SCN SYSTEMS CONTRACTOR NEWS

CONTENT

VP/Content Creation Anthony Savona

Content Director Mark J. Pescatore, Ph.D.
mark.pescatore@futurenet.com

Content Manager Katie Makal,
katie.makal@futurenet.com

Contributor Jennifer Guhl

Group Art Director Nicole Cobban

Art Editor Rob Crossland

Production Managers
Nicole Schilling, Heather Tatrow

ADVERTISING SALES

Vice President, AV/Consumer Electronics & Pro Audio
Adam Goldstein, adam.goldstein@futurenet.com

SALES

John Casey, *john.casey@futurenet.com*
Janis Crowley, *janis.crowley@futurenet.com*
Zahra Majma, *zahra.majma@futurenet.com*
Debbie Rosenthal, *debbie.rosenthal@futurenet.com*
Andi Tureson *andi.tureson@futurenet.com*

FUTURE

Senior Vice President, B2B Rick Stamberger
VP, Sales & Publishing, B2B Aaron Kern
VP, B2B Tech Group Carmel King
VP, Sales, B2B Tech Group Adam Goldstein
Head of Production US & UK Mark Constance
Head of Design Rodney Dive

FUTURE US, INC.
130 West 42nd Street, 7th Floor
New York, NY 10036

Securing AV for the Future of Working

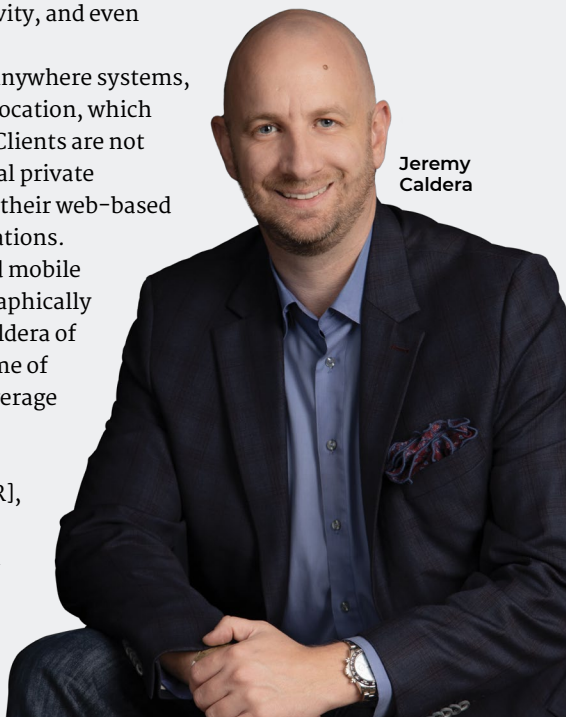
By Jennifer Guhl

Securing AV systems within a corporate setting isn't as easy as isolating an AV network. In the past, AV network security often wasn't given a second thought, leaving many networks open when the potential for risk was thought to be minimal. Now, with AV technology using shared wireless networks and organizational IT resources, AV systems are policed much more carefully. In response, AV experts have to work more closely with clients, especially with their internal IT teams, to navigate potential security risks associated with this new level of integration.

Hybrid workflows and remote learning systems, the use of which surged during the pandemic, are here to stay. Web-enabled devices and videoconferencing systems are now part of our everyday toolkit, and network architecture must include external connections for remote support, video collaboration, wireless sharing, lighting control, room booking, IPTV, and digital signage control. Mark Peterson, who leads Shen Milsom and Wilke's global audiovisual practice, said, "All these parallel network requirements make AV systems vulnerable to unintended access and data transfer into the session layer or even the transport layer, and denial-of-service attacks can cause severe network disruptions."

Since AV technology is now becoming closely integrated with organizational collaboration platforms like Microsoft Teams and Slack, the security risks and potential to disrupt many facets of everyday business has only increased. "If a single AV system stops working, it can disrupt internal and external communication," said Peterson. "Alternatively, if a virus gets into the network fabric, it could cost businesses revenue, productivity, and even reputational risk."

With the pandemic spurring adoption of work-from-anywhere systems, many companies no longer operate out of a central office location, which expands the potential security risks for the organization. Clients are not only looking to build secure networks consisting of a virtual private network (VPN), but ones that can also accommodate all of their web-based conferencing and communication-based tools and applications.


Jeremy Caldera

"Mobile videoconferencing applications and increased mobile bandwidth have resulted in AV endpoints dispersed geographically all over the country," said senior vice president Jeremy Caldera of technology and IT service provider Pearl Technology. "Some of these applications incorporate collaboration tools that leverage email, calendars, and other corporate network resources. Securing these mobile devices will require the 'zero trust' approach and the use of endpoint detection response [EDR], multi-factor authentication [MFA] solutions."

Companies are turning to applications like Duo, which provides MFA, remote access, device trust, single sign-on



Left to right: Steve Greenblatt, Anthony Mini, Mark Peterson

(SSO), and other secure access capabilities, when configuring security for their company's web-based applications. Peterson explained, "AV devices will need to support Duo's use of asymmetric cryptography to verify communications between cloud servers and AV apps running on smartphones in order to be trusted for use inside an enterprise's environment."

Many companies still use single sign-on (SSO), which AV web apps have relied on for years, but using the same login information to access multiple applications is not without risk. "Today, AV products need to support SAML 2.0, the latest version of the open standard protocol under SSO. It allows identity providers to pass authorization credentials to service providers using XML," said Peterson. "But SAML has its own risks, which is why clients are now asking for networked AV products to support Okta, a third-party SSO provider."

The cloud-based Otka platform provides clients with continuous monitoring of cyberthreats while maintaining secure access across thousands of applications and devices. It has the ability to cross-check access against on-premise applications, directories, and identity management systems to make sure employees receive the correct level of access within their organizational network, limiting potential security risks brought on by those within the company.

The pandemic-mediated growth of hybrid working environments, in which many or even most of a company's "office workers" actually work from their home or other remote location, has increased the demand for wireless content sharing, with AV networks needing to support internal networks, guest networks, and bring-your-own-meeting (BYOM) capabilities.

To decrease potential wireless security risks, corporate IT infrastructures need to be able to support multiple independent networks. "All content traffic between software clients and application servers needs to be encrypted in transit and at rest," said Peterson. "Sharing portals are intentionally advertising on open Wi-Fi networks; therefore, the product has to prevent the unauthorized installation of new software applications so that an attacker cannot reverse-engineer the update protocol intended to support a user's first-time use of the wireless sharing product." To support this effort, companies are beginning to embed firewalls that restrict users' ability to edit content.

Technology manufacturers, especially those that create devices that communicate with control systems and networks, are looking more seriously at security than ever before. Many are implementing security features in new products directly, as enhanced security features make them more attractive for use in the corporate AV market. "The benefits to the clients are that these products are going to become more widely accepted," said

With the working world forever changed by the pandemic and remote communication systems becoming increasingly complex, clients can't afford to work with AV partners that don't take security seriously.

Steve Greenblatt, president of Control Concepts, an independent control system solutions provider. "The AV industry is going to look that much better because they are not going to be introducing any potential vulnerabilities." The only downside to these embedded security features is that they can be more difficult to program and may require advanced software features to integrate easily into larger networks.

With potential security risks only increasing within corporate environments, IT and AV departments need to learn to become stronger partners and make sure security is considered when new AV solutions are being integrated into existing networks. "If security is bolted on after the fact, the system will typically have continued vulnerabilities or functionality issues," said Anthony Mini, senior vice president of security and operations at technology and IT service provider Pearl Technology. "Additionally, the cybersecurity departments will need to be aware of application vulnerabilities to AV systems and have insights to know what versions are running and how to patch these systems without breaking the configurations needed to ensure AV systems are functional."

IT teams also need to educate everyone within the company about potential security risks and what risks certain actions bring about. Greenblatt said, "Any employee connecting from an outside network that has potential vulnerabilities will need to have their computer protected. You need to make sure people understand that a public network leaves you exposed, putting your company at greater risk."

In the future, companies may work with third-party security testing firms to assess potential security risks within a manufacturer's product line before integrating those products into their AV network. Peterson said this is a good practice. "Ensuring a secure web application is an ongoing process, and third-party assessments are good investments because testing requires both dynamic application testing and business logic assessments," he explained. Automated testing of web-based applications is also an option, but it requires continued updates and retooling to mitigate potential new external threats.

With the working world forever changed by the pandemic and remote communication systems becoming increasingly complex, clients can't afford to work with AV partners that don't take security seriously. What was once an afterthought could now make all the difference when clients are selecting long-term AV partners. Choose not to take security seriously? You run the risk of being left behind.