MegaIP™

Total Video Solution –
Cybersecurity Protection

MegaIP™ Megapixel Camera Cybersecurity

Examining the Advanced Cybersecurity Capabilities of Arecont Vision Costar MegaIP™ Megapixel Cameras

Arecont Vision®
A COSTAR COMPANY

+1.818.937.0700 | www.arecontvision.com | avsales@arecontvision.com

Table of Contents

Introduction

Arecont Vision Costar is a U.S. company with headquarters, R&D, and manufacturing in the Los Angeles, California area. A major area of concern for our customers around the world today is cybersecurity.

There are many reference points about the cyber threat that security users face today. Verisign, a Virginia-based infrastructure and security company reported back in 2016 that the frequency of cyberattacks is increasing by 75% year over year [see https://tinyurl.com/y8rselzj]. Unfortunately, we see no indication that this trend is changing today.

The sophistication of cyberattacks and the types of devices involved are both increasing in number and evolving in complexity. Consider the attack on Krebsecurity.com and France-based Internet hosting firm OHV in September of 2016. Instead of traditional IT devices, this attack involved over 140,000 network cameras and digital video recorders (DVRs) [see https://tinyurl.com/ycl48tfm]. The devices were transformed into robotic attackers or "bots" by an infection of Mirai malware. The devices were used in repeated Distributed Denial of Service (DDoS) attacks, keeping the targeted websites so busy that they were unable to respond to legitimate user requests.

With the Internet of Things (IoT) growing in use across cameras, appliances, industrial machinery, vehicles, and smart home technology, DDoS-style malware has many more devices to both target and launch cyberattacks from than ever before.

In October 2016, a well-publicized DDoS attack impacted up to 85 web services for an eleven-hour period. Users across parts of North America and Europe were unable to access Amazon, the Financial Times, Netflix, PayPal, Reddit, Spotify, Twitter, and several other well-known services. Beyond the impact on user convenience, an estimated $100M USD loss in revenue resulted from the attack, leading to both the FBI and Homeland Security became involved in the investigation.

The Devil's Ivy hackable flaw exposed in July of 2017 demonstrated that manufacturers and OEM vendors that used the ONVIF-approved gSOAP tool had unknowingly opened their cameras to additional cyber risk [see https://tinyurl.com/ydajthdq]. This flaw impacts hundreds of thousands of existing cameras from white label models to those from well know global brands and requires each camera to be individually patched eliminate the flaw. (Note that Arecont Vision Costar cameras were not impacted by this issue).

Impersonation attacks are also on the increase, and the FBI has estimated that they have resulted in $3B USD in losses over the past three years [see https://tinyurl.com/yb9y6xum]. This type of attack is often instituted unknowingly by a user inside the network clicking on a malicious link from an email. The list of attacks that such an action can invoke seems endless.

Governments and law enforcement agencies are also impacted. Prior to the Trump Presidential Inauguration on January 20, 2017, the Washington Post reported that 70% of the video cameras across the U.S. capital were infected with ransomware. 123 of 187 network video recorders (NVRs) had their data encrypted by the infection [see https://tinyurl.com/yddmyuwo].

Other network-enabled cameras and DVRs have been reported in the media to secretly connect to sites in China. Data, video, and images have reportedly been uploaded to these remote locations without the consent or awareness of the user [see https://tinyurl.com/ycntb82q & https://tinyurl.com/y8o5tl5j]. Other cameras have been infected with malware within seconds of being connected [see https://tinyurl.com/j2svefe], or are easily hacked [see https://tinyurl.com/ycgstsak and https://tinyurl.com/jdc9m6m] as long ago as 2014.

Today, we continue to see cybersecurity attacks that involve cameras, DVRs, and recorders. Attacks by the Peekaboo virus in 2018 [https://tinyurl.com/yc5s2ub9] alone exposed over 800,000 cameras to cyber threat.

Arecont Vision Costar is committed to providing cybersecurity protection for IP network cameras, and this white paper examines the unique cyber benefits of Arecont Vision Costar MegaIP™ cameras, the nature of the attacks, and recommendations for our customers.

Arecont Vision Costar offers the Total Video Solution™ that includes both the MegaIP and ConteraIP™ megapixel camera families, ConteraCMR™ cloud-managed video recorders, and ConteraVMS™ advanced video management software. These products can be used together to leverage advanced ConteraWS™ cloud-enabling benefits. ConteraWS offer strong cybersecurity protection via features such as multi-factor authentication, NIST-level encryption, transport layer security, cross-site request forgery protection, protected login credentials, logically separated data, data redundancy, and proxy server support.

Cybersecurity Awareness & Protection

In the Beginning

Not long ago, physical asset protection across corporations and multiple sectors including education, healthcare, manufacturing, and government was primarily the purview of the security department. At the same time, the maintenance and protection of electronic data systems was the responsibility of the IT department. With the movement of surveillance and other security systems onto IP-based network technology, the IT and security departments are increasingly interconnected. Organizations are rethinking their traditional security responsibilities for the newly merged physical and digital worlds.

IT has traditionally applied a layered security approach for systems and infrastructure and the data contained. Security departments are increasingly adopting these same protections for network enabled technology, including video surveillance.

Changing Security Models

Recent cyberattacks have revealed vulnerabilities beyond traditional IT systems and infrastructure, uncovering the potential threat of attack both on and through many network connected devices. The Internet of Things (IoT) is rapidly growing as network connectivity blurs the line between computing devices, appliances, vehicles, and industrial equipment. IoT is used to create smart homes and offices, network enabled appliances, aircraft, automobiles, ships, and trains. It is found across diverse markets including industry, research, agriculture, energy, healthcare, and manufacturing.

Cybersecurity experts warn about the vulnerabilities that IoT may introduce to other, traditionally secure infrastructure in return for the benefits that the technology brings.

Many manufacturers of security cameras have typically considered their products to be edge devices, relying on the IT department to provide the necessary network protection, limiting access only to those authorized while excluding external threats. Today more manufacturers and their customers are aware that anything connected to the network requires cybersecurity protection.

The Challenge for Security Manufacturers

One challenge for manufacturers of network-enabled security products is to balance ease of installation and ongoing operation with the protection of the device, the network, and the connected infrastructure.

A product with extremely strong cybersecurity protection may turn away customers by being too restrictive or complex for their needs when setting up or during ongoing operation. Equally important, a product that is exceptionally easy to setup and administer may be a gateway to cyberattack. Finding the balance between these two factors while meeting the requirements of IT is a challenge to be solved by manufacturers since not every organization has identical needs.

Arecont Vision Costar addresses this challenge with user IDs/passwords and our own in-house designed architecture for our MegaIP™ megapixel cameras.

Arecont Vision Costar MegaIP™ cameras feature the ability to set user IDs and 16-digit ASCII passwords (use of which is recommended) for basic cybersecurity, and we provide systems integrator and customer training on best security practices through Arecont Vision Costar University™.

As further protection, the design of all Arecont Vision Costar MegaIP cameras differs from competitor offerings. Arecont Vision Costar's Massively Parallel Image Processing™ architecture runs on a Field Programmable Gate Array (FPGA) integrated circuit (IC) in each MegaIP camera. This ensures that the camera cannot be used as a platform for cyberattacks.

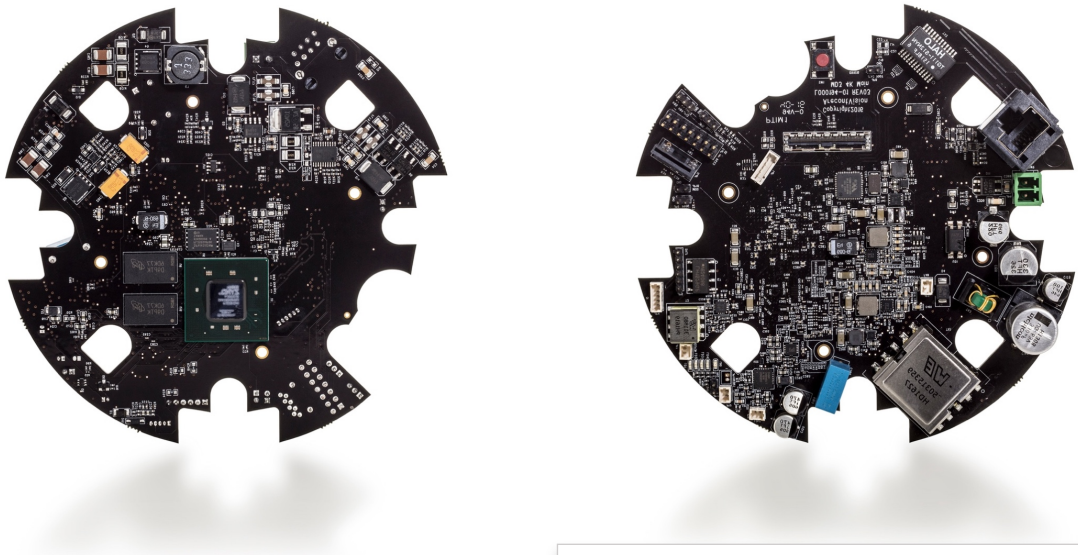
Field Programmable Gate Array

At the core of every Arecont Vision Costar MegaIP™ megapixel camera is an FPGA (Field Programmable Gate Array) integrated circuit, mounted on an Arecont Vision Costar-designed Printed Circuit Board (PCB). The individual PCBs vary based upon the design, capabilities, and features of the individual camera. The MegaIP architecture is in its 5th generation across our single sensor camera platforms such as MegaVideo® and our multi-sensor SurroundVideo® families.

Arecont Vision Costar develops the core code used in our architecture. This eliminates the risk of malicious code being unknowingly introduced when using off-the-shelf 3rd party solutions to deliver camera features and capabilities as other vendors may do. This also eliminates the risk of our cameras being hijacked for other purposes than they were intended for, such as unknowingly hosting a cyberattack on other devices.

The Arecont Vision Costar MegaIP architecture enhances camera performance, reduces time to market for new features, and offers superior upgradeability of security updates and new and improved features.

This architecture and the FPGA integrated circuit are key to the cybersecurity protection offered by all MegaIP camera models.



Top: Arecont Vision Costar MegaIP integrated circuit board on left, flip side of the IC board on right.

Right: MegaIP circuit board in design.

FPGA vs. ASIC Camera Technology

Most surveillance camera vendors build their products based on ASIC (Application Specific Integrated Circuit) chips as the camera processor on which to run a common operating system. The business model for the use of ASICs is to reduce manufacturing costs and time to market.

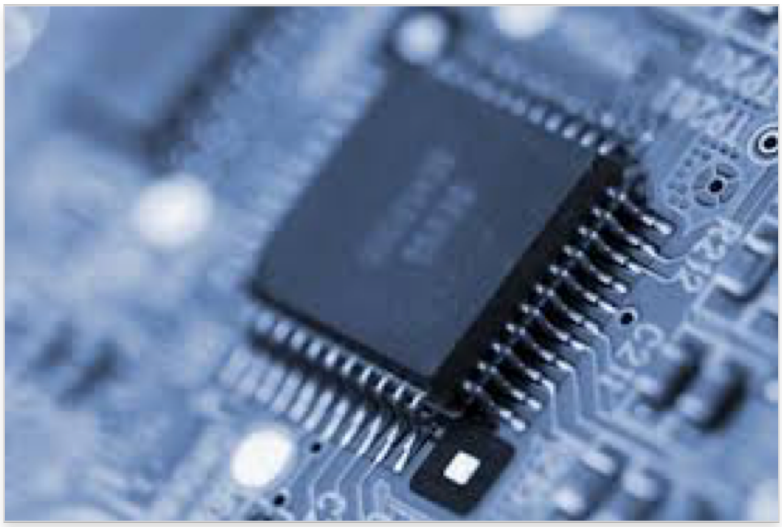
Vendors load a common operating system, their software, and any purchased or licensed 3rd party code for additional features and capabilities onto the ASIC chip at the core of the camera, which is duplicated in mass quantities for one or more camera models.

ASIC-based competitive cameras are typically limited to minor updates and fixes. New features and enhanced capabilities are more complex, and usually cannot be applied. This results in the customer being required to buy a new camera to benefit from the new features or capabilities. More importantly, major enhancements to the camera's security cannot be applied, only minor updates.

Arecont Vision Costar MegaIP™ cameras (MegaBall®, MegaDome®, MegaVideo®, MegaView®, MicroBullet®, MicroDome®, and SurroundVideo® families) are different.

The MegaIP camera architecture runs on an FPGA integrated circuit and can be updated after installation. Our R&D teams develop new features, image enhancements, reduced bandwidth algorithms, security enhancements, and much more that can be updated on the camera architecture. The camera's built-in webpage can be used for an update, or the AV IP Utility can be used to update one or many cameras simultaneously [see https://tinyurl.com/y8ngrxu7 for more information on updates].

By enabling new features to be added or updates to be made, Arecont Vision Costar MegaIP cameras offer an extended useful lifespan for the customer and allow both minor and major security enhancements to be applied. These capabilities protect both customer cybersecurity and their investment in MegaIP.



Note that Arecont Vision Costar ConteraIP™ cameras take a different route to deliver excellent cybersecurity protection from the MegaIP™ family. ConteraIP cameras, instead of FGPA technology, are based on an advanced System-on-a-Chip (SoC) architecture, which can be updated with the latest firmware fixes and security updates. When used in conjunction with ConteraVMS™, ConteraIP cameras gain additional cybersecurity features reliant delivered by ConteraWS™, rather than in the camera as in MegaIP.

Learn more about the Total Video Solution™ and its components, including both Arecont Vision Costar MegaIP and ConteraIP megapixel cameras here: https://tinyurl.com/ycy88j65

Mitigating Cybersecurity Risks with MegaIP™

Arecont Vision Costar MegaIP™ cameras are designed from the ground up to protect and safeguard against cybersecurity risks.

When a hacker accesses an Internet-connected device such as a camera, NVR, or server that is running Linux or another common operating system, it can be at risk. A cyberattack often begins with a malicious virus being loaded that infects the system via the operating system. In some types of robotic cyberattacks, this is often referred to as a bot shell script.

This script can then be used to take over the device. The bot can then launch various cyberattacks on other network-connected devices such as for Distributed Denial of Service (DDoS), ransomware, or false identity/network intrusion attacks. Other approaches can also be used to attack network enabled devices that rely on common operation systems and plug-in 3rd party application code.

Arecont Vision Costar MegaIP megapixel cameras do not have these vulnerabilities. This is because each of our cameras uses an FPGA IC on which we run Arecont Vision Costar's in house developed, proprietary Massively Parallel Image Processing (MPIP) architecture. We do not run common operating systems such as Linux, which are employed by other camera vendors. Known avenues of attack are eliminated by using this model.

Should a hacker illicitly gain access to a MegaIP camera or obtain the user ID and 16-digit ASCII password to log into a camera, the attack effort would be extremely limited in its success. The attacker would be able to view the camera's internal web browser, and the camera's settings could be modified.

A hacker would not be able to repurpose a MegaIP camera for a cyberattack. For example, the hacker, virus, or bot would be unable to load and run a shell script to maliciously attack other networked devices, either on the local network or across the wider Internet.

Anything that the hacker or bot could do would be limited to that specific Arecont Vision Costar MegaIP camera, rather than becoming an entry point for further cyberattacks.

Examples of Cybersecurity Attacks Impacting Security

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/ydy7l786 and http://tinyurl.com/ydajthdq

9/17: Security camera show 'HACKED' in live feed video https://tinyurl.com/ybh7hkpe

11/17: Years after regulatory crackdown, some security cameras still open to hackers https://tinyurl.com/y9kn8yem

1/18: That Intel chip problem? It's now a far worse security issue http://tinyurl.com/ycoxf2dv

5/18: Hackers can peek through surveillance cameras, report says https://tinyurl.com/yadovbdr

5/18: Exposed Video Streams: How Hackers Abuse Surveillance Cameras https://tinyurl.com/y9yhk2xg

6/18: Smart Home Security Camera Sends Footage to Wrong Person, Is Maybe Not So Smart After All http://tinyurl.com/y9oz2m53

8/17: New US Law Bans Hikvision & Dahua Products https://tinyurl.com/yd6uyrwk

9/17: Peekaboo vulnerability exposes hundreds of thousands of security cameras to hacking

9/18: New Bug Leaves Surveillance Cameras Vulnerable to Hacking https://tinyurl.com/yc5s2ub9

10/18: The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies https://tinyurl.com/ycywjdmo

10/18: What Makes IP Cameras Easy to Hack? https://tinyurl.com/yauebpy6

11/18: Five of the Worst Cybersecurity Breaches of 2018 https://tinyurl.com/yd9jhg4j

11/18: Canadian Intelligence Warns Against Buying Tech from State-Owned Companies https://tinyurl.com/y89oygkd

Cybersecurity Information Sources

A good source of related information is the Security Industry Association (SIA) Cybersecurity Advisory Board. You can find the Board online at https://tinyurl.com/ybujl6np. Arecont Vision Costar is a supporter of the SIA and the CAB.

Other sources of public information that are excellent starting points at time of writing are as follows:

- **ASIS International / Cybersecurity**
  https://tinyurl.com/ydy9w9u9
- **Association of Southeast Asian Nations / Regional Forum Statement by the Ministers of Foreign Affairs on Cooperation in Ensuring Cybersecurity**
  https://tinyurl.com/y9724b6x
- **Center for Strategic and International Studies / Updating US Federal Cybersecurity Policy and Guidance**
  https://tinyurl.com/y7xpjko8
- **Council on Foreign Relations / Cybersecurity**
  https://tinyurl.com/yaohyrm2
- **Cybersecurity Policy and Research Institute / Cybersecurity**
  https://tinyurl.com/ybd9xgwm
- **EDUCAUSE / Cybersecurity Policy**
  https://tinyurl.com/ybgrcu8v

- Electronic Privacy Information Center / Cybersecurity Privacy Practical Implications
  https://tinyurl.com/y7c7qjhf
- European Union Agency for Network and Information Security / National Cybersecurity Strategies in the World
  https://tinyurl.com/ya6ze5zx
- Federal Communications Commission / Cybersecurity for Small Business
  https://tinyurl.com/y9f74qaw
- Federal Communications Commission / Cybersecurity Planning Guide
  https://tinyurl.com/yd9btkwl
- Federal Financial Institutes Examination Council / Cybersecurity Threat and Vulnerability Monitoring and Sharing
  https://tinyurl.com/ydheuelq
- Federal Food and Drug Administration / Guidance for Industry: Cybersecurity for Networked Medical Devices
  https://tinyurl.com/ybnnzlzd
- Organization for Economic Co-operation and Development / Cybersecurity Policy Making at a Turning Point
  https://tinyurl.com/y763pchy
- PSA Security Network / Cybersecurity Advisory Committee
  https://tinyurl.com/ybqj4443
- Security Research Alliance / Designed-In Cybersecurity for Cyber-Physical Systems
  https://tinyurl.com/y8d3a53t

There are many more sources of useful cybersecurity information that you can find online or through industry and government groups, as well as standards bodies and educational institutions.

Conclusion

Cybersecurity threats are increasing, and video surveillance systems are not excluded from the resulting risks. Arecont Vision Costar MegaIP™ cameras have not been compromised and used in cyberattacks. Other brands of cameras have been successfully attacked and maliciously repurposed.

Arecont Vision Costar MegaIP camera families (MegaBall®, MegaDome®, MegaVideo®, MegaView®, MicroBullet®, MicroDome®, and SurroundVideo® families) are uniquely cyber protected within the camera itself. This is as a direct result of Arecont Vision Costar's in house-developed Massively Parallel Image Processing™ (MPIP) architecture that runs on the Field Programmable Gate Array (FPGA) integrated circuit. The FPGA is at the core of every MegaIP megapixel single- and multi-sensor camera.

Security updates and new product features can be applied to the architecture of existing Arecont Vision Costar MegaIP cameras when new firmware releases are available from Arecont Vision Costar R&D teams. This extends the useful life of the camera while maintaining their cybersecurity protection.

Balancing the user experience with adequate cybersecurity protection remains at the forefront of MegaIP camera design. Our ConteraIP™ cameras offer a different route to cybersecurity, including security and firmware updates, in conjunction with ConteraVMS™ and ConteraWS™ web services. Both families are ideal choices for security needs.

Well-designed products, employee education, planning, security best practices, and cyber awareness are the keys to any organization's readiness for the challenges of cyberattacks. Arecont Vision Costar supports our customers in each of these areas through products, services, and education.

Arecont Vision Costar MegaIP cameras are an important part of responsible cybersecurity actions for organizations of all sizes protecting their video surveillance systems and infrastructure.

Recommendations

1. Arecont Vision Costar MegaIP™ megapixel cameras should be considered for any video surveillance project. Organizations continue to rely on MegaIP cameras to not be hacked and repurposed in cyberattacks on other networked devices.

2. Arecont Vision Costar MegaIP cameras will continue to balance the user experience with appropriate cybersecurity, including the recommended use of 16-digit ASCII passwords after the camera is configured for use by the installer. No device should be connected to the network without this capability enabled, including surveillance cameras.

3. Cameras that cannot be updated with the latest product features and security updates from the manufacturer should not be part of the network and should be replaced.

4. Cameras with known security risks due to use of common operating systems such as Linux and including use of 3rd party software instead of their own in house developed applications for core functions and features should not be part of the network and should be replaced.

5. Customers should employ best practices in cooperation between the IT and security departments for basic cybersecurity. Having a cybersecurity action plan that is tailored to the needs of the organization is important.

6. Employee education is key to cybersecurity and should be a part of ongoing employee development.

7. Use the Arecont Vision Costar Try-and-Buy program to obtain and install an Arecont Vision Costar MegaIP or ConteraIP™ camera risk-free for a trial at the customer site. It can be purchased at a special price after a free 30-day trial to demonstrate its real-life advantages [see current promotions at https://tinyurl.com/y8dhxdos].

8. Contact Arecont Vision Costar today to discuss your project needs or to learn more.

- Look up the Arecont Vision Costar contacts for your region around the world online here: https://tinyurl.com/yc3om7w3
- Request information at: https://tinyurl.com/ya54mc99

Learn More

Visit us online | www.arecontvision.com

Email us | sales@arecontvision.com

Call our corporate headquarters | +1.818.937.0700

Like us on Facebook | facebook.com/arecontvision

Follow us on Twitter | twitter.com/arecontvision @arecontvision

Connect with us on Linkedin | linkedin.com/company/arecont-vision

Subscribe on YouTube | youtube.com/user/ArecontVision

News Blog. Read our Blog | http://blog.arecontvision.com

AV COSTAR in the News. Get the latest news on Arecont Vision Costar with press releases, videos, events, webinars and more | https://www.arecontvision.com/new

Arecont Vision®
A COSTAR COMPANY

Arecont Vision Costar
425 E. Colorado St. 7th Floor
Glendale, CA 91205 | USA

+1.818.937.0700 | www.arecontvision.com | avsales@arecontvision.com