LENSEC Includes Comprehensive Security Protection in Perspective VMS®

PVMS is Cybersecure Software, Ready with Encryption, Protecting the Entire Security System

FOR IMMEDIATE RELEASE - Houston, Texas, USA – Tuesday, September 18, 2018

LENSEC engineers have outlined several key protection mechanisms that are purpose-built with our enterprise-level video management software. Perspective VMS® comes with several security enhancements included to help protect the system and the data contained within.

LENSEC's Chief Product Officer, Jeff Kellick, says PVMS stands out from the competitor's thick-client software because it is 100% browser-based. Kellick says, "We take advantage of the indispensable web browser. The browser is a software application that is already installed on client workstations, and therefore already vetted by IT professionals. We support up-to-date production releases of the major browsers (Chrome, Firefox, Edge or Internet Explorer). Therefore, we are in line with utilizing an application which the IT department approves without the need for installing any proprietary, 3rd-party application that would require further acceptance tests. With HTML5, Perspective VMS® doesn't need a plugin, which eliminates past generations' browser vulnerabilities. Browsers developed today by Google, Microsoft, and others have established continuous integration and testing to meet evolving threat mitigation standards. Leveraging this platform enables our client software to maintain leading-edge best practices for overall application security."

Configuration Encryption
Out of the box, Perspective VMS® uses RSA encryption to code its configuration files. These files provide initial parameters and settings to the Perspective VMS® services. The files also contain some sensitive data such as usernames, passwords, and database connection information that services need to function. RSA encryption uses a public encryption key and a private decryption key to help ensure that data stays private.

Protecting Web Traffic
Secure Socket Layers (SSL) can be enabled with Perspective VMS® to help protect the web traffic passing between the browser and the PVMS Web Server. Enabling SSL also secures traffic between the web server and other distributed servers within the network. SSL uses trusted certificates and, through a series of negotiation phases, creates a secure encrypted connection.

The data contained within this secured connection is only visible to the hosts involved in the negotiating phases. This helps prevent Man in the Middle (MITM) attacks; an attack in which a third party interjects themselves between two hosts for the purposes of eavesdropping or impersonating one of the hosts.

Protecting Streaming Traffic
When using SSL, Perspective VMS® uses the Web Sockets Secure (WSS) protocol to help protect streaming traffic. WebSockets opens a real-time connection between devices communicating with each other. WSS is the communication protocol that is encapsulated within an SSL/TLS connection. WSS opens secure connections to the streaming services. This direct connection helps reduce the streaming data delivery time to the browser. WSS also helps further reduce the risk of MITM attacks as it creates a direct connection that is encapsulated within an encrypted connection.

On Camera SSL
Typically, the connection from the camera to a streaming server remains unsecured, even in setups that use SSL on the web server. This presents the possibility for eavesdropping from devices within the local network. To fully protect a camera's stream, some camera manufacturers have configurations to allow their cameras to stream over an SSL/TLS connection directly from the camera. When configured, only the camera and server have access to the encrypted data within the SSL/TLS connection.

Planning Networks and Leveraging PVMS Security

There are various levels of surveillance network setup recommended by LENSEC's PVMS product experts for security. On the LENSEC website, we describe typical setups that security integrators may use to build a network architecture. The differences described will vary, depending on the level of security needed by the end-user's enterprise.

Network security is added using SSL and WSS between the Perspective VMS® servers and the client workstations. Additionally, the edge devices may be setup on a subnet, communicating via the streaming service as a proxy.

Overall, the advanced methods recommended will add an extra layer of protection from hackers and harden the network architecture to prevent outside attacks.

If you are interested in learning more about surveillance network security measures regarding Perspective VMS®, please visit LENSEC.com/PVMS.

Contact:
Keith Harris,
LENSEC Marketing & Communications Manager
Email: kharris@lensec.com
Phone: (713) 395-0800
Web: https://lensec.com/