
# What's new?

## Trends that influence surveillance

BICSI MIDDLE EAST & AFRICA

# Cybersecurity

Bicsi
MIDDLE EAST
& AFRICA

# Threats…

AXIS COMMUNICATIONS

**Vulnerability Report**

*Lund, Sweden July 5, 2016*

**CVE-2016-AXIS-0705 Remote Format String**

**Overview:**

An independent researcher discovered a critical vulnerability that makes it po
attacker to gain root access to certain Axis products without authentication.
very advanced and the researcher intends to publish full disclosure on July 18th

**External sources:**

The external disclosure is due July 18th
*Note: This CVE will be updated once the exploit is disclosed.*

**Affected products and firmware:**

AXIS Network Cameras firmware versions between 5.20 and to 6.20.
AXIS Network Door Controllers firmware versions before 1.45.0
AXIS Network Video Door Stations firmware versions before 5.85.1.2
AXIS Network I/O Relay Modules firmware versions before 1.00.0.1
AXIS Network Horn Speakers firmware versions before 1.20.2

**Impact on systems and users:**

An attacker needs to have network access to products in order to ex
Affected Axis devices that are exposed directly to the Internet are at
includes products that are behind a router/firewall where port-f
traversal has been enabled.
Devices that are behind a protected network are at low risk. Networ
AVHS (AXIS Video Hosting System) are at low risk. Network
Camera Companion solution are at low risk, as the remote conn
expose cameras to direct Internet access.

**Axis recommendations:**

Axis strongly recommends to upgrade products at high risk. A
products in low risk in a scheduled and controlled manner.

**Service Release:**

List of available service releases can be found at
http://origin-www.axis.com/ftp/pub_soft/MPQT/SR/service-rel

**Axis Communications AB**, Emdalavägen 14, SE-223 69
Tel: +46 46 272 18 00, Fax: +46 46 13 61 30, www.axis.com
Vat.No. SE 556253-614301

SECURITY WEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Subscribe (Free) | CISO Forum 201

Malware & Threats | Cybercrime | Mobile & Wireless | Risk & Compliance | Security Architecture | Manager

Home › Malware

## Mirai Botnet Infects Devices in 164 Countries

By Ionut Arghire on October 28, 2016

Share 81 G+1 13 Tweet Rekommendera 5! RSS

**Mirai, the infamous botnet used in the recent massive distributed denial of service (DDoS) attacks against Brian Krebs' blog and Dyn's DNS infrastructure, has ensnared Internet of Things (IoT) devices in 164 countries, researchers say.**

In early October, Mirai's developer **released the malware's source code** and also revealed that there were over 300,000 devices infected with it. Soon after, as the botnet was **increasingly used** in DDoS attacks, Flashpoint security researchers determined that **over half a million IoT devices** worldwide were vulnerable to Mirai, because they were protected by **weak security credentials**.

According to Imperva researchers, the investigation of an attack carried out in August has revealed around 49,657 unique IPs hosting Mirai-infected devices, mostly CCTV cameras, already proven popular targets for IoT botnets.

These IP addresses, researchers say, are located in 164 countries, with Vietnam taking the top spot at 12.8%, followed by Brazil at 11.8%, the United States at 10.9%, China at 8.8%, and Mexico at 8.4%. South Korea, Taiwan, Russia, Romania and Colombia are rounding up top ten most affected countries. Remote locations such as Montenegro, Tajikistan and Somalia were also among the affected countries.

Imperva also notes that a few new Mirai-powered attacks were seen after the source code emerged online, though they were low-volume application layer HTTP floods. These used a small number of source IPs, and the security researchers suggest that they might be mere experimental first steps of new Mirai users.

The researchers also note that the botnet's command and control (C&C) code is coded in Go, while the bots are coded in C. Code analysis also revealed that the botnet was built for two main purposes: find and compromise devices to increase the botnet's footprint, and launch DDoS attacks based on received instructions.

THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life

TECH | CONSUMER TECHNOLOGY

## Hackers Infect Army of Cameras, DVRs for Massive In Attacks

Hacking shows vulnerability of internet devices, security experts say

ntrol of home security cameras and video recorders to launch one of the biggest internet attacks in history this month.
ted attack raised questions about how the internet will cope with a flood of connected and vulnerable devices expected
n the next few years. Photo: iStock

REW FITZGERALD
ed Sept. 30, 2016 3:11 p.m. ET

138 COMMENTS

ers used an army of hijacked security cameras and video recorders to launch
massive internet attacks last week, prompting fresh concern about the
bility of millions of "smart" devicesin homes and businesses connected to the

lts raised eyebrows among security experts both for their size and for the
that made them happen. The attackers used as many as one million Chinese-
ity cameras, digital video recorders and other infected devices to generate
uests and data that knocked their targets offline, security experts said. It is
her the attackers had access to video feeds from the devices.

d include French web hosting provider OVH and U.S. security researcher
hose website was disabled temporarily.

Recommended Videos

1. Weekend Sip: Macallan's New Scotch for Millennials
2. Donald Trump's Long List for Secretary of State
3. LA Auto Show: Five Things to Watch
4. In Nod to Trump, Ford to Keep some Factory Work in U.S.
5. Scientists Reveal Biblical Text From Ancient Scroll

Most Popular Articles

1. Reckoning With 'The Big One' in California—and It Just Got Bigger
2. Venezuela's Nemesis Is a Hardware Salesman at Home Depot in Alabama
3. Romney Is Under 'Active Consideration' to Be Secretary of State
4. Pentagon, Intelligence Chiefs Push to Oust NSA Director
5. How to Fight Amazon.com, Best Buy-Style

HACKREAD
Security is a myth

HACKING NEWS | TECH | CYBER CRIME | HOW TO | CYBER EVENTS | SECURITY | SURVEILLAN


YAHOO HACKED: MORE THAN 1 BILLION USER ACCOUNTS IMPACTED

FBI BUST INDIAN STUDENT FOR CONDUCTING DDOS ATTACKS ON A CHAT SITE

MEET 'LEGION HACKING GROUP' HACKING BIGWIGS OF INDIA

LOW-COST ANDROID SMARTPHONES SHIPPED WITH MALICIOUS FIRMWARE

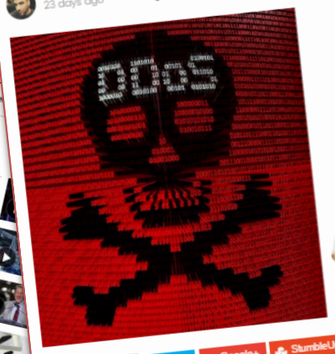
KFC'S SCHEM MEMB

HACKING NEWS | SECURITY

## $55 surveillance camera hacked by Mirai botnet within 98 seconds

Robert Stephens bought the camera from Amazon for testing purposes

by Waqas 23 days ago | Email | @hackread



Facebook | Twitter | Google+ | StumbleUpon | Reddit

The Internet of Things has become more of a joke lately because of the never ending styles of exploitation that these poor devices are being subjected to by malicious cybercriminals and hackers. It is now widely believed that the IoT devices are seriously prone to cyber attacks as their various inherent vulnerabilities make them easy targets for attackers.

**Must Read:** Creepy website shows live footage from 73,000 Private Security Cameras

The latest flaw in the severely hyped IoT devices was discovered by a tech industry veteran Robert Stephens, who identified that his security camera could be compromised within 98 seconds only as soon as it gets connected to Wi-Fi.

Bicsi
MIDDLE EAST & AFRICA

# Recent Threats

## Ransomware (Incident May 2017)

- Ransomware is a version of WannaCry virus
- Malware that locks users files unless a sum is paid using virtual Bitcoin
- Attacked on Washington DC Police 2016
- Britain National Health Hospital May12, 2017
- Affected 99 countries, 75 thousand detection


Bicsi MIDDLE EAST & AFRICA

**A secure system calls for active participation by the entire supply chain and the end users**

Partners in protection

Bicsi MIDDLE EAST & AFRICA

# IP landscape –Video surveillance perspective

# SOLUTIONS ARE MADE OF PRODUCTS

# Total Integrated Solution

**AXIS Camera Station**

*CCTV, Door Station, Access Control management*

Power

Monitor - DVI

Power

*Shutters, Plant, Lighting, Alarm Panels etc*

Inputs

Outputs

**3rd Party hardware integration**

**CCTV Cameras**

**Audio Communication**

**Visitor Management**

*A8004 connected to Door Lock or integrated into Access Control*

**Access Control**

*A1001 connected to Door Lock, Control Reader, Request to Exit.*

CAT5/6 Cables

**POE Switch**

*A UPS can provide power redundancy to connected devices*

Power

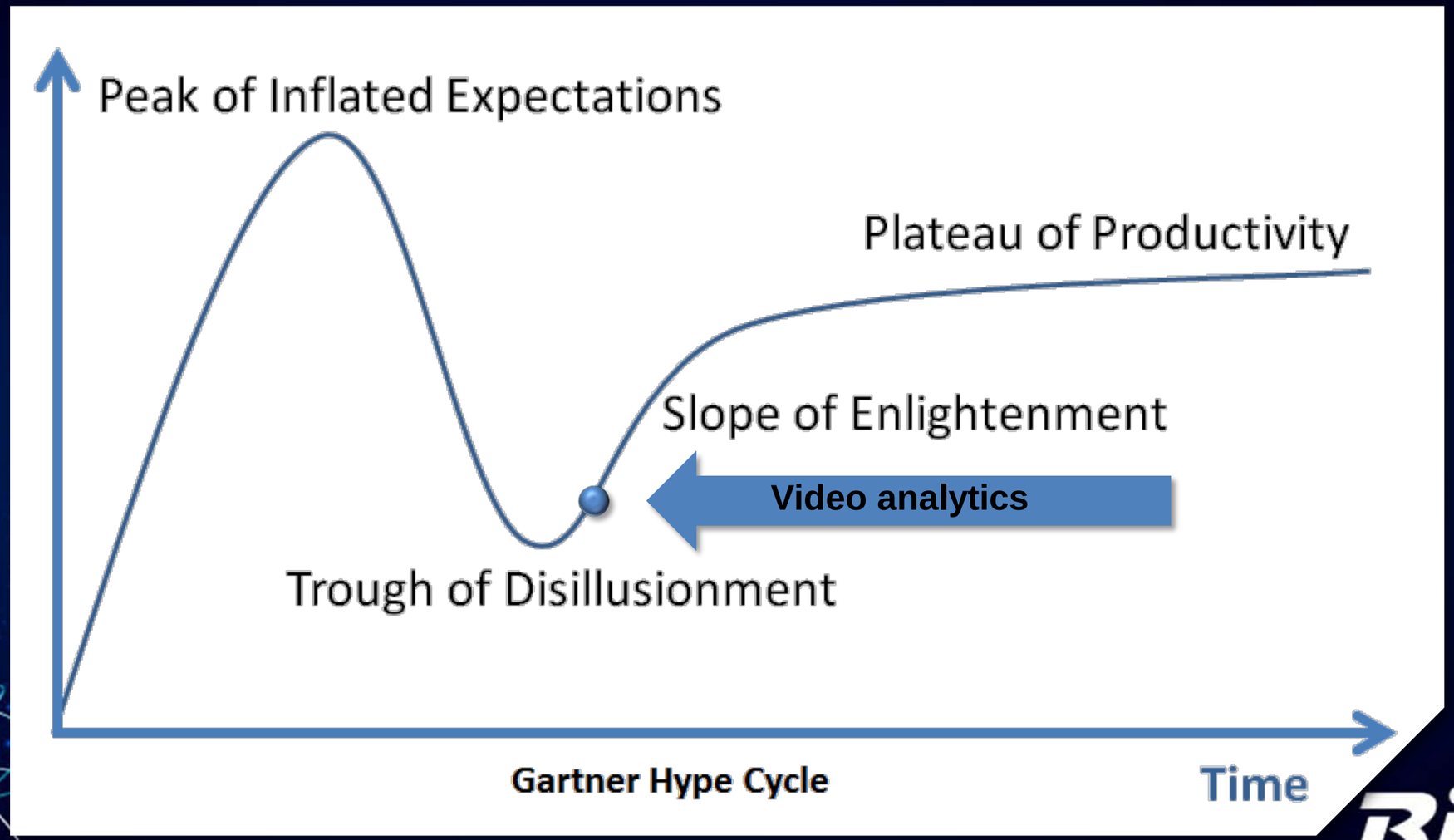
# Which one would you have?

Bicsi
MIDDLE EAST
& AFRICA

# Analytics

BICSI MIDDLE EAST & AFRICA

# The hype cycle




BICSI MIDDLE EAST & AFRICA

# Areas where analytics are seeing success

**Traffic surveillance**

**Intrusion detection**

**Retail analytics**

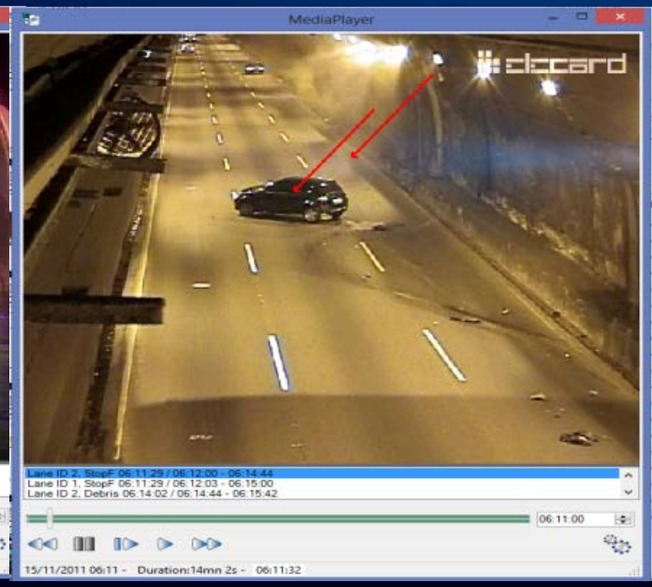
BICSI MIDDLE EAST & AFRICA

# Automatic Incident Detection (AID)

Citilog's Intelligent Automatic Incident Detection (AID) solutions enable traffic operators to identify and address incidents and accidents in real time:

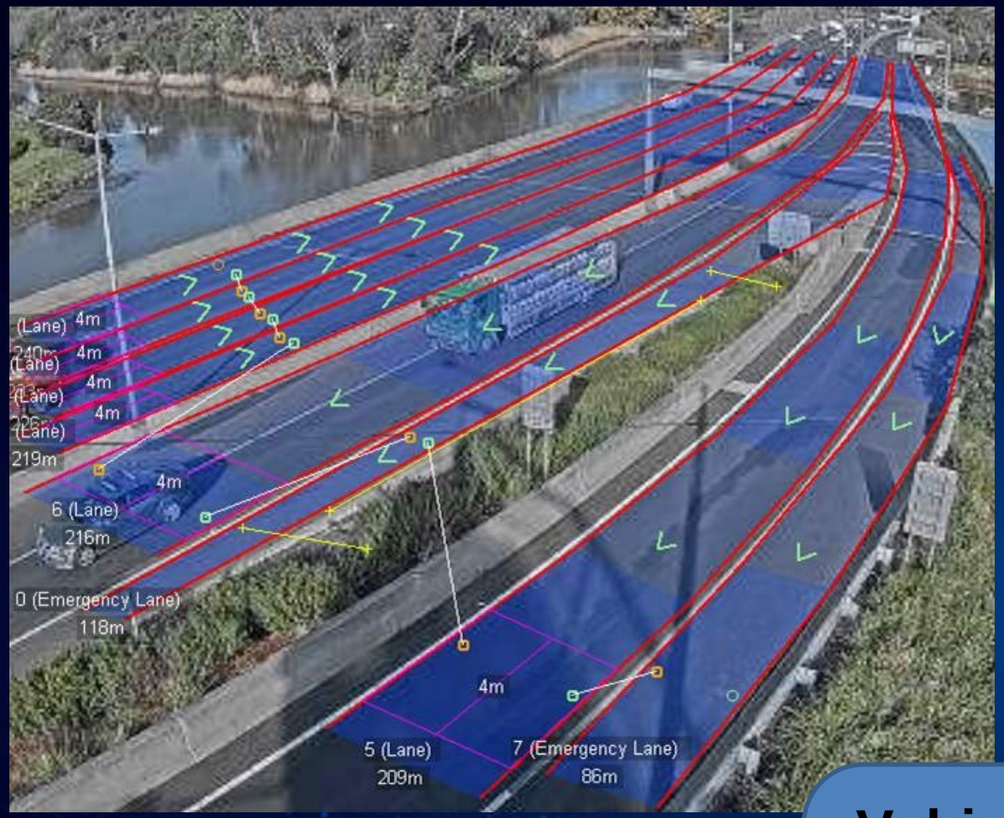
- Stop vehicle
- Congestion
- Wrong way
- Pedestrian
- Debris
- Smoke (tunnels)

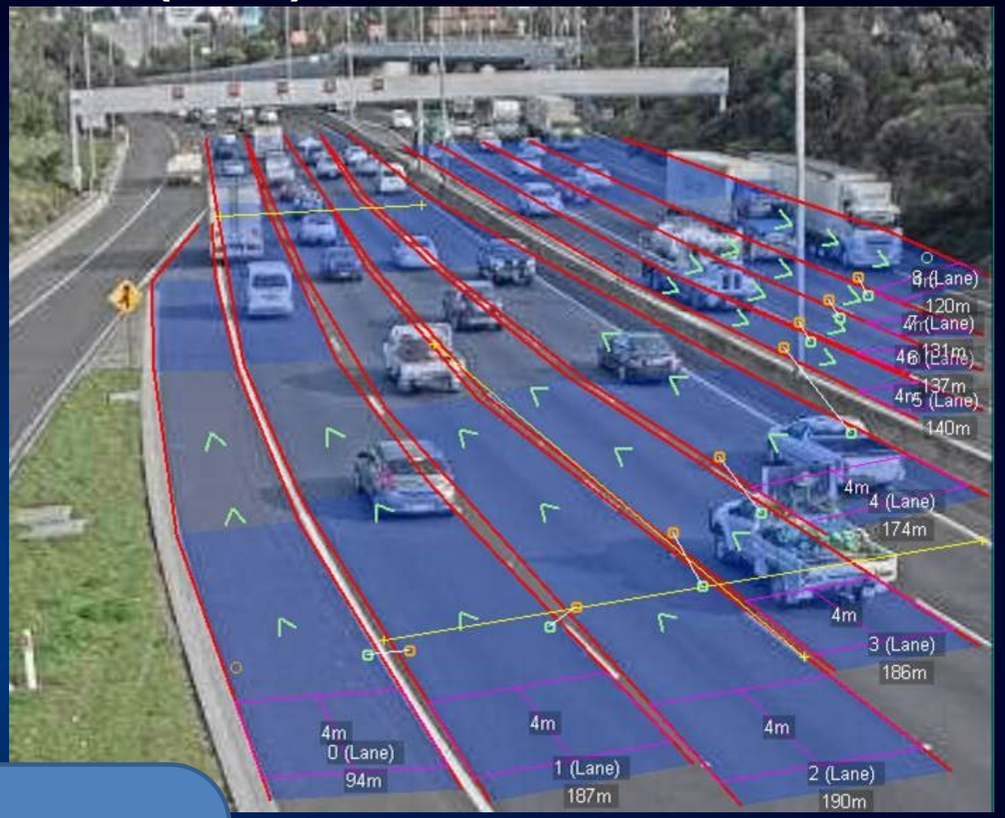






# Automatic Incident Detection (AID)




**Vehicle speed**
**Vehicle classification**
**Breakdown**
**Counter flow**

Bicsi MIDDLE EAST & AFRICA

# Intersection control – Smart City

> Presence detection

> Queue measurement at intersections

> Anti gridlock

# Intrusion Detection Solutions

Detect intruders

Verify events

Take actions

Bicsi MIDDLE EAST & AFRICA


# Intrusion Detection Solutions

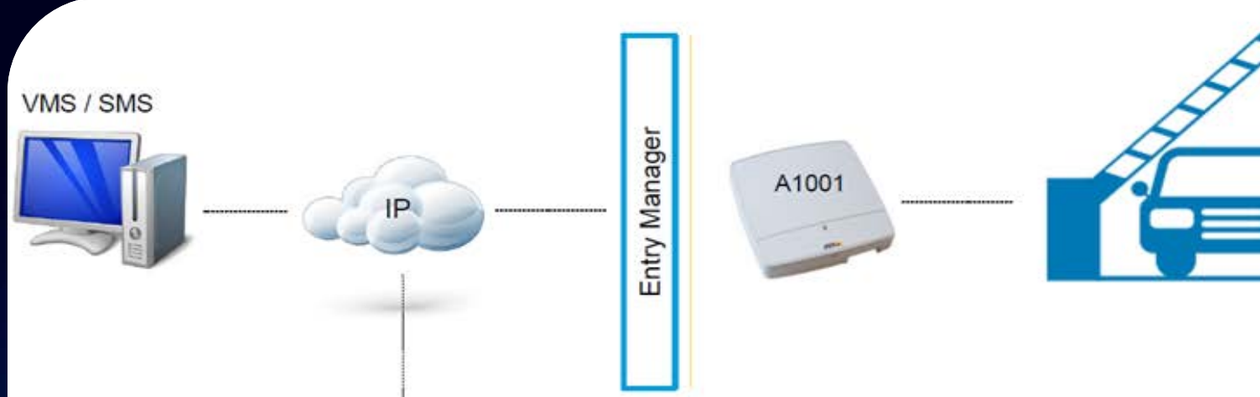
Bicsi
MIDDLE EAST
& AFRICA

# Thermal vs Optical

| A perfect complement adding value to surveillance systems | Network cameras 1920x1080 @   | Thermal network cameras 384x288 @  |
|---|---|---|
| Identification | ★★★★★ | ☆ |
| Detection at daylight | ★★★★ | ★★★★★ |
| Detection at night | ★★ | ★★★★★ |
| Detection in difficult conditions | ★★★ | ★★★★ |

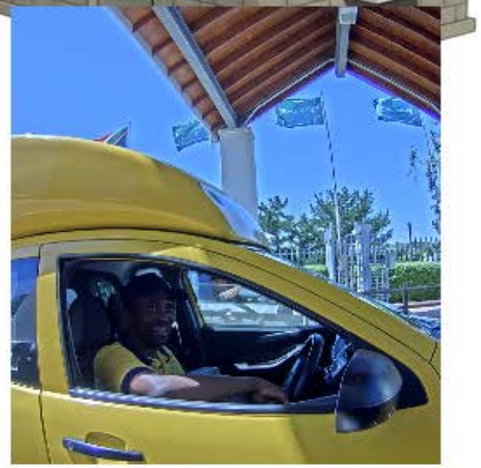
BICSI MIDDLE EAST & AFRICA

…on camera License Plate Recognition





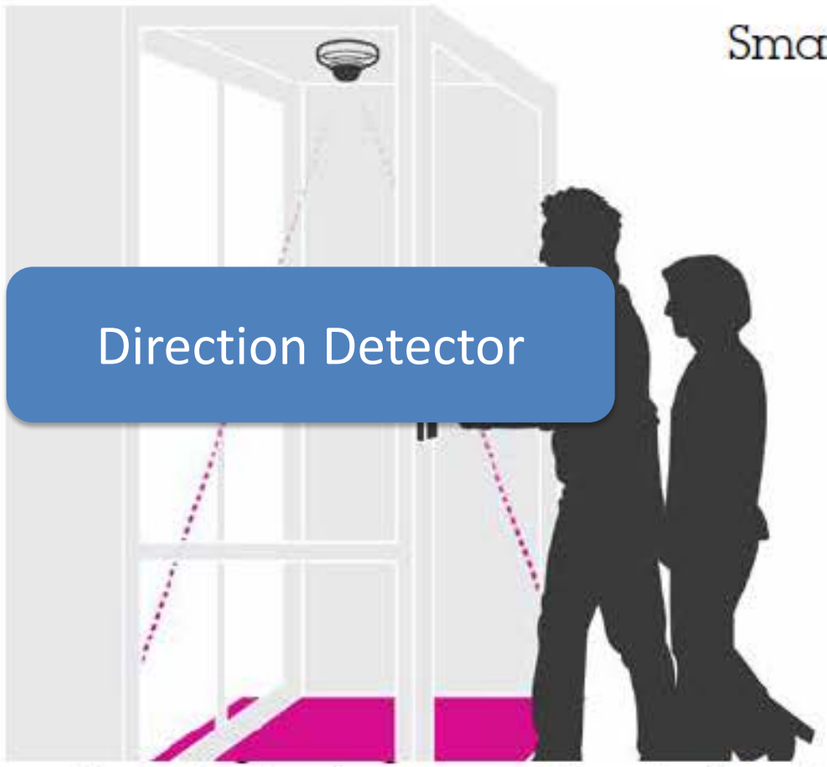


# Boom Gate access management

BICSI MIDDLE EAST & AFRICA

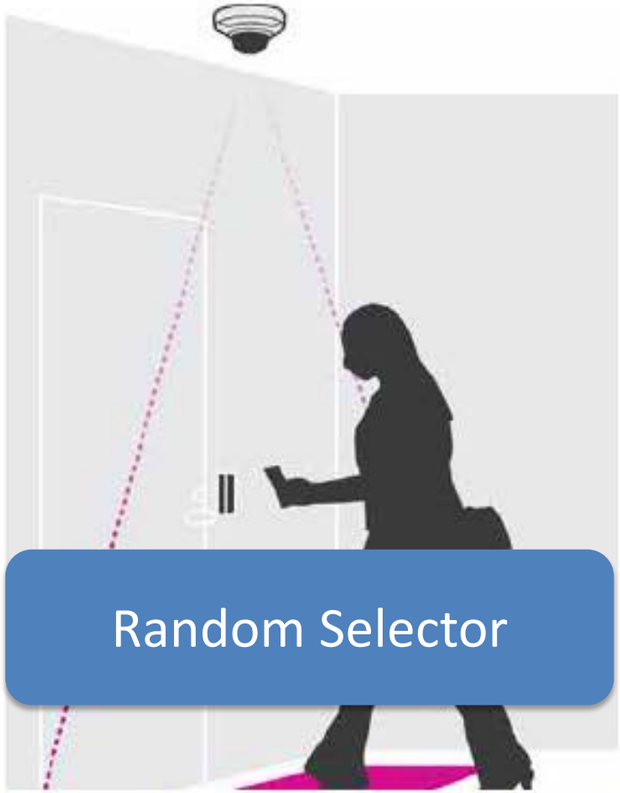
Smart analytics for entrance and exit control



Direction Detector

Smart analytics for preventing tailgating

Tailgaiting Detector

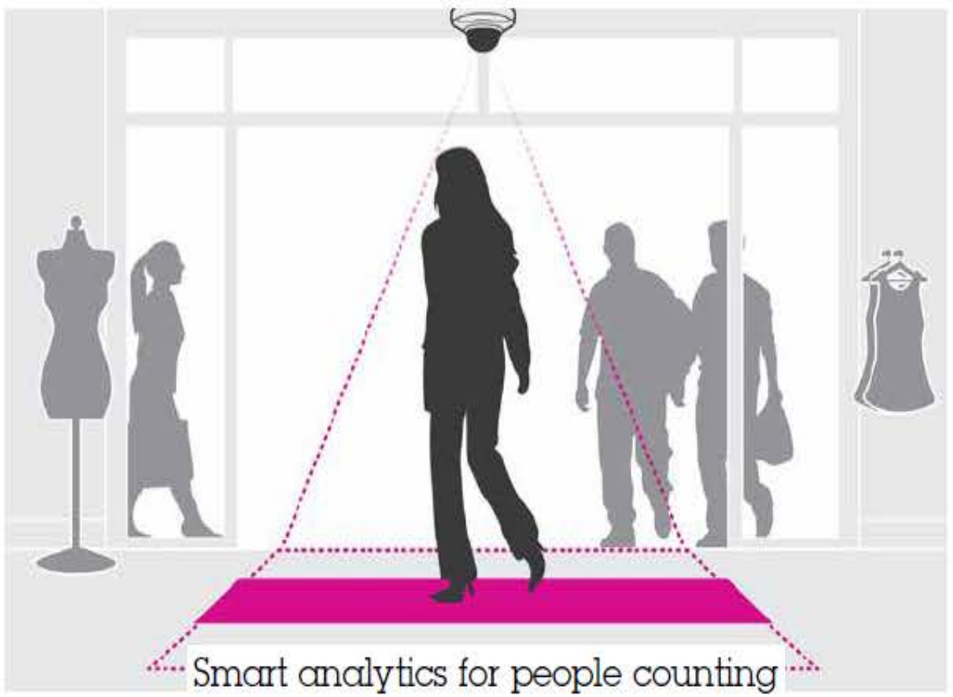


Random Selector

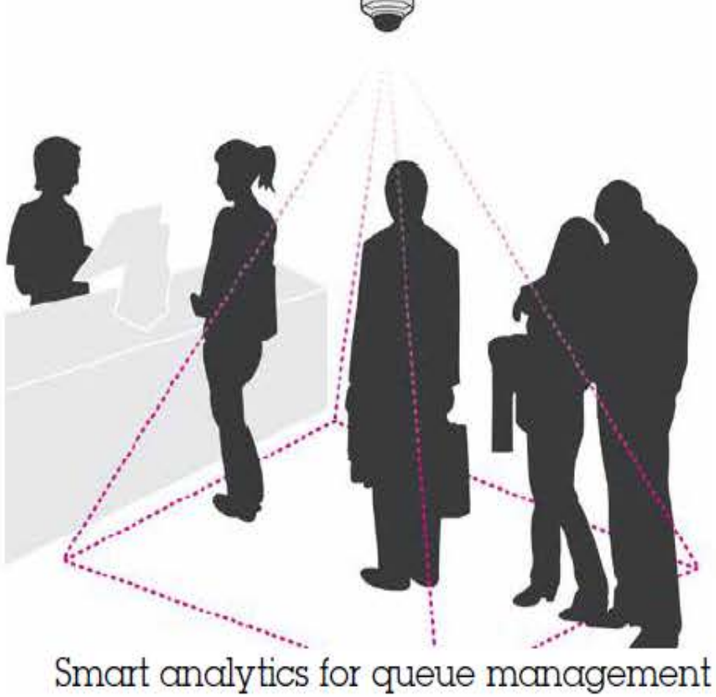
Smart analytics for unbiased inspection

# Edge Based Smart Analytics

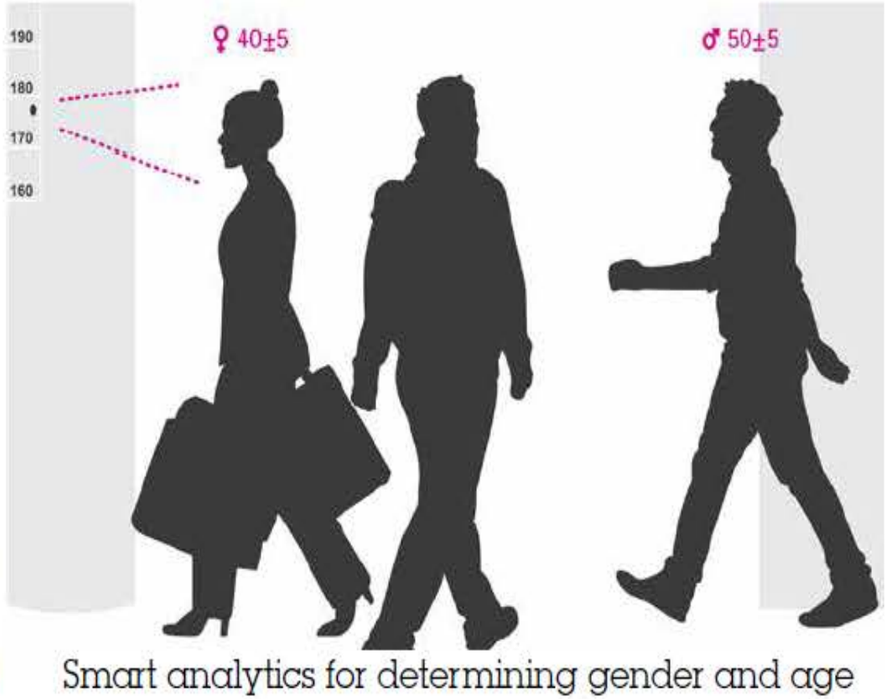
BICSI MIDDLE EAST & AFRICA



Smart analytics for people counting



Smart analytics for queue management




Smart analytics for determining gender and age

People Counting

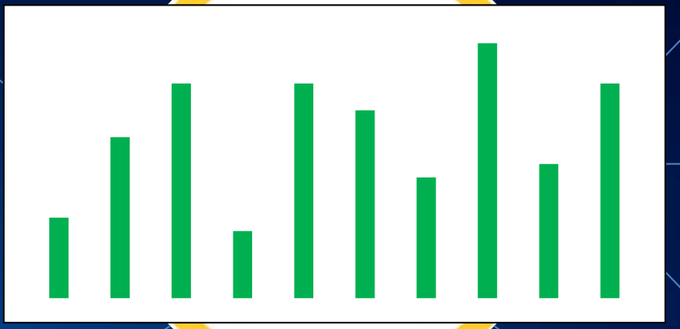
Queue management

Demographics

# Edge Based Smart Analytics

Bicsi MIDDLE EAST & AFRICA

# Video Management

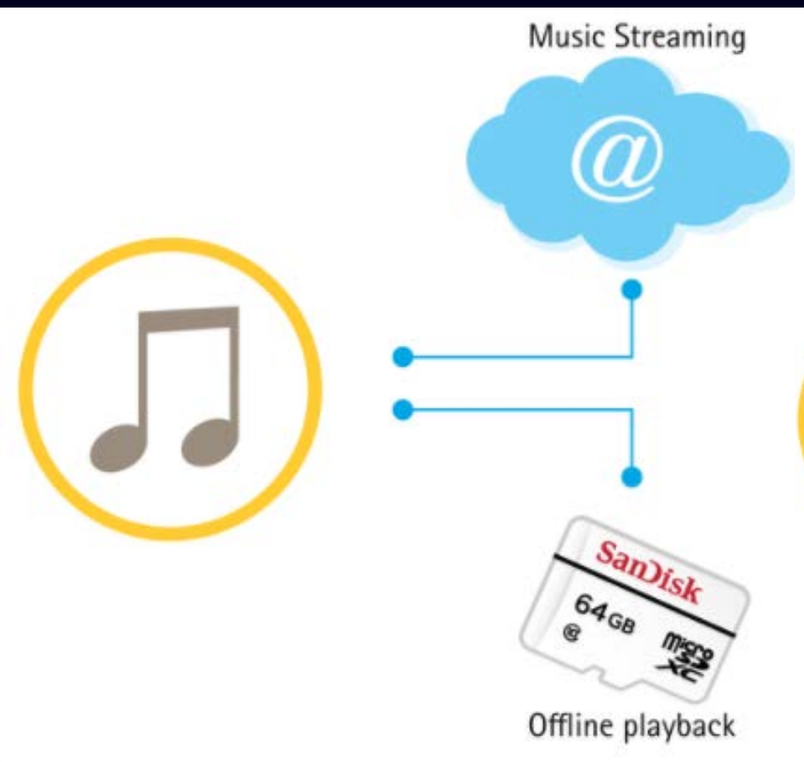


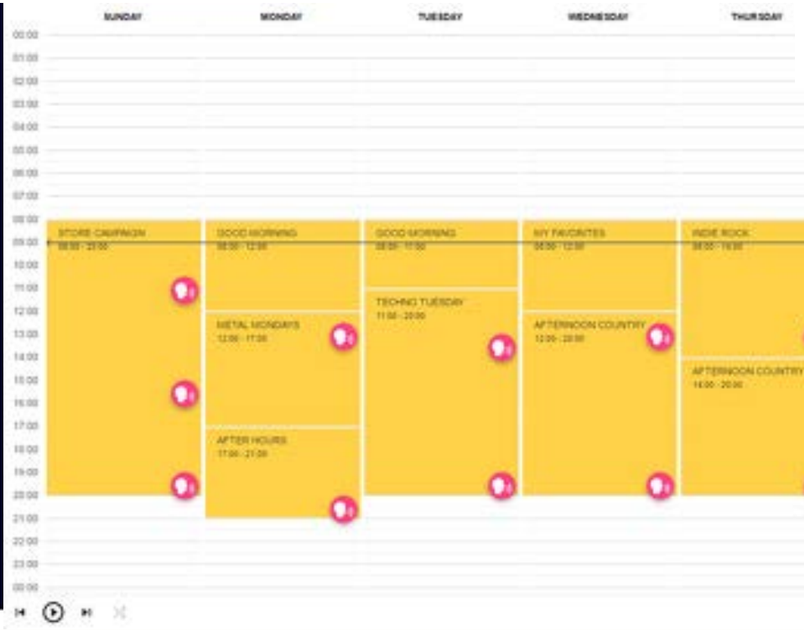
# BI

(Business Intelligence)

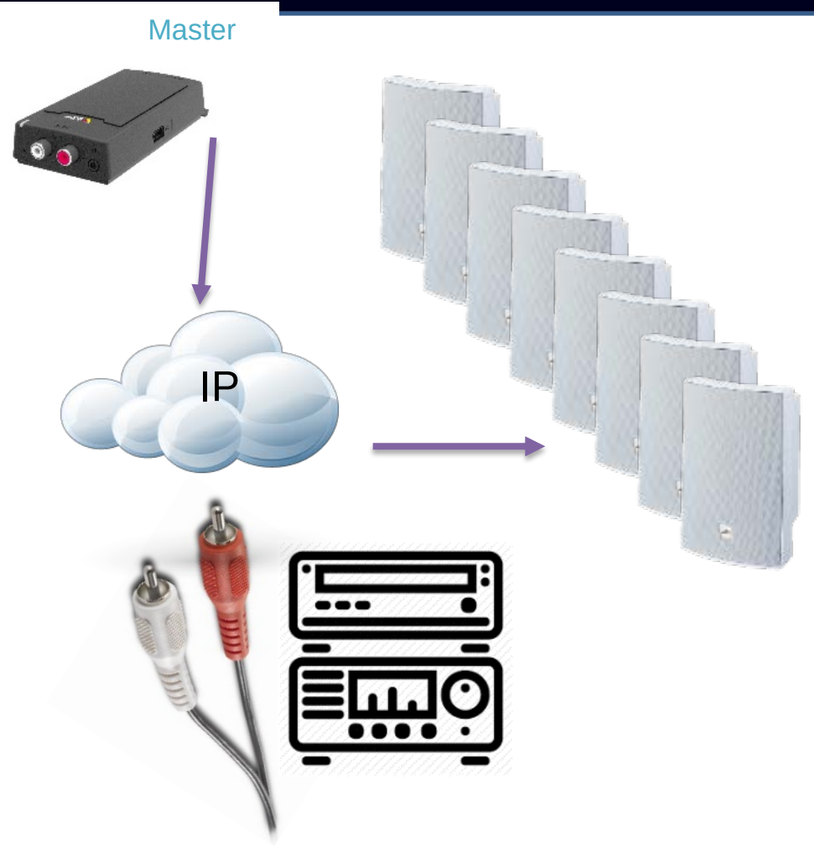
## Security vs Business Optimization

Bicsi MIDDLE EAST & AFRICA








# Adding Audio to the mix…

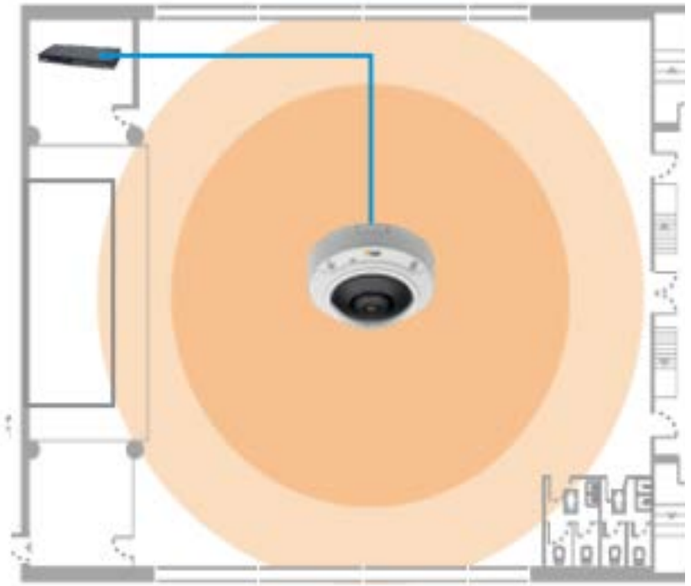
Store Audio Source

Bicsi MIDDLE EAST & AFRICA

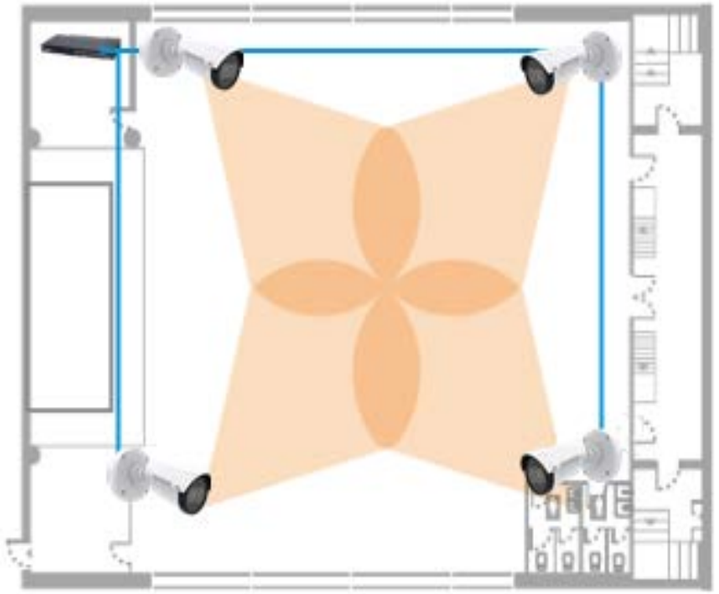
# Multi-sensor seamless wide-angle coverage

# Multi-sensor seamless wide-angle coverage

## Single Panoramic Camera



## Traditional camera coverage



BICSI MIDDLE EAST & AFRICA


Complete 360° with Detailed surveillance

# Image Usability

So is Bad light spoiling your image?

# Too much Light?

Forensic Capture

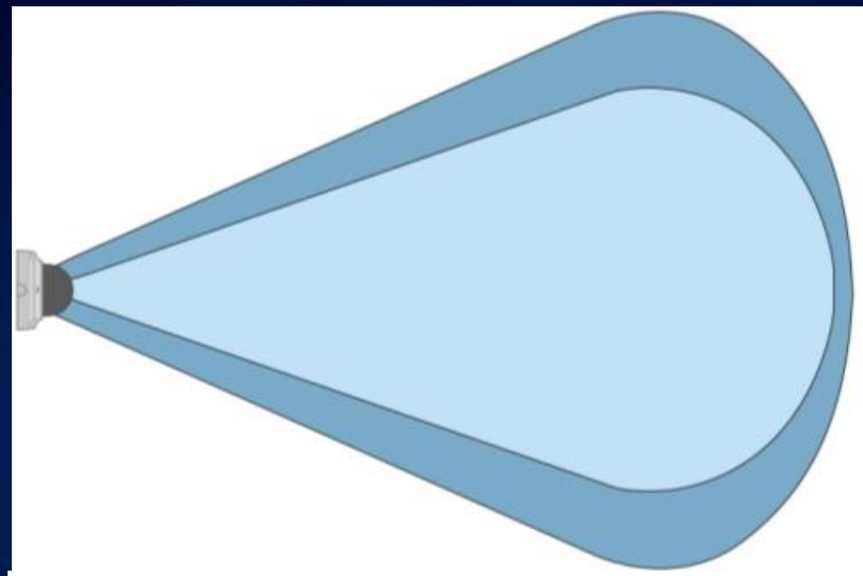
# Not Enough Lite?

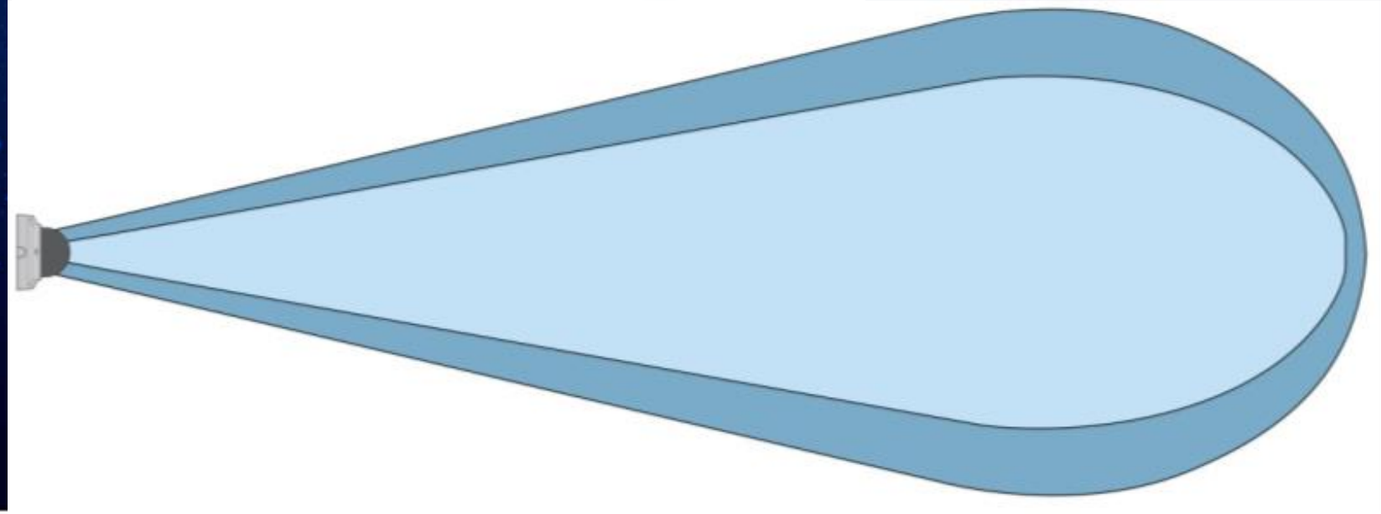
Lightfinder Camera

Legacy Camera

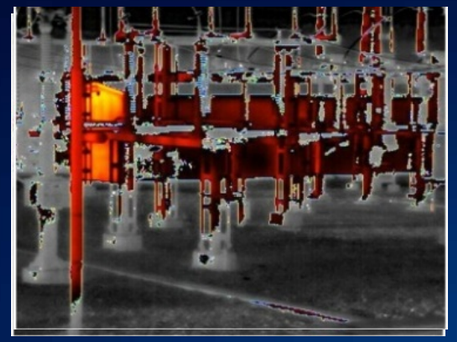
# No Light – Infra Red integrated into cameras

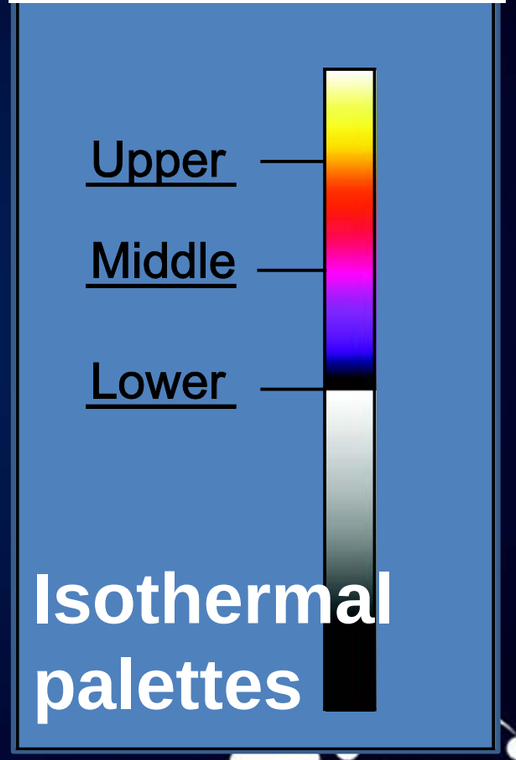
The illumination angle automatically follows the angle of view when adjusting the zoom level at installation





# Temperature Alarm Thermal



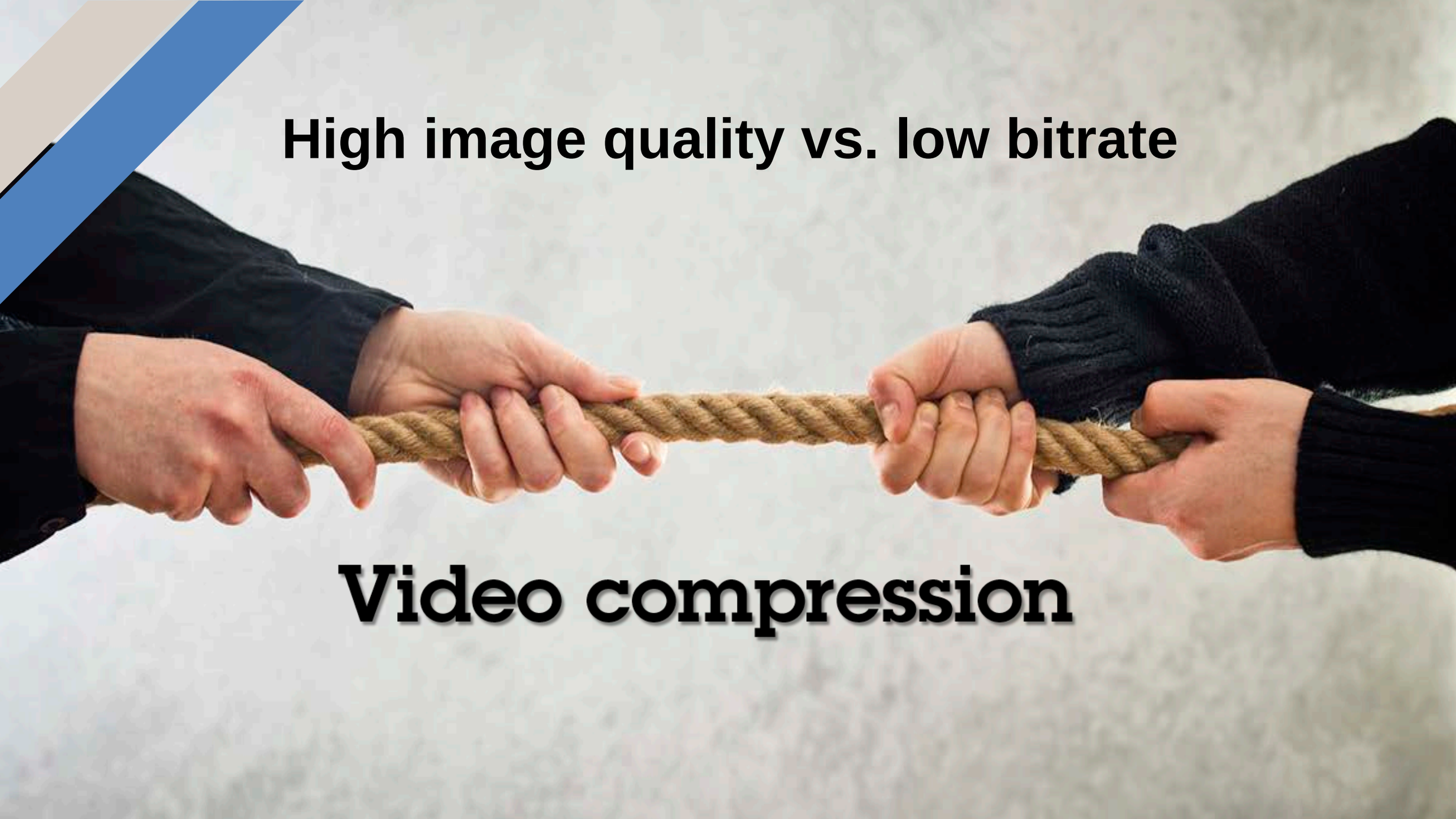




**Find the temperature of critical equipment**

> Set temperature based alarms or monitor sites for hotspots

BICSI MIDDLE EAST & AFRICA

# High image quality vs. low bitrate

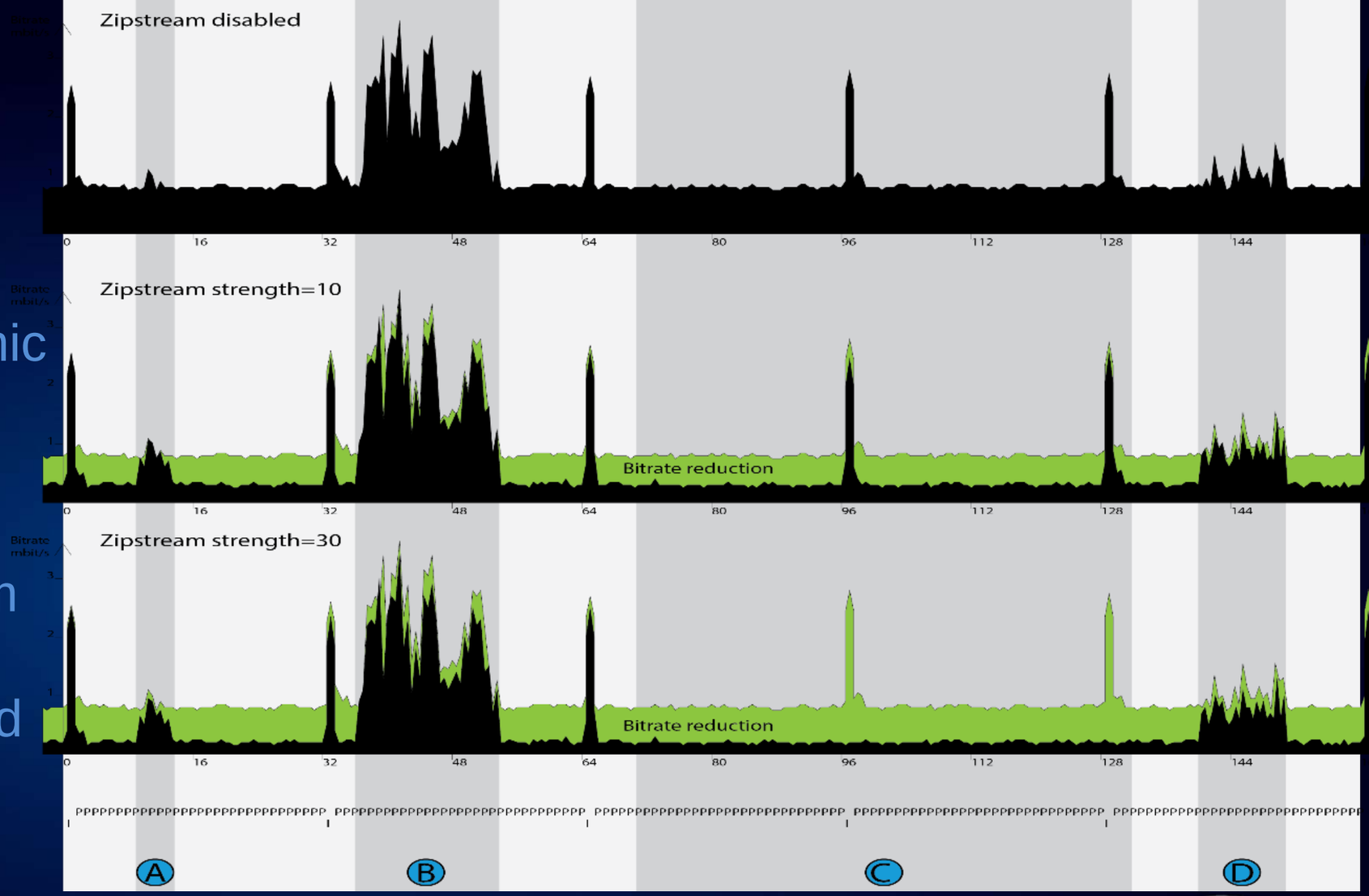


# Video compression

First graph: Zipstream disabled

Second graph: Zipstream with Dynamic ROI enabled

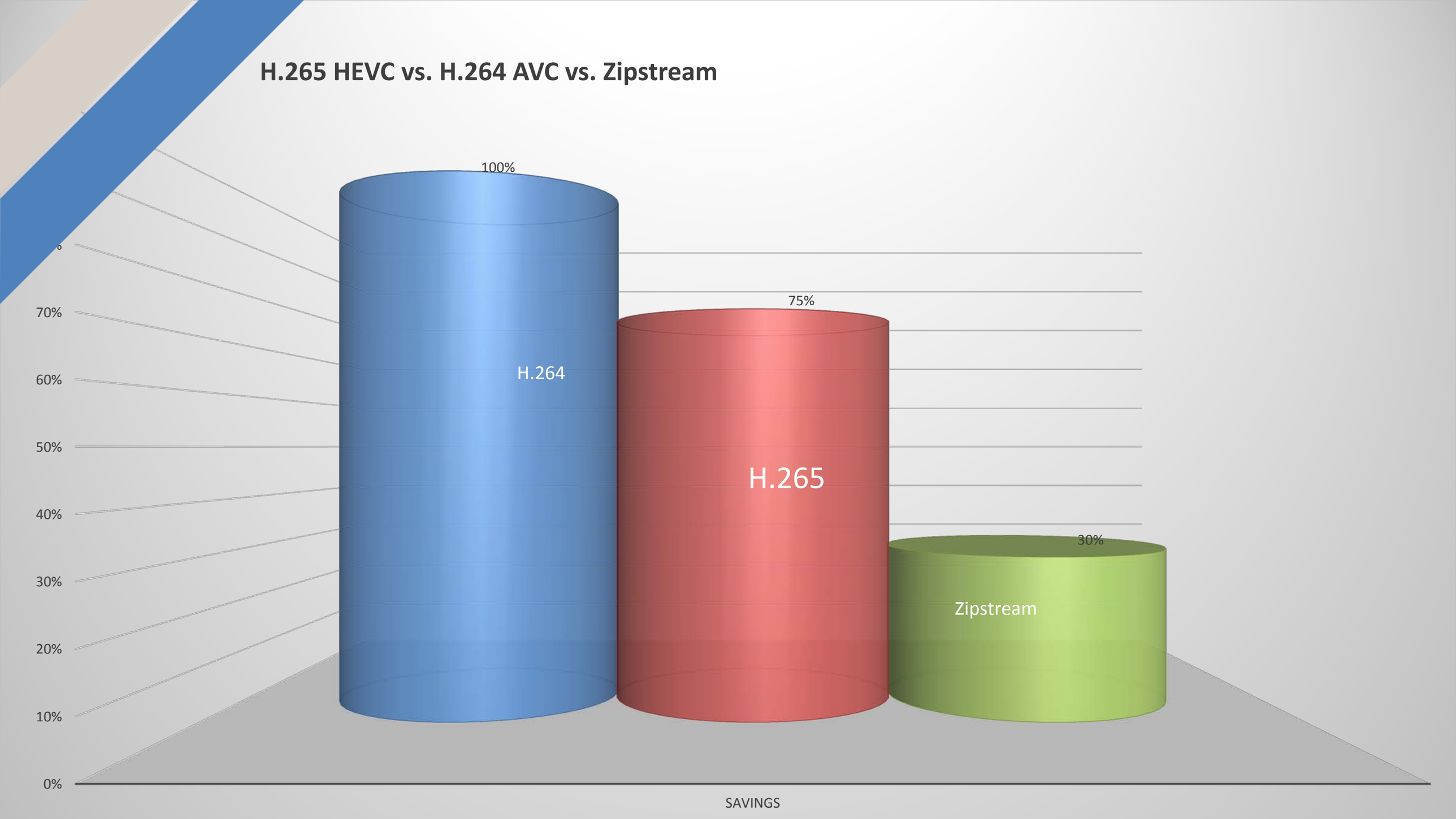
Third graph: Zipstream with Dynamic ROI + Dynamic GOP enabled




Reducing Bandwidth and Storage

Bicsi MIDDLE EAST & AFRICA

# H.265 HEVC vs. H.264 AVC vs. Zipstream




FUJI RVP
1
0A
1


FUJI RVP
2
1A
2

# THANK YOU

Bicsi
MIDDLE EAST
& AFRICA