MARCH 2022 // EBOOK

svconline.com

SOUND&VIDEO CONTRACTOR

REVIEWS | TECHNOLOGY | APPLICATIONS

IS AVoIP SAFE?

IS AVoIP SAFE?

Along with the challenges that the AV industry has faced due to the movement toward IP technology, there’s also been additional uncertainty caused by the ongoing news related to cybersecurity.

By Phil Hippensteel and Cynthia Wisehart

Security is an increasing reality, which means networks must do more than efficiently and successfully move signal. AV elements must be secure and trustworthy network citizens. AV systems integrators must be able to participate in the design of secure systems, which means both helping to protect the signal integrity and bandwidth management of the network infrastructure, as well as being an engaged and knowledgeable partner on issues of network security. Additionally, integrators must understand what is needed from manufacturers to provide a range of security levels that work in the real world. In the eternal tradeoff of convenience/usability and security, there is no one best answer, no set of clear-cut have-tos. Rather what is needed is awareness of the issues and technical fundamentals and willingness to understand what matters to customers and IT partners. AV integrators have a role to play in facilitating dialog and specifications. They have a unique viewpoint on how tradeoffs between user and experience and security play out, especially in bandwidth and resolution intensive situations where latency is not an option.

The IT industry has been confronted the problem of cybersecurity for decades and they understand it through their own lens and experience, and through the ways they have quantified it through guidance and more formally through standards. Typically, security experts have framed guidance and goals that include:

- Confidentiality
- Integrity
- Authenticity
- Availability

Our AV systems should be able to transmit media while preventing interception and misuse by unauthorized persons. Unauthorized persons should not be able to modify media that is transmitted in order to ensure its integrity. The third item—authenticity--is critical as we need to be sure of who is sending and who is receiving all messages or media. Finally, we must ensure that our systems and media transmissions cannot be stopped or redirected away from an intended destination.

Following the lead of IT managers, the broadcast industry began to focus on these goals nearly a decade ago through the work of the Joint Taskforce on Networked Media (JT-NM). In its Cybersecurity Final Report 2020, it provided many examples of failures to achieve these goals and was critical of attitudes that offered flimsy excuses. For example, saying devices are on a closed network or shouldn't be connected to the Internet isn't acceptable. What is a "closed" network? Should we trust everyone in our large company or university?

This begs the question whether the AV industry doing the same thing. We also are likewise concerned with what IT managers think of AV security. Looking back at the conversion of telephony to IP, we learned that major manufacturers of telephone equipment needed to accelerate their understanding of IP and its related security implications. Those that did this survived and worked within IT. Other companies pulled out of the telecommunications industry. A similar cycle will undoubtedly occur as the IT and security expectations of AV systems mature.

For many manufacturers that process is already well underway. For example, Andrew Ludke, Sr. Director, Product Management AV Solutions at Crestron cites examples of their approach like authenticating using Active Directory or LDAP. As evidence of their security consciousness he cited the fact that they are certified by FIPS, NIAP and JITC, which are all government programs. For many customers of the DM-NVX series of products, secure distribution of configurations is a necessity. Remote access using command line is possible but only with HTTPS from a browser and with SSH and PKI encrypted key exchanges. These are protocols used by financial institutions.

Joe da Silva, Director of Product Marketing at Extron said that security is "in the forefront of the design process, never an afterthought." As an example he pointed to their NAV Pro AV series of products. These use 802.1x port authentication for pre-admission access control. Additionally, all control messages use AES-256 encryption, which is widely accepted by IT.

SECURITY STARTS WITH PRODUCT DEVELOPMENT

As AV/IT matures, more and more of the underlying practices of IT security come into our world. As APIs, firmware updates, and IoT-based

CONVERSATIONS

DVIGEAR

Steven Barlow and Matthew Pulsipher of DVIGear say that most of their customers put their equipment on a dedicated network which isn't part of the corporate network—a very common practice in integrated AV/IT networks. Even with that precaution, Barlow said that their SDVoE servers also maintain one communications port for control and one port for media. The communications port uses SSH for remote control and command execution. They also do not use back door passwords. To learn the SDVoE command set, the servers allow the creation of a sandbox, preventing the accidental execution of malicious commands while hastening the understanding of the command set. –Phil Hippensteel

MATROX

Matrox's Samuel Recine is the current active chairperson for the ProAV working group in AIMS. AIMS is active on standards initiatives support SMPTE ST-2110, and the Pro-AV tailored IPMX (IP Media Experience) standard. According to Recine, the security situation in ProAV is constantly improving. He says the push to adopt better security isn't always coming from the manufacturers or systems integrators. It's primarily coming from the end consumers and IT department standards where cybersecurity is priority one. Recine also says that the thinking that internal networks can be "easier to work with" versus what's outside the organization's firewalls is increasingly giving way to John Kindervag's "Zero Trust" model. It advocates the benefits of simplicity and commonality of approaches when treating "all" assets, including those inside firewalls, with the exact same rigor. Recine points out that up to this point, manufacturers have adapted well and have made strides. For example, SRT delivered meaningful improvements over RTMP. However, Recine also feels there is still significant improvement available. Most of the media payloads (video, audio, keyboard strokes, mouse clicks, etc.) in Pro AV networks are still secured mostly with individual approaches by vendors. The communication and control layer of Pro AV products is mostly shifting to HTTPS, which leverages TLS and AES encryption. This allows IT managers to screen their different types of products from different brands with a common approach. Recine feels the inevitable next step for Pro AV media payloads through standardization efforts such as IPMX. –Phil Hippensteel

ATLONA

Paul Krizan, Product Manager in Networked AV at Atlona said 15 years ago, security wasn't a requirement. He said, now, it is. Consequently, they are hardening all their devices. Like some others, Atlona is encrypting configuration data and web pages that are used in the configuration process. Some of their devices allow multiple levels of users. This can allow more granular control over who makes changes. As an example of their security consciousness, he pointed out that their Omni-Stream Products use 802.1x port authentication. He also mentioned the use of security scans after each firmware change. This is consistent with R143 mentioned previously. –Phil Hippensteel devices proliferate in AV, the chain of trust starts with knowing that product development and updates are done in a secure, traceable way. Ideally, code is encrypted and signed, and FIPS compliance ensures that there has been no tampering. When something goes online at a facility it has followed a known path from developer to manufacture to distribution to customers.

That's an ideal, and even in consumer devices security can be uneven. Sometimes the tradeoffs between perfect compliance and efficiency are out of proportion for the relatively low risk of the application. It's still worthwhile for integrators to ask and understand how rigorous a manufacturer is with securing the life cycle of a device and its components from tampering. IT people care about that; it's a good thing to know about the products you spec, just like knowing the latency, resolution, and features. Many manufacturers are implementing time-tested security practices from IT to help ensure their devices and components are not a potential soft spot. Or if the AV device is a potential soft spot, the integrator is at least conversant in the tradeoffs. Just being knowledgeable about the options builds trust with IT partners. On the one hand, that FIPS-certification may be a key selling point, on the other hand, if it's too pricey just being aware of the tradeoffs and candid about them enhances an integrator's professional credibility with an IT person.

AV pros may also want to educate themselves about dependencies—the software manufacturers acquire from encryption libraries, whether open source or paid dependencies. Large companies audit this as a matter of basic practice. Again, in AV there are reasonable tradeoffs—the open source code that provides greater functionality may not be as secure; the functionality may be more important. Increasingly it may behoove integrators to have someone on staff who understands IT security and can talk to product vendors, who can ask the questions about third party dependencies, DevOps cycle precautions, and the development chain from source code to shipment to service. Knowledge is power, and the more integrators ask about security, the more incentivized manufacturers are to meet those needs. There may be a lot of customers who are fine without all the rigor of DevOps security, but getting a sense for how seriously a manufacturer takes security is one more aspect for evaluation and weighting.

ACCESS CONTROL AND ENCRYPTION

Above the device level, security is about access control and encryption of content. Here's where integrators can bring a lot of value to the in-the-field side of security. You want to see products using common protocols for traffic and directories, which makes deployment, provisioning, and access control more seamless.

On the content encryption side, 802.1x is what IT pros like to see, as it means that device will be encrypted on their network. But, in the spirit of tradeoffs, it also means anyone else on the network can technically see that traffic, so it is not ideal for sensitive video without secondary controls to ensure only authorized users can see it. Control is an area where the AV industry has made strides both in terms of commissioning and directory management but also in terms of human involvement. The industry's long history of empowering users has matured to put more access control and encryption power into the control software that drives AV systems. Off-the-shelf AV-friendly switches have also contributed additional security features and brought AV and IT closer together.

WHAT DO IT PROS THINK?

Let's take two IT managers at a very large financial institution. They preferred not to be identified except to mention that the company has a multinational presence.

One way their IT department has related to video is through the physical security department. That's where the responsibility for thousands of security cameras falls. Individuals in that department seem to feel that they had little to be concerned with except who can see the video. However, they said, the video could violate privacy, reveal company secrets, or more. One manager told us that the camera security was so weak, he could defeat any camera. The managers also suggested that real security is more than just passwords and authenticity. Today, it involves profiling individuals and systems that try to have access to your systems and devices as more than one level of scrutiny may be necessary. In their company, they typically have three firewalls and even business partners must pass through those to get access to financial records. In addition, they suggested that an unauthorized person may have state-sponsorship. A key lesson that we can learn from this financial institution's IT department is how they think of audio and video - they're just another form of data on the network, and just as vulnerable.

As an associate professor of computer science, Dr. Scott Weaver at Messiah University has this to add about the surge of consumer of collaboration tools like Zoom and Teams, which are easy to use without proper authentication. It isn't that the tools don't provide the functionality. The problem is that users don't choose to implement these tools. Consequently, unauthorized persons can join his classes. The only reasonably secure way to prevent this is to require that each participant's camera be turned on and aimed at his or her own face. However, that increases bandwidth requirements. It may also be impossible in large classes due to the tiling issue on screens. We concluded that the same kind of issues can arise relative to protecting intellectual property in a commercial environment. Employees that are less than diligent might have other persons monitoring collaboration calls who were never invited to be a part of the call. So just as video and audio are just data on the network, the human factor is always one of the security soft spots.

STEPS TO TAKE

Most important is to educate yourself and your employees about new security issues and protections. Invest in security. Five-year-old security technology should be thought of as completely antiquated. Technically competent security professionals demand premium salaries. Many need to be recruited from the IT industry. But with a eye towards the future they could be worth it.

Also, you can investigate vendors that supply equipment. Don't work with those that have poor security policies like device backdoors and remote connections using unencrypted traffic. If possible, insist on proper authentication procedures including certificates. Never, never allow default passwords to go unchanged. Some hackers use software that roams the Internet looking for combinations like root/root and admin/admin. Sadly, they sometimes find a victim. Use or hire someone who knows how to use the many security scanning tools that are available. Open ports are an invitation to attackers.

One suggestion comes from Jack Douglass, Vice President of Business Development at PacketStorm Communications. Douglass sits on and chairs several industry groups that develop standards. He suggests that you emulate the environment in which your deployment will take place. Then use that emulated network to put your AV devices through their paces. PacketStorm was an Emmy Award Winner for their 6XG Network Emulator. It can create an environment that nearly perfectly matches the real-world situation that will be used for deployment--just in a box in a lab. In this way you can safely use all the scanning and penetrations tools, test remote configurations, and carry out other necessary tasks.

CAN STANDARDS HELP?

Andrew Starks, Director of Product Management for Macnica, also sits on the board leadership for the AIMS Alliance and is active in the IPMX standard. “A standard can say that product A and B meet certain standards and can interoperate in a secure way—that is support a common set of protocols and a baseline way to a defined outcome. We can say ‘security should support this and this is how it’s done’. Standards don’t actually change anything; they specify how things should be done and maximize interoperability. That’s at a different level than all the security practices and protocols. Everybody can do security just fine on their own. If you want to do it interoperably you have to agree.

“In truth there is an awful lot that can be done with an insecure system. And the most secure systems are often that way because they don’t get to use the latest drivers and they’re hardware encrypted. So there are tradeoffs. Many in this industry do take security very seriously but if we want to say security is the most important thing it’s really not—accessibility and functionality are the most important things if we’re honest. We’re always going to have this tension with IT.” But the more you know about security and the security needs of your customers, the more you can make a system as secure as possible within their risk tolerance and accessibility needs, and the reasonable level of security for the value of the things they’re protecting.

“This conversation will continue to matter,” he says and emphasizes that security can be improved at the device manufacturing level without doing anything to affect accessibility. “We need to keep asking questions about that. It can look like a cost or look like a pain, but then you do it and realize you should have been doing it all along. Security is something we are going to be asking ourselves about repeatedly for the foreseeable future. It’s hard to think what part of AV it doesn’t touch.”

CONVERSATIONS

AURORA MULTIMEDIA

Aurora’s Paul Harris tied the security goals of Confidentiality, Integrity, Authenticity, and Availability to SDVoE, which Aurora integrates in many of their products. In implementing this technology, he said there should be constant screening of the mac addresses on the network by having lookup lists. He also says an SDVoE network should be viewed as a matrix switch from the integrator’s viewpoint with the understanding that that they have the same level of responsibility for it as they would with a matrix. Too often the integrator and the IT department may have disagreements about who is responsible for issues that develop. Harris was also very positive on Netgear’s development of IGMP Plus, which makes deployment and maintenance of the multicast network easy. That is in line with goal four – availability. Since SDVoE is aimed toward implementing 10G video transport, it claims to be inherently more secure since it won’t be on the wide area network. –Phil Hippensteel

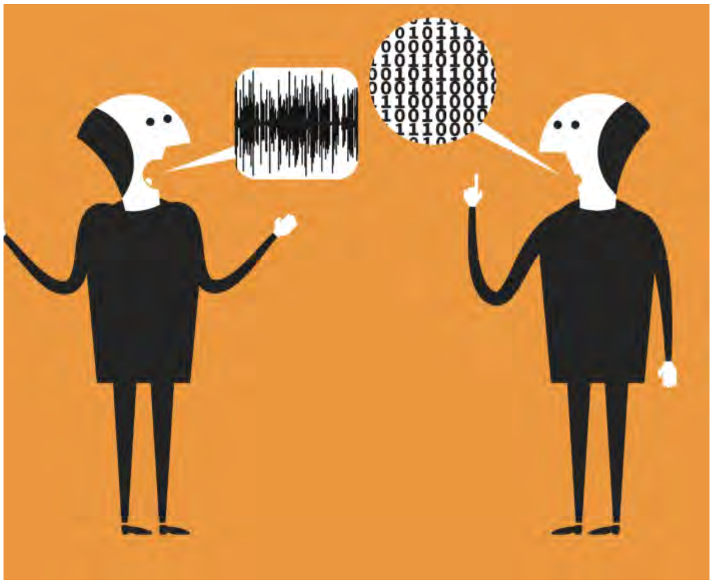
DATAPATH

Are there situations where using an isolated network for AV makes sense? Datapath representatives made a compelling argument. Mark Bohs and Mike Moore told us about their customers’ requirements and how they fit their products to meet these needs. They said that most of their installations are in control environments such as EMS centers, law enforcement centers, and university security centers. New configurations and firmware upgrades are done by individuals on-site. If the video is moved from one site to another, the responsibility is assumed by the company or agency IT department. While Datapath is thinking about methods to securely move videoamong locations, they are waiting for that part of the market to stabilize on a few methods that are based on standards. They are currently choosing some features from the 2110 standards. However, presently 10G Ethernet using RTP is satisfactorily moving video and control data between processors and screens for their applications. –Phil Hippensteel

AUDINATE

Audinate says the company is applying some of the proven insights of the IT realm to AV by monitoring and managing the network such as limiting access to authorized personnel only, logging access to the network and providing audit trails, and providing IT-grade administration tools. Dante Domain Manager was conceived to couple AV-grade performance with IT-grade network control and security. This means security awareness at the directory and control levels, but Audinate also sees their role in helping with access control and secure distribution of content—whether that’s preventing networking hijacking or protecting revenue-generating assets, making sure content is shared to the right zones, subnets and audiences. It is critical that AV professionals elevate network security as a must-have for these applications and an increasing array of applications – from healthcare and industrial settings to transportation and performing arts environments. This elevates the value of the AV professional to end-users, and it places AV professionals in the same conversations and at the same level as our IT counterparts. -Cynthia Wisehart

DO YOU SPEAK IT?



Using the words "smooth transition" when it comes to implementing networked AV might be a stretch if there is a lack of communication between the AV and IT departments.

Cindy Davis (AVTechnology , AV Network)

The AV and IT departments of many corporate companies and institutions of higher education have joined forces as one. However, it's clear that almost as many have not, and communication between them is at best, a challenge.

If you want to avoid the dreaded four words, "not on my network" it will help to understand some IT needs and terms when talking to the head of the department.

THE LANGUAGE BARRIER BETWEEN AV AND IT

There's a language barrier that isn't helped by the fact that there's not a published common set of AV standards. The IT world, on the other hand, references a 3-inch-thick book of standards from the Institute of Electrical and Electronics Engineers (IEEE).

It is incumbent on AV manufacturers to provide and support the AV team with the language needed for IT to see that a product is compliant. For instance, a manufacturer should be able to confidently state that a product supports 802.1X, an IEEE standard for port-based Network Access Control (PNAC). This provides an authentication mechanism to devices wishing to connect to a LAN or WLAN.

AV STARTING POINTS FOR TALKING TO IT

Paul Zielie, consulting solutions architect at AVCoIP LLC recommends starting with an accurate scope of the project, and answer these questions first:

1. What is the business value, including the internal sponsorship the project brings?

2. How many devices need to be added to the network, and where they will physically reside?

3. Where will network traffic be required? Will admin or user computers need to access the devices? Will the devices need to get to the internet or the wide area?

Brushing up on the language of an IT networking professional so you can fluidly communicate with them can help. Remember, you are playing in their sandbox, and they are responsible for protecting the data of your enterprise, and every device that goes on the network is a risk.

Phil Hippensteel, an instructor at Penn State Harrisburg, said AV managers should have a good understanding of the following before going to the IT department:

1. How variable subnet masks work, e.g., 255.255.255.224
2. The differences between TCP and UDP traffic
3. How ARP, DNS, and DHCP work.

BE READY TO ARTICULATE WHY

An IT manager knows the network benefits of communications systems such as email and VOIP, as well as access to servers and printers. A convincing case for why AV belongs on the network will sell the "why" to the IT folks.

"There are two primary benefits to using networked AV products," said Zielie. First is the scalability and cost efficiency of using existing, standardized infrastructure to implement AV services. Second is reducing the operational costs and decreasing incident response times associated with the AV application by leveraging the ability to remotely access AV equipment and perform troubleshooting and maintenance. Standardized infrastructure and reducing operational costs are familiar IT concepts, so you're speaking their language.

At the basic level, having networked AV products allow for centralized and streamlined control capabilities. Having each device on the network allows for easy deployment of code, firmware, and troubleshooting of devices.

PREPARING FOR A CONSTRUCTIVE AV ON THE NETWORK CONVERSATION

Helpful information you should bring to the IT department to have a constructive conversation include:

A basic network diagram of what you are trying to accomplish

Network ports that need to be open on the network for proper communication

Necessary VLAN configurations in order for proper isolation of communication protocols

Bandwidth requirements necessary at the local network switch and between network switches

A network risk assessment document detailing the security protocols of the various equipment being placed on the network

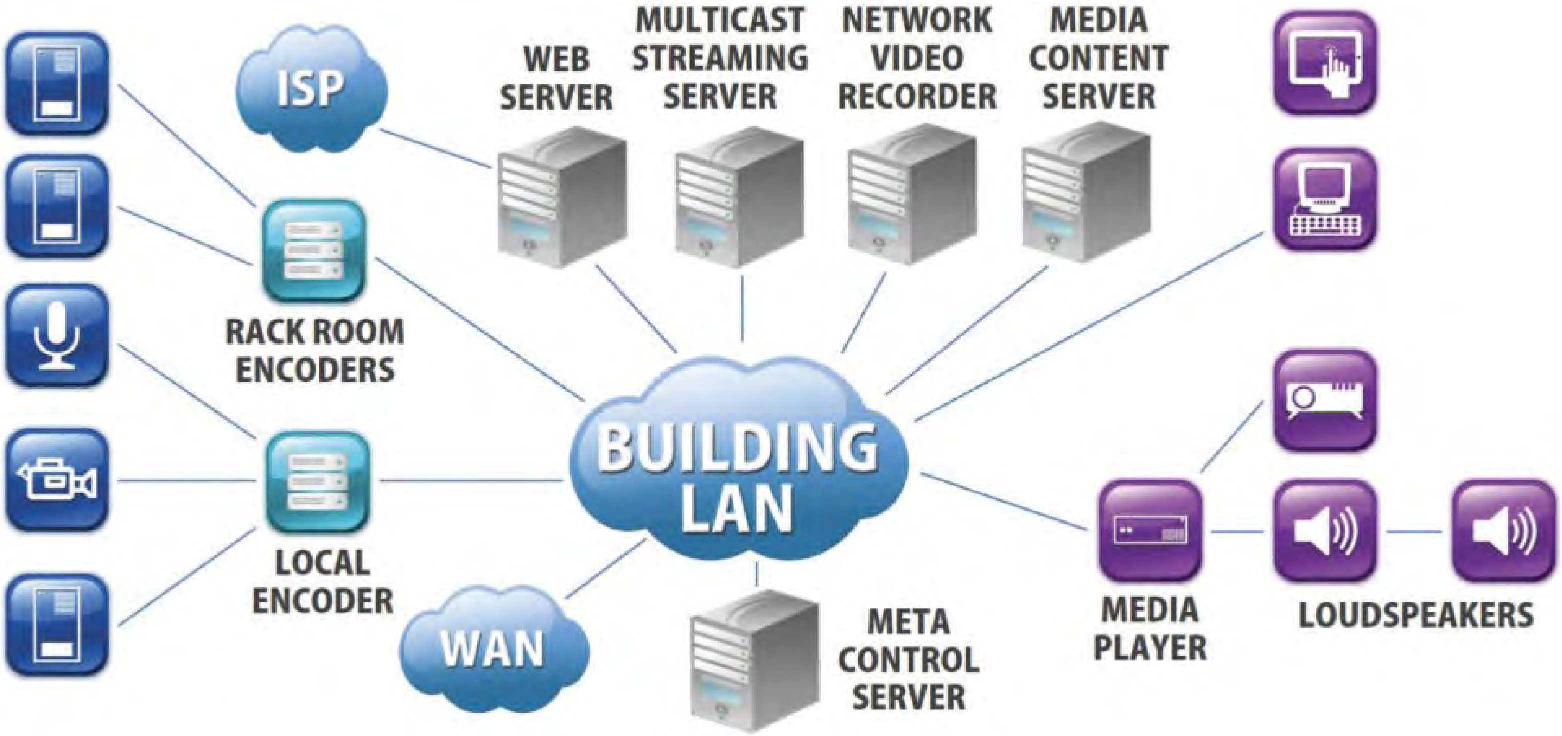
Is any special network hardware required? For instance, in the case of AVB, particular network switches must be used to handle the AVB traffic

An IP scheme concept for the equipment and an understanding of what devices are capable of doing. For instance, can a DNS name be set? Is the device capable of being set to a static IP address? How must other devices communicate with this device?

NAVIGATING

"You need to be able to understand and describe where the network traffic needs to go," said Zielie. Think of where the network traffic will be required—just between devices? Will admin or user computers need to access the devices? Will the devices need to get to the internet or the wide area?

"VLAN and multicast route requirements come out of the understanding of where network traffic will be required, possibly combined with the need for security or bandwidth control," Zielie said. "Your network people should be able to help you come up with the right combinations."



ADVERTORIAL

SECURE AV SOLUTIONS FOR A COMPLEX WORLD

With new threats mounting almost daily, cyber security is a top concern for AV signal distribution systems in every application. Customers insist on a high-level of security for the handling and distribution of their most guarded assets–their data. This data invariably takes the form of visual information that must be viewed and shared across the enterprise. But how can this information be distributed without risking unwanted theft, hacking or eavesdropping?

DisplayNet® – The Secure AVoIP Solution

DVIGear's DisplayNet is an award-winning product family for AV distribution that leverages proven 10G Ethernet technology to switch, extend and distribute uncompressed AV signals in real time with resolutions of up to 4K/60p. DisplayNet is built on the latest SDVoE technology and provides unmatched image quality with zero frame latency, minimal (if any) compression and zero artifacts. Unlike conventional matrix switchers, DisplayNet also integrates powerful features, such as software defined MultiViewer, an Advanced Video Wall controller, and a versatile Command Script Editor. These features enable a wide range of applications within a single system, replacing numerous dedicated components.

The DisplayNet platform has been built from the ground up to provide secure, scalable AV signal distribution. DisplayNet endpoints send and receive a myriad of AV signals across a dedicated 10G network using AES 128-bit encryption, which makes eavesdropping impossible. A DisplayNet Server is at the heart of each system and is designed to prevent rogue server attacks through various encrypted security measures. Each DisplayNet system can be customized to determine which endpoints are allowed to communicate with others in the system to provide a further level of secure isolation. In addition, all server / endpoint communications can be encrypted to avoid the possibility of eavesdropping. DisplayNet also provides a secure mechanism for interfacing with third party control systems so that its versatility as an open and easy-to-program platform is not compromised.

HyperLight® - The Secure Optical Cable Solution

For point-to-point video distribution, DVIGear's HyperLight® Active Optical Cables (AOC) provide the ultimate in signal quality, reliability, and security. These cables are compact, lightweight, and highly flexible, yet robust and unfailingly durable. Fully HDCP compliant, they support EDID and HDCP communication. Power is provided by the source device. HyperLight cables can support up to 8K resolution and are available in lengths up to 100 meters (328 ft.).

Unlike commodity-grade cables, Hyperlight AOC are designed for use in mission-critical applications where image quality, dependability and security are paramount. Video signals are transmitted over internal, plenum-rated optical fibers, making them immune to interference from environmental noise. More importantly, this optical transmission path provides a very low RFI / EMI profile, which allows the cables to be installed in sensitive applications with the strictest security requirements. This makes HyperLight cables ideally suited for a wide range of high-profile applications that require ultra-high-resolution signals to be extended over long distances without the risk of security issues.

CONTACT:

DVIGear Inc.
Tel: (888) 463-9927
Email: sales@dvigear.com
Web: www.dvigear.com/HyperLight
www.DisplayNet.com

DISPLAYNET®

Software-Defined AV Distribution

The Future of AV Distribution

DisplayNet® delivers the **performance** of traditional matrix switchers, with the **future readiness** of AV over IP. By leveraging cutting edge SDVoE technology, DisplayNet offers 4K/60 (4:4:4) video distribution with limitless scalability, zero-frame latency and zero image artifacts.

DisplayNet provides unique features such as **Software-Defined MultiViewer** and **Advanced Video Wall** that enable a wide range of applications without the expense of ancillary products. **Silent** operation, powerful **Network Security** features, versatile **KVM Routing** and support for **Dante®** digital audio provide system designers with exceptional versatility. A highly intuitive web-based UI and API greatly simplifies setup and installation, as well as integration into third-party control systems.

Contact us today to learn how **DisplayNet** can make your next AV system future ready.

ZERO COMPROMISE – **INFINITE** POSSIBILITIES

DVIGEAR® Dante® Powered by SDVoE® ALLIANCE

sales@dvigear.com | (888) 463-9927 | www.displaynet.com

Dante® is a registered trademark of Audinate Pty Ltd.