



**WHY SECURE AV?**

AV equipment has inherent, well-known vulnerabilities. It’s built to communicate! Historically, this equipment didn’t reside on a network, but with a rise in AV over IP for its simplicity and ease-of- use, coupled with the exponential growth of automated hacking (even with segmented VLANS we observe breaches), AV equipment is wide open to malicious threats.

As AV integration experts, it is our responsibility to do whatever we can to protect our customers’ AV environment(s)—as it’s a solution in the IOT (Internet of Things) space. **Securitatem** Secure AV protects your organization’s data by automatically detecting, responding and blocking any malicious threats these environments are confronted with on a daily basis.

**FEATURES & BENEFITS**

* A dedicated AV firewall is included.
* Automated monitoring: We monitor (24/7/365) every data packet that crosses the AV/UC boundary with automated response (block, ticket, notification).
* Automated blocking: We detect and BLOCK malicious traffic that eliminates threat exposure.
* Customized Block Lists: Automatically implemented to an internal Security Operations Center.
* Annual Vulnerability Scan: We identify vulnerabilities that compromise the security of your entire system.
* Customized Reporting: We can, on a monthly, quarterly or yearly basis provide detailed reports of connections viewed, muted and blocked in your AV environment to depict the security state of the AV environment.
* AV/UC environment scanning: We can provide monthly or quarterly scanning (optional add-on).
* Encrypted Communication: Available as an optional add-on.

Call us for more information and to set this in place for your AV (IoT) environment:

[**info@bravatek.com**](mailto:info@bravatek.com) **https://bravatek.com/solutions/software/securitatem-av/**