Arecont Vision
Leading the Way in Megapixel Video™

ARECONT VISION TECHNICAL UPDATE

Issued 14 March 2017

Number: TU-3/14/17 CyberPositioning

Arecont Vision Cybersecurity Positioning

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/yrvstv & *Hikvision devices open to hackers* https://goo.gl/PtHq7r
- 2/16: *Cameras reported to "phone home to China" with your video* https://goo.gl/MWJ35T
- 9/16: *DDoS on Krebsecurity.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/QAzl04
- 11/16: *Security camera infected by malware 98 seconds after plugged in* https://goo.gl/pu8fA0
- 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/NkuKGW, and *DC and South Dallas cyberattacks* https://goo.gl/XmhIhr
- 3/17: *Racz speaks out on why Genetec sees Hikvision products as security risks; Hikvision to Genetec: "Vague accusations and outrageous claims"* https://goo.gl/xHBvzj
- 3/10: *Dahua, Hikvision IoT Devices Under Siege* https://goo.gl/sO9snH

Arecont Vision®

Leading the Way in Megapixel Video™

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 MegaLab™ test and certification facility, which in 2016 opened participation to network infrastructure and cybersecurity vendor solutions [*see press release at https://goo.gl/zymbXN*]. Dozens of video management system (VMS), network video recorder (NVR), analytics, utility, and infrastructure vendors have participated and tested their products through the MegaLab 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.