evidence recorded for the full duration intended. Viakoo was built with a secure architecture that establishes layers of defense to safeguard the data it collects and ensure Viakoo's continuous operation.

Table 1. Overview of Viakoo Security Measures

Security Measure	Details	Benefits
No Video Content, Diagnostic Data ONLY	Only diagnostic data are collected to determine Video Path Uptime, Video Stream delivery quality, and Video Retention Compliance.	NO VIDEO CONTENT is touched by Viakoo.
Outbound-ONLY Connectivity Required	Diagnostic data is automatically transferred every 20 minutes (a user-configurable interval) or upon demand by user.	Limited network connectivity to Viakoo, no persistent connections. **Viakoo requires Outbound-ONLY connections over HTTPS Port 443.** No connection INTO customer premise can be initiated by Viakoo.
No VPN Needed	HTTPS secure connections are used (i.e. connection on standard HTTPS port 443). Secure connection is automatic requiring no manual steps. Standard port usage requires no special port configurations.	Risk due to VPN exposure is ELIMINATED.
Encrypted Diagnostic Data Transport	▸ AES 256-bit encryption authenticated using 2048-bit RSA key ▸ Digitally signed by DigiCert High Assurance Certificate Authority	Encryption means that data cannot be deciphered even if breached.
Viakoo Secure Service Architecture (SaaS)	▸ Role-based access privileges ▸ Multi-tenant data architecture ▸ Multi-layered firewall ▸ Data secured in virtual private cloud with only highly secured external access points.	Data collected by Viakoo is strictly controlled. Only customer-authorized users are able see all or part of the data— depending upon their assigned roles.
Digitally Signed Software Agents	The Agent installation packages and updates for the Viakoo software Agents are digitally signed.	This best practice assures that the software was indeed issued by Viakoo and that it has not been altered or corrupted since it was issued.