

## Cautionary Advisory Regarding Forward Looking Statements

You should not place undue reliance on any forward-looking statements contained in this webinar presentation. The Company assumes no obligation to update forward-looking statements to reflect actual results, changes in assumptions, or changes in other factors affecting forward-looking information, except to the extent required by applicable laws.

[Arecont Vision Costar, LLC, a Costar Technologies, Inc. company](#)



# Real World Cybersecurity: *Reducing the Risk*

November 2018  
Webinar

# Here We Grow Again!

- Arecont Vision Costar is in growth mode for outstanding sales & support team members around the globe

### Arecont Vision Costar Targets Sales Growth in Europe, the Middle East, and India

October 31st, 2018



**Arecont Vision International Sales**  
A COSTAR COMPANY

*New resources provide enhanced support to customers and partners*


Los Angeles, CA and Dubai, UAE (October 31, 2018) – **Arecont Vision Costar**, the leader in network-based video surveillance solutions, announces the promotion of a key staff member and the addition of skilled new sales resources to improve customer and partner support across several international growth regions.

The company, a business unit of **Costar Technologies, Inc.** (OTC Markets Group: CTSI), is increasing its presence in Europe, the Middle East, and India through strategic hiring. The international sales organization has its regional headquarters in Dubai, United Arab Emirates, and is responsible for all worldwide Arecont Vision Costar sales and support activities outside of the Americas.

### Arecont Vision Costar Adds Brian White to Great Lakes Sales Region

November 12th, 2018

*Experienced senior sales leader to support customers and partners in key territory*



Los Angeles, CA (November 12, 2018) – **Arecont Vision Costar**, the leader in network-based video surveillance solutions, announces the selection of Brian White as Regional Sales Manager for the Great Lakes Region. The company, a new business unit of **Costar Technologies, Inc.** (OTC Markets Group: CTSI), was launched on July 13<sup>th</sup>, 2018 and is expanding its sales and support across the Americas.



# Continuing Awards for Our Newest Products & Services

- Arecont Vision Costar receives its newest industry award on Wednesday, 14 November...

## Arecont Vision ConteraIP™ Multi-Sensor Camera Takes Home New Product of the Year Award

September 25th, 2018



Award presented to Arecont Vision Costar at GSX 2018 by Security Today

Las Vegas, NV (September 25, 2018) – Arecont Vision Costar, the industry leader in IP-based megapixel camera technology and video surveillance solutions, announces receipt of a prestigious award for the brand new ConteraIP™ multi-sensor panoramic dome camera series. Arecont Vision Costar's newest multi-sensor camera was recognized as a New Product of the Year in the "Video Surveillance Cameras – IP" category, and the award presented at GSX 2018 in Las Vegas, Nevada by 1105 Media's Security Today Magazine.

The ConteraIP multi-sensor panoramic dome camera was first publicly unveiled on April 11, 2018 at ISC West. Arecont Vision has a long history of innovation, introducing the security market's first multi-sensor megapixel cameras in 2006. The ConteraIP multi-sensor is now the newest member of the Arecont Vision Costar family of industry-leading panoramic and omnidirectional megapixel surveillance cameras. The new camera is in early customer trials and is expected to be available for all customers soon.

## Arecont Vision ConteraIP™ Multi-Sensor Camera Named 2018 Campus Safety BEST Winner

October 8th, 2018



Los Angeles, CA (October 8, 2018) – Arecont Vision Costar, the industry leader in IP-based megapixel camera technology and video surveillance solutions, announces that the ConteraIP™ multi-sensor panoramic dome camera is the recipient of an important security industry award. The new camera has been recognized as a 2018 Campus Safety BEST winner in the "CCTV Surveillance Hardware" category.

The ConteraIP multi-sensor panoramic camera offers a choice of 8 or 20MP (megapixel) dome configurations. It is ideal for schools, colleges, and healthcare providers as the camera provides a panoramic 180° view from a single, affordable, high performance dome unit. It delivers superior, non-stop situational awareness while reducing the number of cameras and cabling required. This reduces the cost to buy, install, and maintain a modern surveillance system, while being less overt by having fewer cameras deployed.

## Arecont Vision Costar Total Video Solution Takes Home ASTORS Homeland Security Award from ISC East

Total Video Solution offers megapixel cameras, VMS, recorders, & web services



New York City, NY (November 14, 2018) – Arecont Vision Costar, the leader in network-based video surveillance solutions, it has been awarded an ASTORS 2018 Homeland Security Award. The recognition is for the new Total Video Solution offered by the company, which includes megapixel cameras, VMS system, video recorders, and web services.



# Real World Cybersecurity:

*Reducing the Risk*

# Cyberattacks Are On The Rise

- The threat of cyberattack continues to grow dramatically

Global cost of cybercrime will grow from \$3 trillion in 2015 to \$6 trillion annually by 2021

August 28, 2016 By Pierluigi Paganini

f My Page Like 61  
G+1 8

The cost of cybercrime could reach \$6 trillion by 2021 (global annual cybercrime costs has been estimated \$3 trillion in 2015).

The global cost of cybercrime continues to increase, this isn't a surprise due to the intensification of this kind of illegal practice. According to an analysis conducted by Cybersecurity Ventures, the cost of cybercrime could reach \$6 trillion by 2021 (global annual cybercrime costs has been estimated \$3 trillion in 2015).

Security experts are questioning about the effective grow of the cost of cybercrime in the next five years, trillion dollars plus is a worrying trend, but anyway possible as explained by Larry Ponemon, founder of the Ponemon Institute.

...the global cost of cybercrime continues to increase, this isn't a surprise due to the intensification of this kind of illegal practice. According to an analysis conducted by Cybersecurity Ventures, the cost of cybercrime could reach \$6 trillion by 2021 (global annual cybercrime costs has been estimated \$3 trillion in 2015).

https://goo.gl/5YGD64



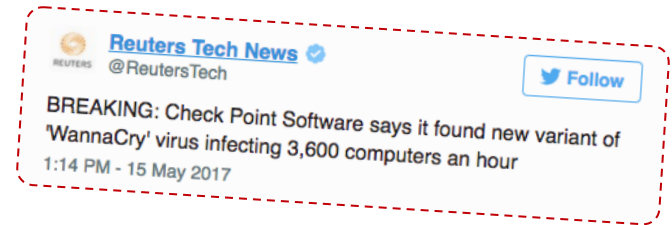
in tw f e u

Research by McKinsey and the World Economic Forum points to a widening range of technology vulnerabilities and potentially huge losses in value tied to innovation.

More and more business value and personal information worldwide

...the global cost of cybercrime continues to increase, this isn't a surprise due to the intensification of this kind of illegal practice. According to an analysis conducted by Cybersecurity Ventures, the cost of cybercrime could reach \$6 trillion by 2021 (global annual cybercrime costs has been estimated \$3 trillion in 2015).

https://goo.gl/WCiPsZ



Cyber crime is big business. Companies are reporting a growing number of cyber attacks – many of them aimed at their intellectual property – and are spending more on information security measures as a result.

> financial center is required for taking a progressive approach to cyber

...the global cost of cybercrime continues to increase, this isn't a surprise due to the intensification of this kind of illegal practice. According to an analysis conducted by Cybersecurity Ventures, the cost of cybercrime could reach \$6 trillion by 2021 (global annual cybercrime costs has been estimated \$3 trillion in 2015).

https://goo.gl/hHHrYG

## What is WannaCry ransomware and why is it attacking global computers?

Malicious software has attacked Britain's health service and companies in Spain, Russia, the Ukraine and Taiwan. What is it and how is it holding data to ransom?



© What is ransomware, how does it work, how does it spread and why is it attacking the NHS? Photograph: Alamy

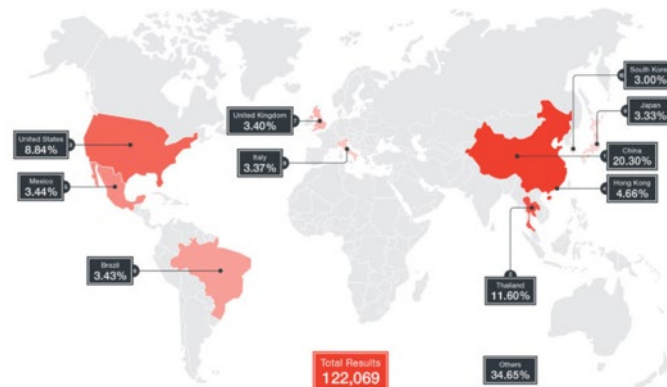
WannaCry malicious software has hit Britain's National Health Service, some of Spain's largest companies including Telefónica, as well as computers across Russia, the Ukraine and Taiwan, leading to PCs and data being locked up and held for ransom.

<https://goo.gl/NCoM9v>



## Secure Your IP Cameras, a New Botnet Has Arrived

Over 122,000 IP cameras are vulnerable to becoming part of the newly discovered Persirai botnet.

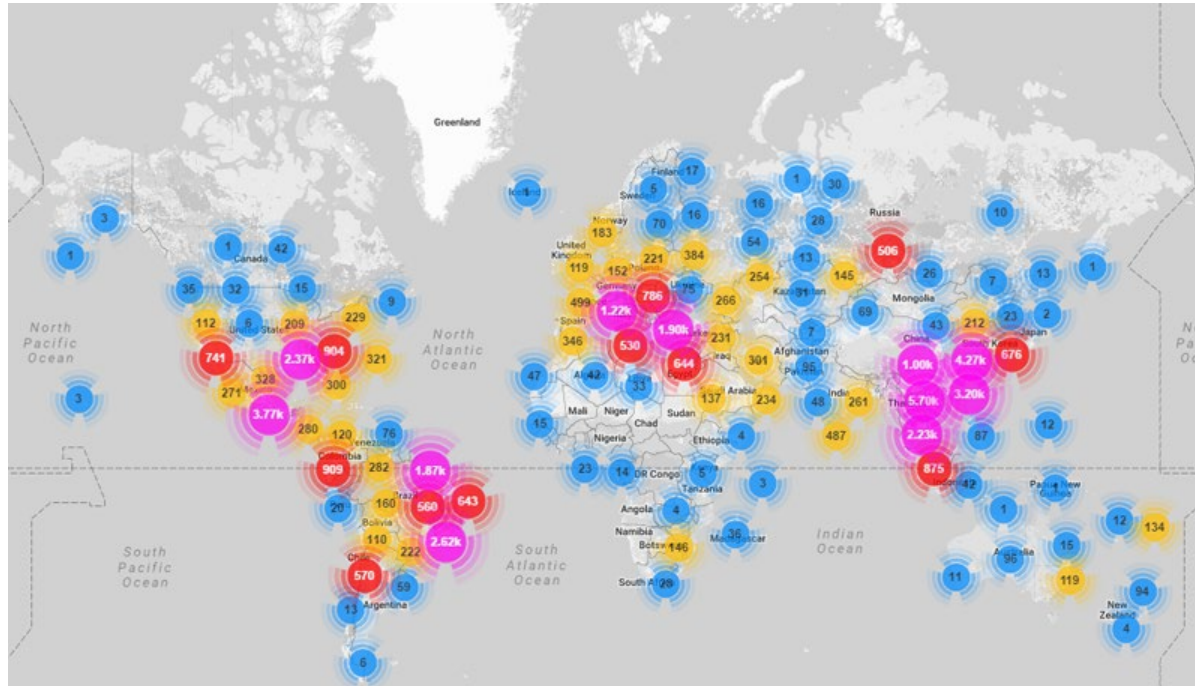


<https://lnkd.in/gZp9it4>

- Virus and malware protection software, firewalls, and services address known issues, security exploits, behavior, and malicious code
- Viruses and malware continue to evolve
  - *Vendors in the network security sector invest much time, effort, and resources to stay on top of emerging threats*
- Malicious code that has not yet been identified is much harder to stop before doing damage

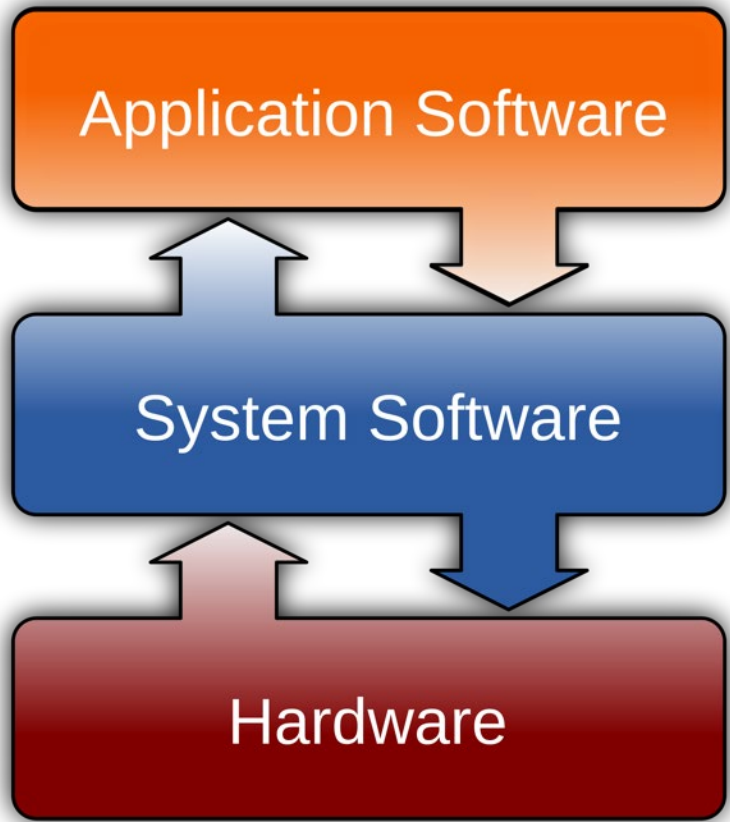
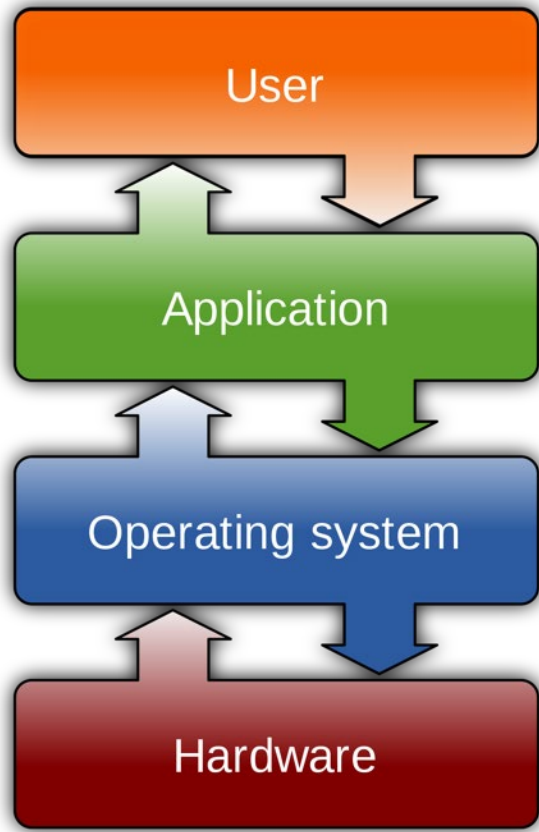
# Mirai Malware

- Targeted Linux Devices
- Largest DDoS attack
  - *620 Gbit/s – Krebs on Security*
  - *1 Tbit/s – French web host OVH*
- Identified 60 common factory default UN/PW's
- Infected Devices Continue to Function
- Blocks Remote Admin Ports
- Modified in 12/2017 to utilize zero-day flaw





# Operating Systems



## Network Security Can Be At Risk



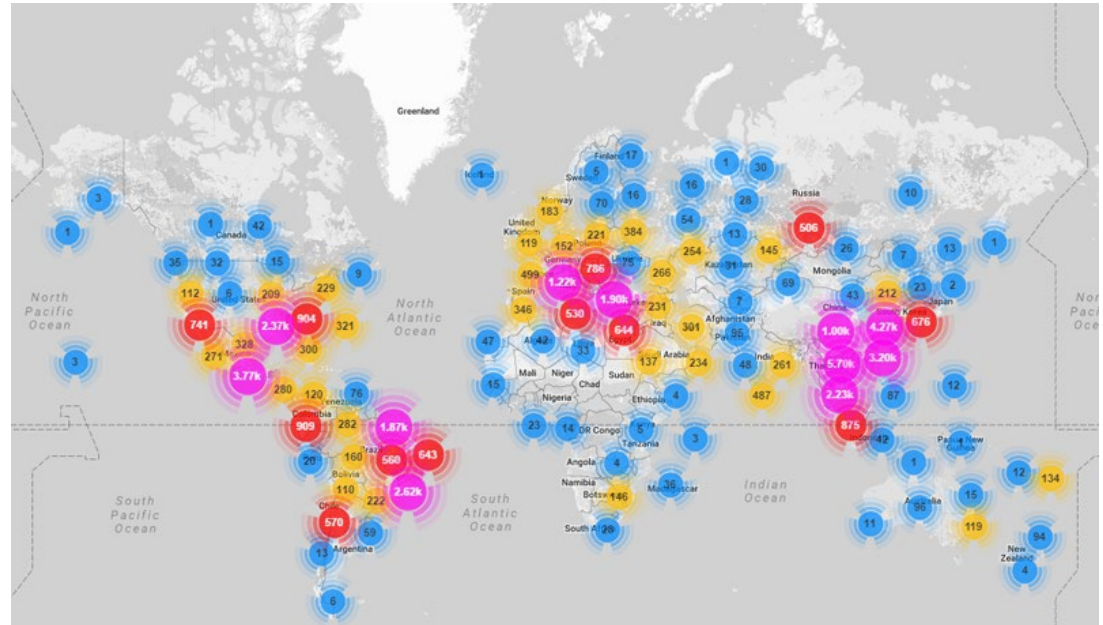
- Once a hacker or virus has gained access to a device, they can take control of it and use it to infect other devices
- Passwords and network protocols (802.1x, HTTPS, etc.) are largely ineffective once the device has been compromised
- Infected devices can spread malicious code, malware, ransomware, network intrusions, robotic Distributed Denial of Service (DDoS) attacks, or other nefarious purposes

# IoT Devices (Cameras) Are Not Well Protected

- **Example media reports of security system cybersecurity concerns – None impact Arecont Vision cameras:**
  - 4/14: **Hackers turn security camera DVRs into Bitcoin makers** <http://tinyurl.com/jdc9m6m> & **Hikvision devices open to hackers** <http://tinyurl.com/ycgstsak>
  - 2/16: **Cameras reported to “phone home to China”** with your video <http://tinyurl.com/y8o5tl5j>
  - 9/16: **DDoS on KrebsOnSecurity.com & OHV DNS service** uses 140,000+ network cameras & DVRs <http://tinyurl.com/ycl48tfm>
  - 10/16: **DDoS on 85 web services** including Amazon, Financial Times, Netflix, PayPal, Spotify, & Twitter suspected to have included many IoT (Internet of Things) devices from cameras to appliances for loss of \$100M <http://tinyurl.com/yb9y6xum>
  - 11/16: **Hikvision cameras reported to send their data to China after being plugged in**, Chinese government can access installed cameras when they want <http://tinyurl.com/ycntb82q>
  - 11/16: **Security camera infected by malware** 98 seconds after plugged in <http://tinyurl.com/j2svefe>
  - 1/17: **70% of Washington, DC police video cameras** & 123 of 187 NVRs hijacked by ransomware attack, days before Trump Presidential Inauguration <http://tinyurl.com/yajbnn8h>; **DC and South Dallas cyberattacks** <http://tinyurl.com/y7qjcf8o>
  - 3/17: **Why Genetec sees Hikvision products as security risks** <http://tinyurl.com/lS44ygl>
  - 3/17: **Dahua, Hikvision IoT Devices Under Siege** <http://tinyurl.com/j93btX8>
  - 4/17: **Dahua Devices Dangerously Exposed to Cybersecurity Hack** <http://tinyurl.com/jxjlc8w>
  - 7/17: **‘Devil’s Ivy’ gSOAP Vulnerability Could Afflict Millions of IOT Devices, including ONVIF cameras** <http://tinyurl.com/ydy71786> and <http://tinyurl.com/ydajthdq>

# Operational Practices

- Change Passwords – Devices
- Change Passwords – Sites
- Change Passwords – Often
- Physically Lock Computers
- Disable Boot Devices
- Set Bios Password
- Weigh the benefits of remote access



# Exterior Cameras Practices

- Set Alarms for Offline Cameras
- Review Video leading up to the alarm
- Check Connection Point Access



# Network Practices

- Standard Security – Yes
  - 802.1x, SSL
- Separate Traffic
  - *Wired and Wireless*
- Separate Access
- Update bridge points
- Audit connections

## Advanced

- Block Unused Ports
- Change Standard Ports
- Monitor Outgoing Communications



# Arecont Vision MegalIP™ Camera FPGA Technology

- Arecont Vision **MegalIP™** cameras have never been reported as being used in any cybersecurity attacks
- Should a hacker gain access to a **MegalIP** camera, or obtain the user ID and 16-digit ASCII password to log into the camera, the attack would only impact that device
  - *A successful hacker or virus attack could change the camera webpage and change individual camera settings or take it off line*
  - *The camera could not be taken over for any function other than for which it is designed*
  - *A bot or virus could not take control and use the camera to launch cyberattacks on other network enabled devices or infect other devices across either the the local network or the Internet*

View all Technical Updates: <https://www.arecontvision.com/bulletins/Technical>

## Arecont Vision Cybersecurity Positioning

### ARECONT VISION TECHNICAL UPDATE - Issued 14 March 2017

Arecont Vision is uniquely positioned for continued cybersecurity protection of our customers.

We design and manufacture Arecont Vision cameras in the United States. This ensures top quality, industry-leading megapixel cameras at a competitive price.

At the heart of each of our cameras is an Arecont Vision-designed circuit board, on which we mount a Field Programmable Gate Array (FPGA) integrated circuit. We operate the 5th generation of the Arecont Vision-developed Massively Parallel Image Processing (MPIP) architecture on that circuitry.

We do not use Linux or other common operating systems (OS) which are typically found in competitor cameras. These OS systems present a cybersecurity risk to the devices that rely on them.

Due to the in-house developed MPIP architecture, Arecont Vision cameras cannot be repurposed for use in cybersecurity attacks as other vendor's cameras have been.

Press coverage of cyberattacks involving video surveillance devices continues. Examples include:

• 4/14: Hackers turn security camera DVRs into Bitcoin makers <https://goo.gl/vrvtvz> & Hikvision devices open to hackers <https://goo.gl/PtHs7r>

• 2/16: Cameras reported to "phone home to China" with your video <https://goo.gl/MWJ35T>

• 9/16: DDoS on Krebssecurity.com & OHV DNS service uses 140,000+ network cameras & DVRs <https://goo.gl/Df4Mkr>

• 10/16: DDoS on 85 web services including Amazon, Financial Times, Netflix, PayPal, Spotify, & Twitter suspected to have included many IoT (Internet of Things) devices from cameras to appliances for loss of \$100M <https://goo.gl/P7nW46>

• 11/16: Hikvision cameras reported to send their data to China after being plugged in, Chinese government can access installed cameras when they want <https://goo.gl/QA3d04>

• 11/16: Security camera infected by malware 98 seconds after plugged in <https://goo.gl/bu8fA0>

• 1/17: 70% of Washington, DC police video cameras & 123 of 187 NVRs hijacked by ransomware attack, days before Trump Presidential Inauguration <https://goo.gl/NkuKQW>, and DC and South Dallas cyberattacks <https://goo.gl/Xmh1hr>

• 3/17: Racc speaks out on why Genetec sees Hikvision products as security risks; Hikvision to Genetec: "Vague accusations and outrageous claims" <https://goo.gl/yHBrvz>

• 3/10: Dahua, Hikvision IoT Devices Under Siege <https://goo.gl/yC9arH>

At Arecont Vision, we develop our own core features and technology for use in our cameras, rather than purchasing them from 3rd parties. This ensures that malicious code is not inadvertently introduced into our products. For time to market and cost reasons, other vendors typically purchase code or IC chips from 3rd parties for core features and technology potentially introducing additional risk into their products.

Arecont Vision cameras offer user IDs and 16 digit ASCII passwords. Arecont Vision University training programs provide best practices recommendations for password and cybersecurity protection to ensure camera passwords systems stay secure. Should a hacker ever obtain the user ID and password for an Arecont Vision camera, only that device can be impacted. The unique Arecont Vision architecture ensures that the camera cannot be repurposed to participate in Distributed Denial of Service (DDoS), ransomware, network intrusion, or other common cyberattacks across the network.

Security updates, new features, and enhancements can be applied to Arecont Vision cameras after installation. Arecont Vision has introduced standard network protocols (802.1x, HTTPS) in many of our cameras, and firmware updates are or will be available that provide these protocols for use by Arecont Vision cameras already in use.

Arecont Vision believes in promoting industry standards and smart cybersecurity practices, and our employees strive to bring this message to the security industry. Among our initiatives is our commitment to the Security Industry Association's Cybersecurity Advisory Board, of which one of our executives is a founder and active participant. Other executives participate in various SIA committees, while a senior executive is an active member of the SIA Board of Directors and the SIA Executive Committee.

Arecont Vision continues to invest in our MegalIP™ test and certification facility, which in 2016 opened participation to network infrastructure and cybersecurity vendor solutions (see [press release at https://goo.gl/2ymb0V](https://goo.gl/2ymb0V)). Dozens of video management system (VMS), network video recorder (NVR), analytics, utility, and infrastructure vendors have participated and tested their products through the MegalIP and the Arecont Vision Technology Partner Program.

The choice is simple: If a customer wants to ensure cybersecurity protection, Arecont Vision cameras should be their first choice.

# Arecont Vision Costar Cyber Security Resources

Leverage the [Arecont Vision Costar Partner Portal](#)

- ✓ <https://www.arecontvision.com/signin.php>
- ✓ <https://www.arecontvision.com/dashboard.php>

- Mega

- *Arecont Vision & Cyber Security white paper*
- *Gold Standard preso – AVC Made in USA section*

- Contera

- *Total Video Solution – Platform Cyber Security Overview*
- *Get More for your Security brochure*
- *Gold Standard preso – ConteraVMS & ConteraWS slides*







# Real World Cybersecurity:

*Reducing the Risk*

Watch for our email to replay today's webinar to review the slides at your convenience

Follow the AVC News Blog or our Social Media for the Latest News



**Arecont Vision**  
A COSTAR COMPANY

[www.arecontvision.com](http://www.arecontvision.com)

[sales@arecontvision.com](mailto:sales@arecontvision.com)

+1.818.938.0700

**Arecont Vision**  
NEWS BLOG

<http://blog.arecontvision.com>

AV News Center

<https://www.arecontvision.com/news.php>



Connect with us  
**LinkedIn**

[linkedin.com/company/arecont-vision](http://linkedin.com/company/arecont-vision)

**f** Like us on  
**Facebook**

[facebook.com/arecontvision](http://facebook.com/arecontvision)

**You Tube**

[youtube.com/user/ArecontVision](http://youtube.com/user/ArecontVision)

Follow us on  
**twitter**

[twitter.com/arecontvision](http://twitter.com/arecontvision)

[@arecontvision](https://twitter.com/arecontvision)