

Overview



Salare develops and markets VoIP security appliances and OEM security software for use in IT infrastructures supporting all types of enterprises

Salare Security LLC
200 S. Wacker Drive
15th Floor
Chicago, IL 60606

Phone: 312.994.2336
Fax: 815.572.8270

info@salaresecurity.com

www.SalareSecurity.com

Salare Security's vPurity™ appliance provides effective protection against data leakage and malware security solutions for Voice over IP (VoIP) networks. Utilizing a patent-pending unique technology, The Salare Security vPurity™ solution is a network edge appliance that is easily deployed and is the only data leakage prevention solution that can handle encrypted payloads. Unlike other security appliances, vPurity™ does not use deep packet inspection and does not degrade the quality of service of voice transmissions.

The vPurity™ solution provides IT security and telecommunications professionals with the ability to:

- detect and identify unauthorized data migration events
- prevent unauthorized data migration
- prevent point to point encrypted media streams from carrying data
- prevent data from leaving the organization without Quality of Service (QOS) degradation

Traditional data security products are not equipped to identify or protect against the unique security challenges associated with VoIP enterprise systems. The "real-time" nature of voice traffic, combined with new protocols, hardware and applications, require security products that are purpose-built for VoIP.

Technical Specifications

- ▶ Robust Server Grade Appliance
- ▶ Dual Core 3.0 GHz Processor
- ▶ 2 Gbyte DDR2 RAM
- ▶ Dual 160 Gbyte Raid Hard drives
- ▶ Silicom Quad Bypass NIC
- ▶ Fedora Core 8 OS
- ▶ Integrated Appliance Firewall

An enterprise voice network provides a significant opportunity for loss of data. Malicious insiders or outsiders look for opportunity and stealth when planning and executing the theft of enterprise data. Deployment of VoIP systems provides the opportunity because this is a new path out of the network that cannot be protected with existing Data Leakage Prevention (DLP) products. Enterprises need to keep voice communications private so internet telephone traffic is encrypted which very effectively hides any malicious activity. This means that IT security administrators, responsible for keeping safe confidential data for privacy and compliance, MUST pay attention to the risks inherent in VoIP.

Other security appliance vendors are working to develop inferior solutions based around Deep Packet Inspection (DPI) techniques. DPI-based solutions are not effective as they are unable to inspect encrypted voice. Encryption of the voice channel is necessary for other privacy reasons to protect the media content from monitoring and interception and is routinely used in mature VoIP deployments today. DPI solutions are also less desirable as they slow down and interrupt the voice network and severely degrade the voice Quality of Service (QOS).

Salare Security's vPurity™ solution is the ONLY solution that can find hidden data inside of encrypted voice transmissions and do so without degrading voice quality.

Benefits

- The only commercially available VoIP data protection software that detects data inside of encrypted VoIP
- Comprehensive protection against VoIP specific data loss threats and attacks.
- Accurate and reliable protection of VoIP infrastructure from internal and external security attacks.
- Zero day attacks are detected and stopped by a non-signature based-defense.
- Easy to use. Web based user interface provides all the necessary functionality to configure, administer and monitor vPurity™ appliance.
- Real-time log reporting mechanism to provide all the information needed by IT security and telecommunication staff to keep the VoIP network secure.
- Bypass NIC protects against service interruption due to power loss or hardware failure.
- Industry Leading Research through affiliation with the IIT VoIP Lab.
- Standard and custom reports provide operational and analytical information to executives and managers.

Features

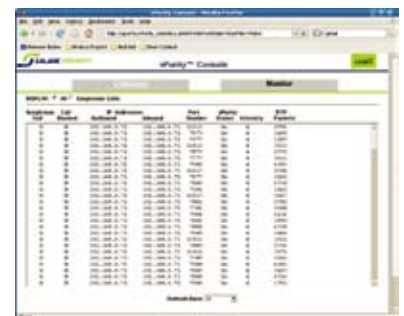
Detects and prevents transmission of data over streaming voice and video channels

- The technology utilizes a revolutionary approach that does not require packet inspection and can defend against use of encrypted media streams to smuggle data without adversely impacting the transmission of voice or video.
- Salare's solution does not require extensive hardware or complex security policy management.
- Finds data even in encrypted payloads.
- Web-based interface allows for authorized access from any location.
- Real-time reporting provides both exploit and event reporting.
- Appliance-based or software-based product distribution available.
- Executive level reports provide concise summary information in a graphical format.
- Reports can be easily exported to .XML, .CVS or .PDF formats.

“ vPurity is the ONLY data protection solution available that is designed to find hidden data in Voice over IP (VoIP) enterprise systems. ”



Console Manager



Detailed Packet Analysis