**Securitatem™ AV - FREQUENTLY ASKED QUESTIONS**

Bravatek is excited to offer an integrated security solution that empowers your organization to prevent, detect, respond and report on security issues specific to your AV/UC equipment – “Securitatem AV” (Securitatem Latin for Security).

**WHAT DOES Securitatem AV PROTECT ME AGAINST?**

BVTK Securitatem AV, looks at every data packet coming into and out of your AV/UC environment and uses machine learning determines if the traffic is a threat to your environment and then reacts according to how you set your policy (block the traffic, report the traffic or ignore the traffic) — this protects your environment against common attacks such as eavesdropping, botnets, denial of service attacks, man in the middle attacks, open relays and other common issues. It protects you against the common attacks that impact these organizations such as:

* Compromised servers – Example: A small business phone bill increased from under $1,000 per month to over $8,000 per month and the server was relaying international calls from Africa
* UC Ecosystem Attacks
* Insecure Endpoints
* Eavesdropping and Modification
  + Control Channel Attacks: Fuzzing, DoS, SPIT and Toll Fraud
  + SIP Trunking and PSTN Interconnection
  + Identity, Spoofing and Vishing
  + Attacks Against Distributed System

**WHAT DOES Securitatem AV INCLUDE?**

* Secure Setup and Installation
* 24/7/365 Setup and Installation
* Customized threat and block lists
* Annualized vulnerability scanning
* On demand reporting about how your environment is doing
* External monitoring of illicit data sale sites for potential customer exposures

**WHAT DOES** **Securitatem AV DO FOR MY ORGANIZATION?**

Enormous amounts of critical, sensitive information are commonly exchanged via electronic meeting rooms and unified communications environments every day. Our program is designed to address the specific security needs of the AV/UC environments and protect that information on an ongoing basis without using a ton of scarce IT/security resources.

**OUR SECURITY PROGRAM ALREADY DOES THIS, AND WE DON’T NEED ANY ADDITIONAL SUPPORT**

* We focus on your AV/UC environment only and can tie into your existing security program processes. We augment what you are already doing without adding to their workload.
* Our process is designed to ensure that the new environment fits into your existing security program by leveraging the technology and tools that are in place and filling in the gaps to address UC/AV threats and risks.
* Most AV/UC environments are considered to be insecure and so they are operated on isolated networks. Because security is expensive many times these networks don’t have the same protection that the corporate networks do and are easy to compromise as a result. We fill in that gap cost effectively.

**DON’T YOU ALREADY SET UP EVERYTHING SECURELY—WHY DO I HAVE TO PAY EXTRA?**

* We make every effort to implement all our Securitatem AV installs in a secure manner. The issue we are addressing with our certification process is to enable you to secure the data exchanged over your AV/UC systems to stay secure over time. We do that by providing you tools that can either report issues or stop issues and then report them to your security team.
* Yes, we do set it up securely and then we give you the tools to keep it that way.

**DO I HAVE TO BUY IT?**

* No, you are always free to opt out of the service. The first two weeks are free and comes with a threat report that reviews the first couple of weeks of operation.
* Can I turn it back on later? Yes, you can. Contact: info@bravatek.com

**WHAT DOES Securitatem AV PROTECT ME AGAINST?**

* BVTK Securitatem AV looks at every data packet into and out of your AV/UC environment. Using machine learning, we determine if the traffic is a threat to your environment and how to react according to how you set your policy (block the traffic, report the traffic or ignore the traffic)—this protects your environment against common attacks such as eavesdropping, botnets, denial of service attacks, man in the middle attacks, open relays and other issues.
* It protects you against the common attacks that impacted these organizations such as:
  + A small business phone bill increased from under $1,000 per month to over $16,000 per month without an apparent reason. Our solution detected that the UC server had been broken into and the entire system was being used to relay international calls from several locations in Africa.
  + A well-known venture capital firm lost multiple investment deals because their AV environment was penetrated, and confidential deal information was sold.



**Prevent Detect & Respond Report**

[**www.solutionzinc.com**](http://www.solutionzinc.com/) [**helpdesk@solutionzinc.com**](mailto:helpdesk@solutionzinc.com)