SECURITY INDUSTRY ASSOCIATION

SIAWEBINARS
Info for the Security Industry

Serving Healthcare Remotely, Efficiently and Securely

April 2, 2020

SIAWEBINARS
Info for the Security Industry

Serving Healthcare Remotely, Efficiently, and Securely

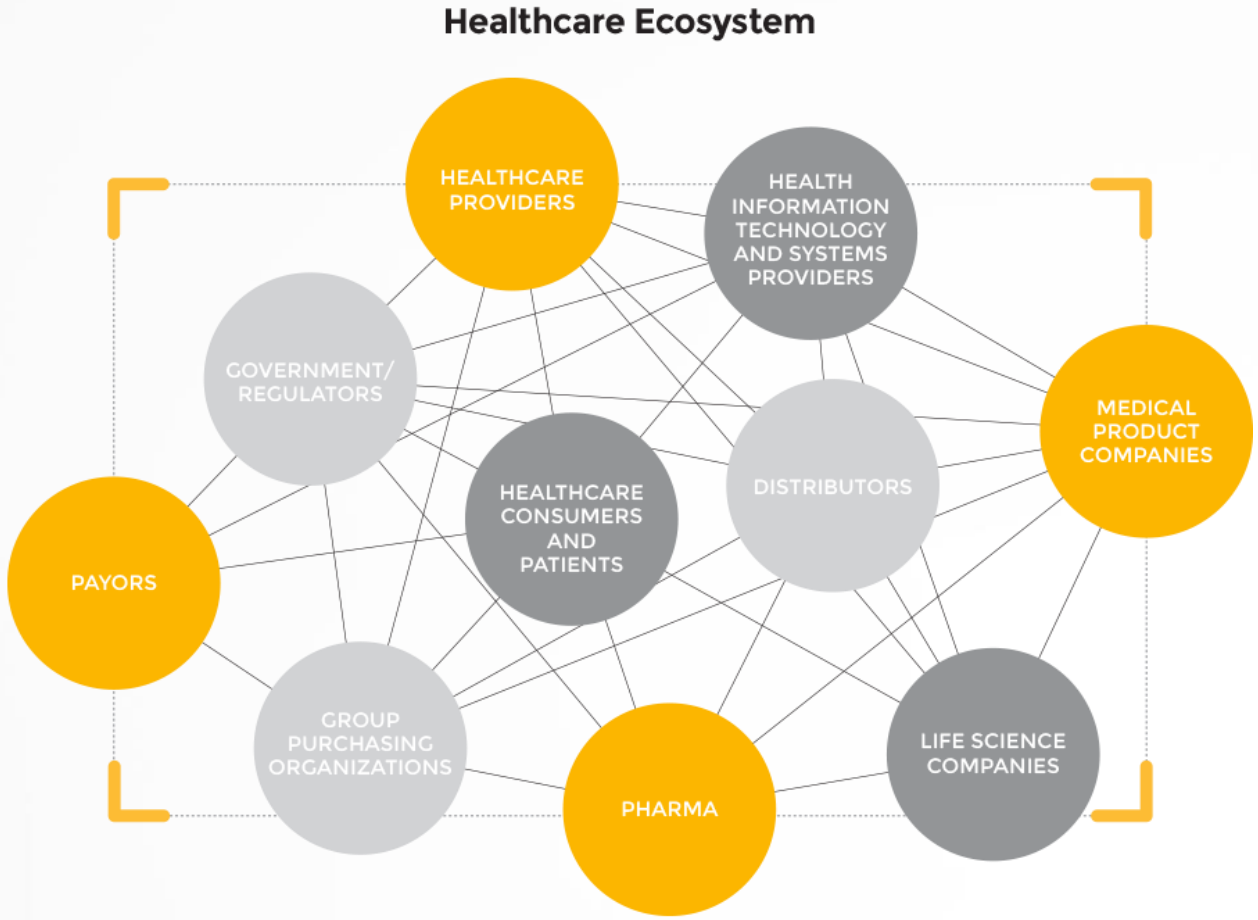
John Gallagher
Vice President
Viakoo, Inc.

VIAKOO

Learning Objectives

- Unique Needs of Healthcare Organizations
- Risk/Compliance/Administration
- Newly Emerging Requirements (firmware, passwords, certs)
- Selling Better
- Enabling Digital Connection
- Timing/Detect/Diagnose/Recommend
- How to Improve Efficiencies

Differing Needs

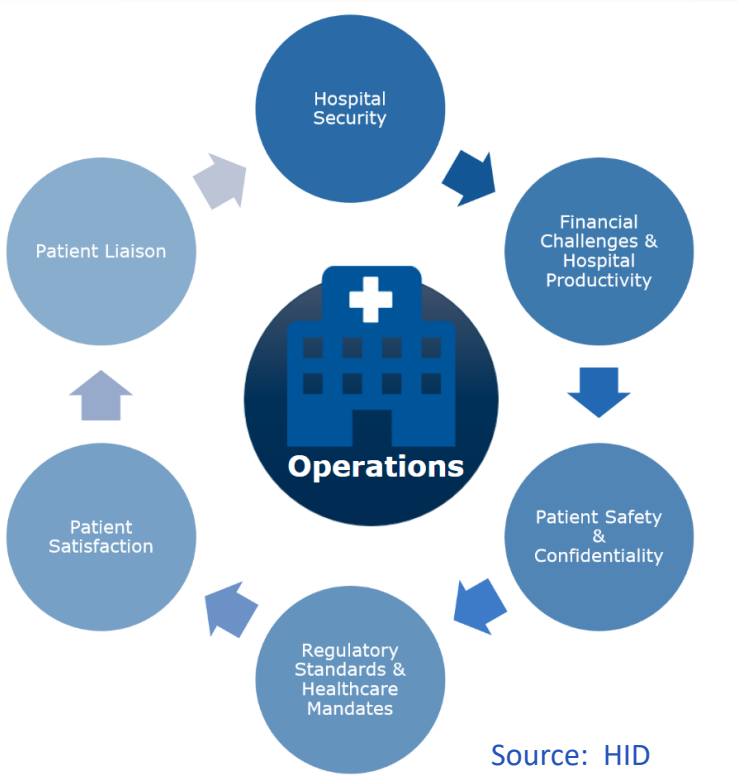


- Broad Ecosystem
  - Not “one-size-fits-all”
- Driven By:
  - Patient Outcomes
  - Employee Safety
  - Cyber Security
  - Compliance/Audit
  - CMS Directives
  - Joint Commision
  - …. (many others)

Requirement: Security for employees, medical staff, patients, visitors, contractors, materials, and vendors from entry to exit

Key Operational Considerations

- Many Specialized Areas:
  - Emergency, Neo-natal, ICU, Pharmacy, Inventory Control, Parking Lots, etc.
  - Each with unique security requirements
- Security with Many Moving Pieces
  - Need to credential/onboard new and visiting staff
  - Many onsite workers
  - Open access
- Audit/Compliance
  - Joint Commission
  - Cyber/physical issues → HIPAA



Source: HID

Typical Security Concerns

- Loss of high-value medical equipment and assets; internal or external theft
- Access, use and theft of drugs and other pharmaceutical items
- Securing ‘hot labs’ with nuclear medicines used for radiation
- Workplace, domestic or street violence
- **Patient elopement, accountability**
- Illegal parking
- Infant abduction
- Vandalism
- Liability

Source: Security Today, March 2019

What Helps?

- Reducing cost of Physical Security
- Reducing complexity of physical security
- Eliminating manual processes, like data entry
- Avoiding sending people onsite
- Centralized/streamlined management
- Proof of operational performance
  - Audit, employee retention, etc.

Emerging Needs

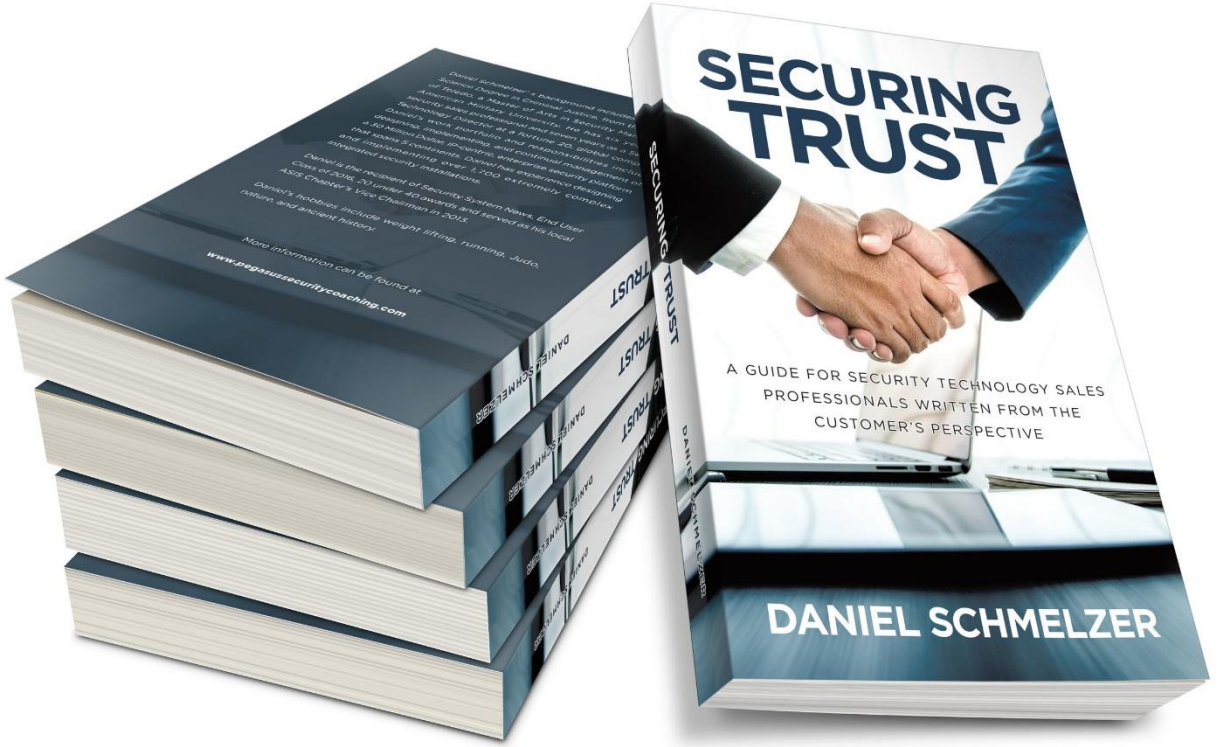
- Healthcare Physical Security is functionally IoT, which brings
  - Security issues (security cameras #2 most successful attack method)
  - Lifecycle management
- Drives new requirements
  - Need for comprehensive management of firmware updates, password management, device-level certificates
  - Tight integration with IT and other systems

Selling into Healthcare

- Where Integrators/Consultants Should Focus:
  - How to help your customers sell internally (different constituencies)
  - Structuring proposals better (outline business case)
  - Demonstrating ROI ***early***
  - Connecting with IT ***early***
  - Tangible, measurable goals
  - Automation

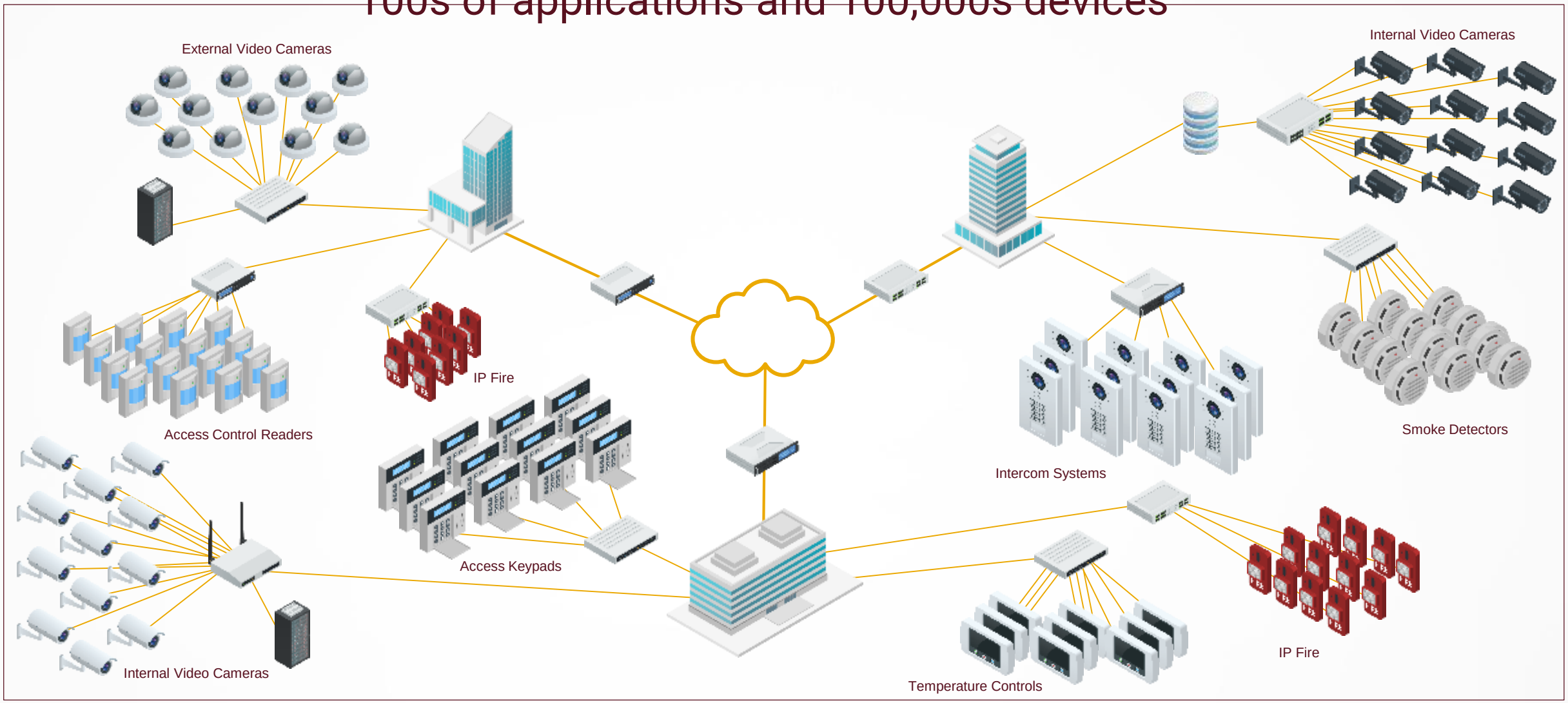
Learn from Dan

- A Guide for Security Technology Sales Professionals
- pegasussecuritycoaching.com
- This is an e- book written by Daniel Schmelzer with the purpose of equipping security sales professionals with the tools and knowledge needed to enhance the relationship between a vendor and the customer.
- First five people to email me at john.gallagher@viakoo.com will get free electronic copy

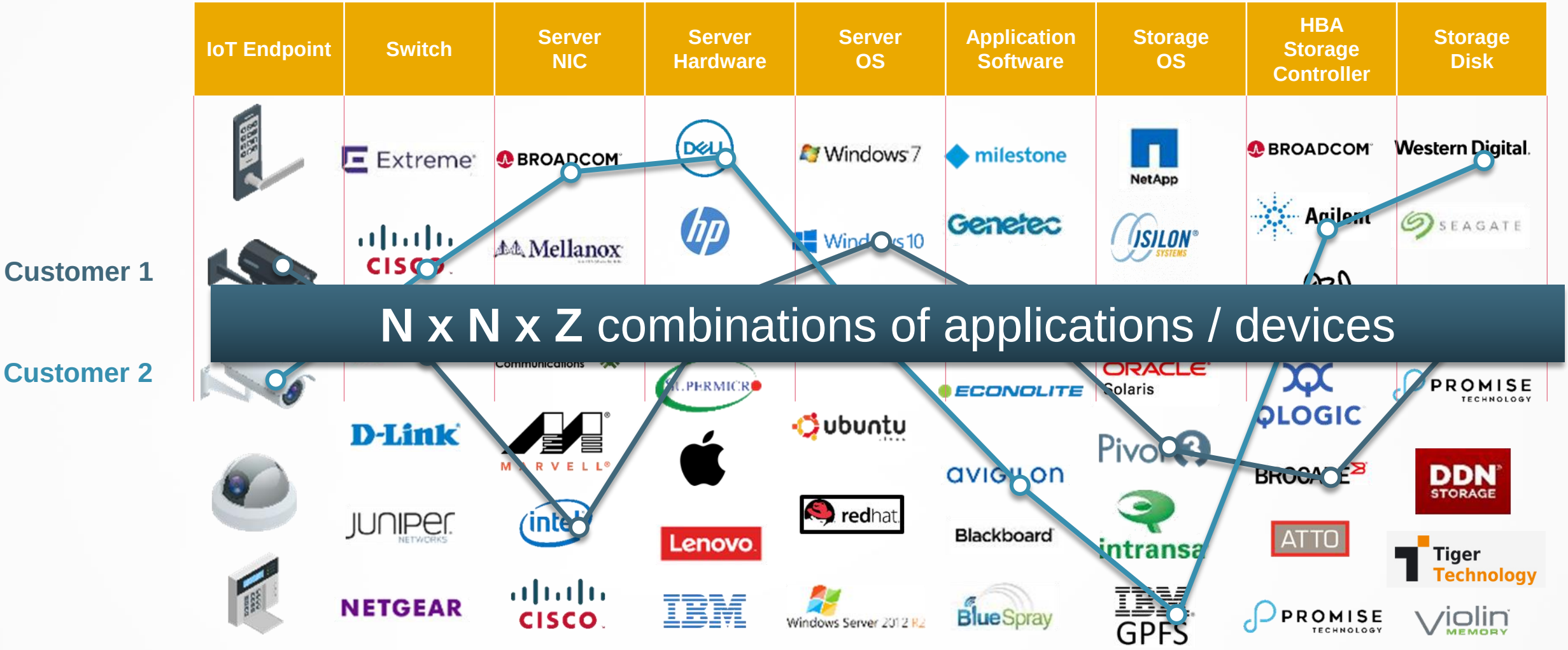


Complex, Unmonitored and Vulnerable

100s of applications and 100,000s devices



End-to-end monitoring is required and complex



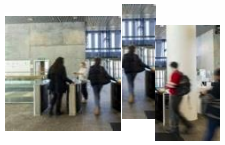
Obvious/Basic vs. Subtle

Dead Cameras

Overheating

Failed Hard Drives

Symptom has Few Possible Causes



Not recording

Missing Data

Retention

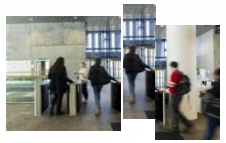
Quality Issues

Numerous Direct and Indirect Causes

What We Can Eliminate with Digital Connection

HIGH COST MAINTENANCE

Not recording



Missing Data

Retention

Quality Issues

Symptom Many Have Numerous Direct and Indirect Causes

Don’t Go There: Fix It Remote

Manual Reactive Service

Customer finds the Problem

Problem detection

Roll a truck

Access to log data

Manually troubleshoot/ Fix-it plan

Root cause diagnosis

Do the repair

80% of time/cost

20% of time/cost

Proactive Service

Automated detection

Continuous diagnostics

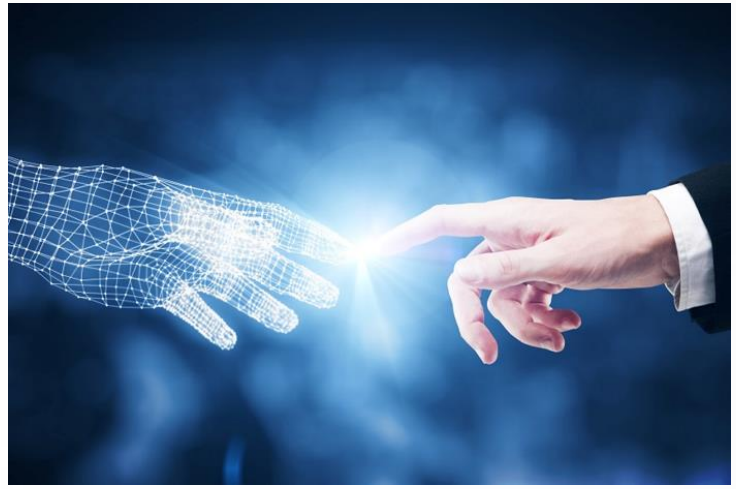
Tells you how to fix it

Saves Time / Removes Cost

74% Remote problem resolution

Digital Twin Technology Advantage

- Virtual representation
- Predictive System Analytics
- Secure access
- Collaborative Problem Resolution
- Virtual Preventative Maintenance



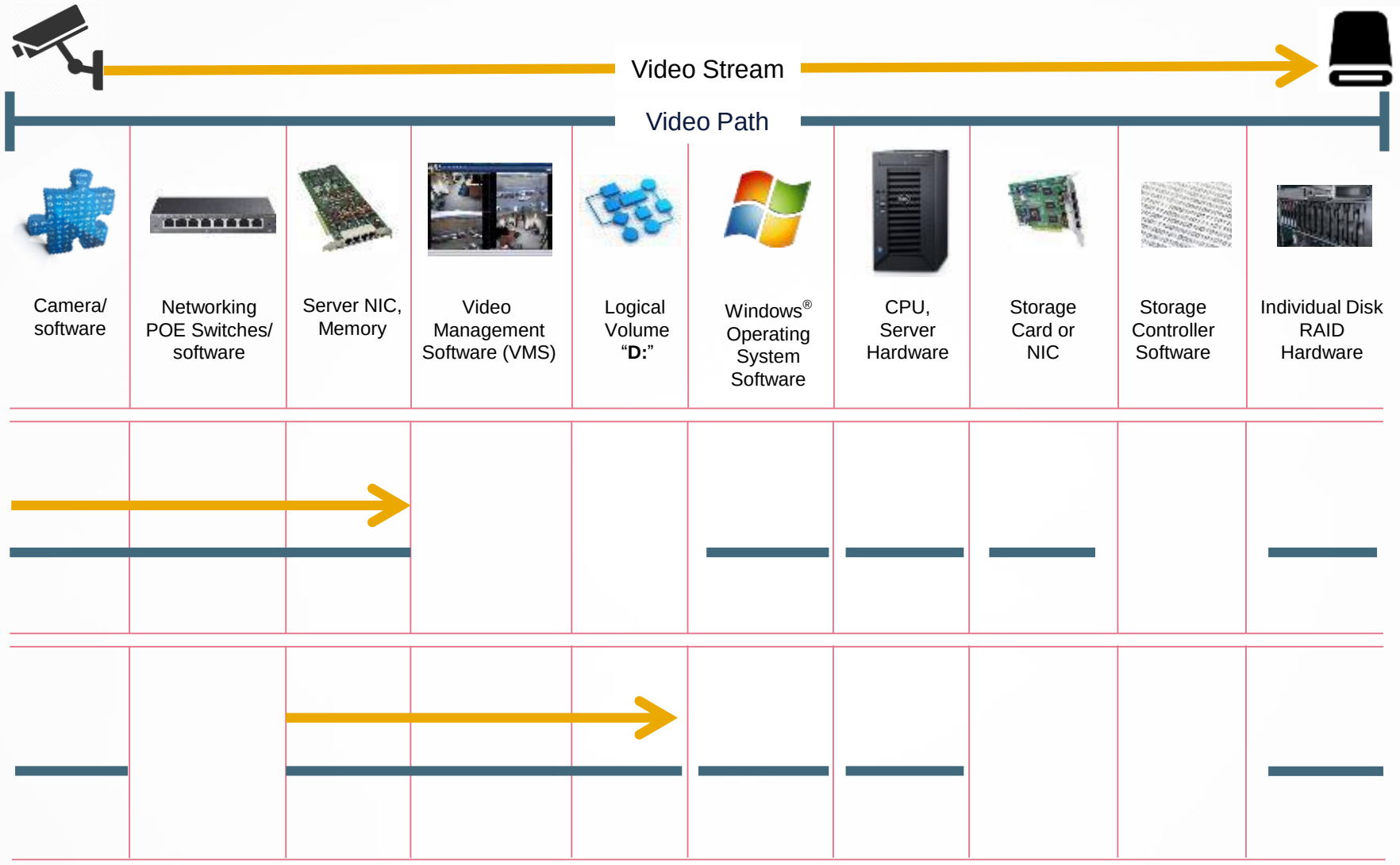
What's is a digital twin and what's it for?

A digital twin is **a virtual representation of a product**. It can be used in product design, simulation, monitoring, optimization and servicing and is an important concept in the industrial Internet of Things.

What can a digital twin do for You?

In short, a **digital twin** is a dynamic software model of a physical thing or system. Its purpose is to analyze and simulate real-world conditions, anticipate response to changes and improve operations to add more value for the end-user.

End-to-end is the best way to solve the problem



IoT Application Level
is end-to-end application centric

Components are seen with Stream as an **integrated team** working together.

Device Monitors
like Solarwinds lose track of stream at NIC. Components are seen as independent **devices**.

Content Managers
focus on content, not path. Components are seen as independent **devices**.

Example of Maintenance Contract SOW

- **Monthly**
  - Review of network monitoring reports
- **Quarterly**
  - Place a telephone call to the End User to obtain feedback about their ongoing system experience with the system i n terms of performance and functionality.
  - Physical inspection of all cameras
  - Cleaning of all outdoor cameras
  - Physical inspection of server room equipment
  - Field of View (FoV) review for all cameras, including greenery check for outdoor cameras, and nighttime lighting ch eck for outdoor cameras.
- **Semi-Annual**
  - Physical inspection of all indoor cameras
  - Cleaning of all indoor cameras
  - Quality review of live camera images, and recorded camera day and night images
- **Annual**
  - Provide annual scheduled and non-scheduled maintenance summary report, along with any recommendations pro mpted by the report contents.

What Can Be Virtualized

- **Monthly**
  - Review of network monitoring reports
- **Quarterly**
  - Place a telephone call to the End User to obtain feedback about their ongoing syste m experience with the system in terms of performance and functionality.
  - Physical inspection of all cameras
  - Cleaning of all outdoor cameras
  - Physical inspection of server room equipment
  - Field of View (FoV) review for all cameras, including greenery check for outdoor ca meras, and nighttime lighting check for outdoor cameras.
- **Semi-Annual**
  - Physical inspection of all indoor cameras
  - Cleaning of all indoor cameras
  - Quality review of live camera images, and recorded camera day and night images
- **Annual**
  - Provide annual scheduled and non-scheduled maintenance summary report, along with any recommendations prompted by the report contents.

Digital Connection & Analytics

Future (AI/ML)

Example: Hard Drive Maintenance

○ Hard Drive Maintenance	Problem detection/root cause	Automated Fault Detection means no longer relying on end users to find the problems, but rather software to continually, systematically check the integrity of the infrastructure, end-to-end, all subsystems, hardware and software, detecting anomalies and determining their causes and remedies. • Automated Alerts means getting notification reliably and immediately, so that proactive steps can be taken to resolve problems before end users are even aware of them. • Automated Diagnostics analyze all available information to detect and predict likely faults in equipment. It advises management, operators and maintenance personnel of when actions to prevent equipment failures. • Service Assurance automation eliminates Manual Analysis and Trial-and-Error approaches by automatically collecting and providing diagnostics data and the likely Root Cause. This will eliminate between two-thirds to three-quarters of the hourly service call costs – related to break fix - service repair/invoices

Example: Documented Failures

- Time and cost per device for documentation

• Documentation to be provided noting any failures of equipment	Standard reports	Automated diagnostics eliminate most of the inspection work that is currently performed. Up-to-date accurate dashboard displays and on-demand reporting enable accurate decision-making and planning. Corporate policies exist to direct the decisions and efforts of personnel in support of organizational objectives. • Accurate records enable compliance verification. • Self-updating records provide an always-accurate means of verifying compliance. Manually updated records provide infrequent status snapshots, which are insufficient for verifying that compliance status is fully maintained with no lapses. • Automation enables continual compliance status awareness, and supports Alerting on specific compliance lapses anywhere within the global electronic security systems infrastructure. • Metrics for security systems infrastructure would include video network path uptime from an end device to its server, per-video-stream recording success, and video retention as relates to corporate policy and governmental regulations	Automated diagnostics eliminate most of the inspection work that is currently performed.

Example: Device Testing

- Estimated testing cost per device

• All systems need to be tested to assure communicating and functioning properly	End to End diagnostics Every 20minutes 24x7	Cost savings stem from replacing inefficient and less-effective manual processes, with automated knowledge-based detection and diagnostics. Automated diagnosis is performed against a technology knowledgebase, and is more accurate and comprehensive than technician-based diagnosis done against the technician's personal experience or the experience of a technical team. With full diagnostics information at their fingertips, the best talent can be leveraged from anywhere-anytime. The need for a specialist to travel to a site location is significantly reduced or eliminated. Service Assurance automation will reduce the video check interval from 7 days down to 20 minutes. This will eliminate 99% of the current multi-day liability risk that stems from offline cameras and recording failures remaining undiscovered for up to 7 days.	Cost savings stem **from replacing inefficient and less-effective manual processes,** with automated knowledge-based detection and diagnostics. Automated diagnosis is performed against a technology knowledgebase, and is more accurate and comprehensive than technician-based diagnosis done against the technician's personal experience or the experience of a technical team.

Can be Done Virtually: Test & Inspect

Scope of Work for Preventive Maintenance on all Security Equipment to Include:	Virtual PM Capable	Details	Details
Clean, Test and Inspect all equipment listed	Test and Inspect	The heart of Service Assurance is a database of records, a digital model of the actual video infrastructure, detailing all components and their current status and historical status. These records are the source of automated dashboard displays, as well as informational and actionable reports. • Automated reporting and alerting reduce MTTR and eliminate errors that would occur from acting on incomplete or inaccurate information. • They also help keep IT infrastructure personnel informed of both network-impacting security system conditions and security-system-impacting network-conditions. • Predictive analytics provides a framework to analyze data over time, leading to improved corrective and ad hoc preventive actions, and potentially to preemptive actions based upon historical patterns, such as when to replace a piece of outdoor equipment before it fails, reducing unplanned and lengthy downtime to planned and miniscule downtime	The heart of Service Assurance is a database of records, a digital model of the actual video infrastructure, detailing all components and their current status and historical status. These records are the source of automated dashboard displays, as well as informational and actionable reports. Automated reporting and alerting reduce MTTR and eliminate errors that would occur from acting on incomplete or inaccurate information. They also help keep IT infrastructure personnel informed of both network-impacting security system conditions and security-system-impacting network-conditions.

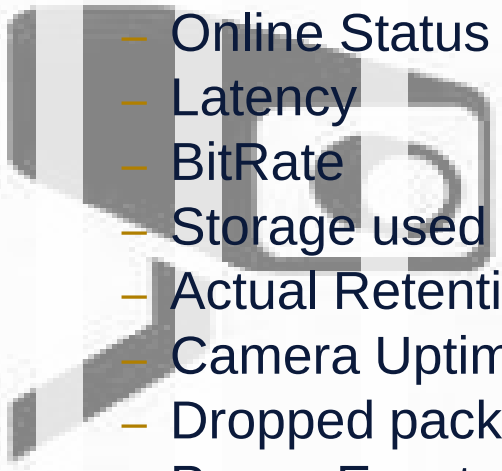
Why not already? Why is this so hard?

Distributed Configuration
Chaotic Loads
Changing Environments
Chains of Components
Varying People and Tools
Organizational Relationships
Absence of Information

To Diagnose Video Stream Issues, You Need

Configuration

- Name
- IP
- MAC
- Frame Rate
- Codec
- Resolution
- FW Version
- Retention Goal
- Power Requirements



- Performance
  - Online Status
  - Latency
  - BitRate
  - Storage used
  - Actual Retention
  - Camera Uptime
  - Dropped packet events
  - Power Events
  - From Camera bitrate

- VMS Settings
  - Driver Compatibility
  - Motion Settings
  - Port / Password Settings

Digital Connection Reduces Maintenance Costs

- Virtualizing Preventative Maintenance
  - All remote except cleaning lenses
- Informational Truck Rolls
  - since all information is in tech's hands
- Needless Travel
  - by your best technicians
- Rip & Replace
  - caused by mis-diagnosis and "guesswork"
- Lengthy Problem Resolutions
  - traditionally taken days, week, or even months
- Elimination of Finger-Pointing
  - causing delays, downtime, and cost

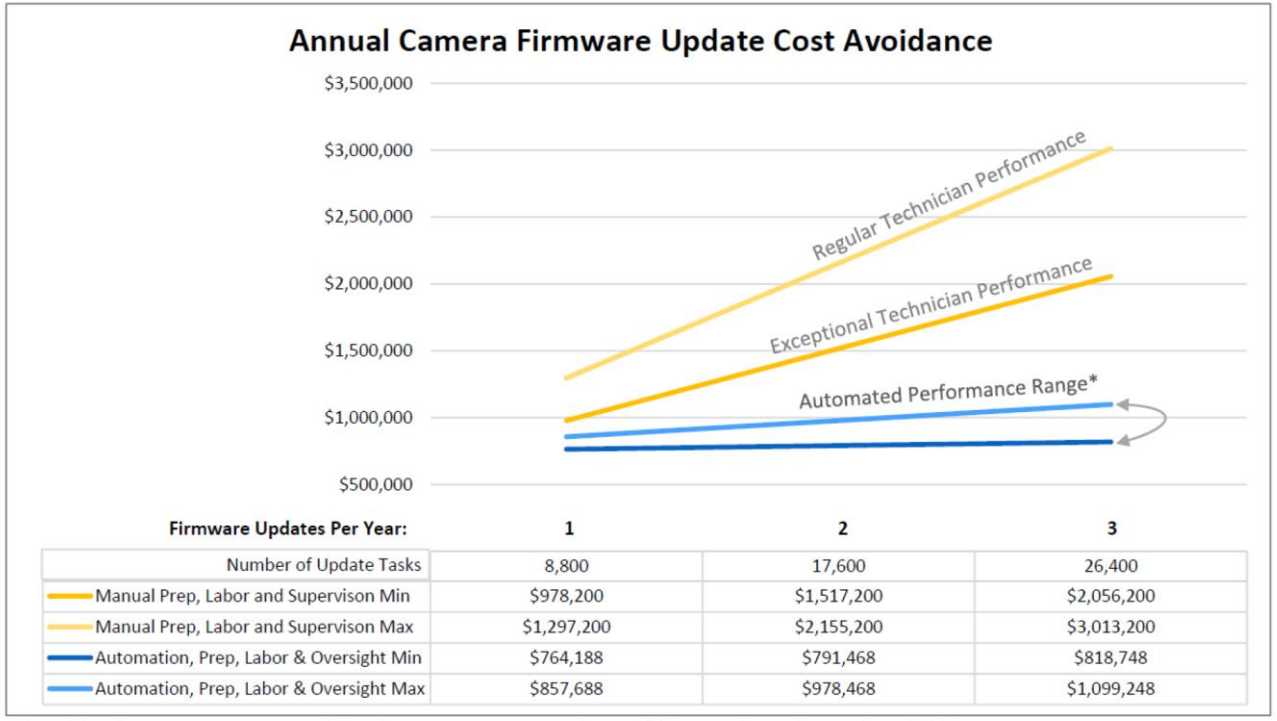
Can’t be Done Virtually: Physical Maintenance

- Cleaning
- Device Replacement
- Discussion and Storytelling
- Goodwill

Emerging Requirements Addressed By Automation

- Cyber Hygiene
  - Firmware Upgrades
  - Password Management
  - Certificate Management
- Compliance/Audit Support
  - Push-button reporting
  - Compliance-as-a-Service

Figure 1. Automation confines camera firmware update costs to a reasonable range.



Firmware Updates Per Year:	1	2	3
Number of Update Tasks	8,800	17,600	26,400
Manual Prep, Labor and Supervison Min	$978,200	$1,517,200	$2,056,200
Manual Prep, Labor and Supervison Max	$1,297,200	$2,155,200	$3,013,200
Automation, Prep, Labor & Oversight Min	$764,188	$791,468	$818,748
Automation, Prep, Labor & Oversight Max	$857,688	$978,468	$1,099,248

*Based on how many automated simultaneous camera updates will be monitored by each technician.

Moving from manual management to automatio n reduces time, cost, and risk

Access control

Video cameras

Power supplies

Humans & Hardware

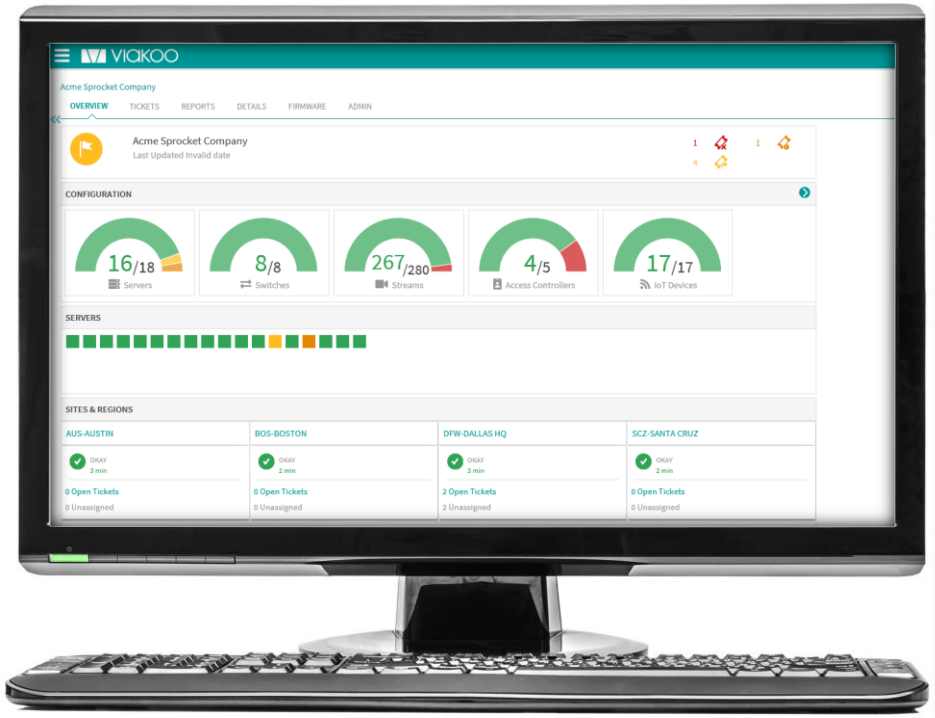
Managing IoT

Code Blue

Visitor kiosks

Intercoms

Automation



Questions?

Post-webinar questions or follow-up:

john.gallagher@viakoo.com