



Searchable Surveillance

IT Security Overview

White Paper prepared by 3VR Security, Inc.
— February 26, 2007



Abstract

The purpose of this paper is to detail the capabilities and security measures built into 3VR Searchable Surveillance Systems to address the IT security requirements of modern security buyers. Of particular importance are the following 3VR features:

- *3VR appliances conform to industry leading information security baselines and pose equal or lesser risk than alternative appliances or workstations on the market.*
- *The architecture of 3VR's product enforces strict avoidance of components that present security risks and constant utilization of proprietary protocols that maximize the difficulty of intruder access.*
- *3VR does not install Internet Explorer, Internet Information Server, File Transfer Protocol or Telnet clients.*
- *3VR appliances require only 1 open port for network communication from 3VR appliances*
- *In over 18 months of widespread commercial deployment, 3VR has not generated any security compromises.*
- *3VR does not currently support BlackIce, Tivoli or SAV but is open to doing so in the future. 3VR recommends testing, tuning and optimization of our appliance for use with these applications. This would ensure maximum information security and strong application performance for physical security's needs.*

Information Security with 3VR

Operating System

3VR's application runs on Windows XP Embedded (XPe). Software version 5.0, released in January 2007, is current with all patches and security hotfixes.

3VR's specific configuration of XPe significantly reduces security risks as described in the appropriate sections below.

Applications

The 3VR appliance runs 6 applications:

- MySQL 4.1.3b
- Shell.exe (3VR proprietary)
- Controller.exe (3VR proprietary)
- ContentServer.exe (3VR proprietary)
- LogServer (3VR proprietary)
- OpCenter (3VR proprietary)

Only interconnects between 3VR applications are by proprietary protocols. This reduces the risk and likelihood of viruses attacking the system. To attack the 3VR system, adversaries would be required to build complex protocols. Furthermore, the resources on 3VR's appliance do not make it useful for DOS attacks.

Services

3VR does not install, nor run, risky applications like Internet Explorer, Internet Information Server, File Transfer Protocol or Telnet clients. All the services 3VR runs have been examined and are fully locked down. 3VR recognizes, however, that the smaller the set of services and open ports, the lower the general risk. Accordingly, our engineers are continually reducing the service footprint within our software. Future releases will have fewer services and fewer open ports both for 3VR's own proprietary protocols and for operating system services. We particularly focus on low-numbered ports and services that have historically represented vulnerabilities.

3VR believes the only potential risk is pirating the Device Update Agent and launching an artificial upgrade. This complicated task, however, would require reverse engineering 3VR's proprietary protocols. The actual threat is low as the expertise is rare and the value of doing so is minimal.

Below is the list of services run by the 3VR system:

- COM+ Event System
- Cryptographic Services
- DCOM Server Process Launcher
- Device Update Agent
- DHCP Client
- DNS Client
- Event Log
- Logical Disk Manager
- MySQL
- NT LM Security Support Provider
- Plug and Play
- Print Spooler
- Protected Storage
- Remote Procedure Call (RPC)
- Remote Registry
- Security Accounts Manager
- Shell Hardware Detection
- Smart Card
- SNMP Service
- TCP/IP NetBIOS Helper
- Themes
- Windows Audio
- Windows Mgmt. Instrumentation
- Windows Time
- Wireless Zero Configuration
- Workstation

Ports

3VR only requires 1 open port for communication from our appliances. Port 3044 communicates system administration, searching, management and recorded video. Live video is communicated over a distinct port, port 2500.

For purposes of performing “over the wire” system upgrades, port 3020 is used. BoA could open up these ports only for the specific times that upgrades are performed.

No other ports would need to be open for any other time or reason.

SMTP

3VR provides limited SMTP support that is constrained to minimize risk to acceptable levels. 3VR provides outbound-only SMTP and only when a customer specifically configures it. No SMTP forwarding is allowed. E-mail content is always automatically determined by the software. Furthermore, the SMTP client is coded directly into the application and there is no receiving code in any of 3VR’s applications.

Patch Management Plan

3VR manages patch updates through the device update agent which no one can access without the 3VR client tool and proprietary protocol. Customers can administer patch upgrades by using 3VR’s enterprise service manager application, which is built into the appliance. 3VR also releases hotfixes via the client tool.

Account Management Plan

3VR designed its account management solution to maximize the security of the underlying Operating System and the overall Network.

3VR completely disables Windows login both locally and remotely. The only Windows account and group that exists is administrator. This provides a safe way of locking down the system as the account is inaccessible for login or remote privilege.

3VR separates login to the 3VR application from login to Windows. Passwords for user accounts are stored in a SQL database using a one-way hash. None of the 3VR user accounts has access to the Operating System. 3VR does have an internal engineering account that has limited system access but can be disabled if requested.

3VR does not force changing of passwords, but the only risk inherent in this is to 3VR's own internal software. An adversary could only change data maintained by 3VR software. Since there is no system access available, there is no risk to the system or network.

3VR does not currently link to ActiveDirectory.

Bandwidth Utilization

3VR has designed its network architecture to ensure that the system minimizes resource utilization and rapidly respects bandwidth constraints even on network connections as low as a DS0.

3VR uses TCP links for video and data. We rely on TCP to provide retransmissions in case of data loss. TCP has sophisticated algorithms for congestion avoidance that allow it to efficiently use slow or lossy networks without swamping them with retransmits. Finally, 3VR naturally degrades bandwidth for live video streaming by employing adaptive frame dropping.

Most importantly, all of these design elements ensure that the 3VR appliance will not engender or contribute to hysteresis.

Bandwidth consumption in the application is highly dependent on load (for example, the number of faces recognized per minute).

- Live video, 10 fps CIF: 64 Kb/s
- Searching, 32 events with 3 images per event, 150 KB total per page of search results (search results are downloaded one page at a time as the user asks for them).
- Alerting, 20 KB total per event.
- Depending on event load, there is some amount of new event notification traffic flowing from server to client.

Physical Access

3VR appliances can be physically accessed onsite via mouse, keyboard and monitor.

Because of 3VR's account management architecture, a malicious user does not have access to the underlying system. Moreover, even if the user somehow accessed the system, because networking services such as web client, telnet and FTP are not installed, an attack would be extremely difficult.

Antivirus

3VR ensures that viruses do not attack the system or the network by enforcing explicit signing of all software that is installed. 3VR uses SHA1, 160 bit key for this task. Because of this, sniffing the transmission and intercepting/modifying is not a practical risk.

3VR's antivirus strategy focuses on lockdown. 3VR does not currently perform antivirus scanning.

As noted in the abstract, 3VR is open to supporting SAV in the future once testing, tuning and optimization have been performed.

Tivoli

3VR has an SNMP service that could be enabled and used to support Tivoli endpoints.

BlackICE

3VR currently has no support for BlackIce. As noted in the abstract, 3VR is open to supporting SAV in the future once testing, tuning and optimization have been performed.

Clients

3VR supports a remote viewing client (OpCenter.exe). OpCenter connects to 3VR appliances via ports 3044 as explained in the Ports section. OpCenter uses the same account management plan as described in the Account Management section.

3VR assesses that the security risk of this client is minimal and acceptable as the 3VR system client is neither extensible nor scriptable.

About 3VR Security, Inc.

3VR Security, Inc. is the creator of the award-winning 3VR Searchable Surveillance System™, which integrates a best-in-class DVR with the most effective search, intelligence, and crime-fighting tools to enable fast, comprehensive investigations and theft and fraud prevention. Backed by leading venture investors (Kleiner Perkins and VantagePoint) as well as the U.S. government's intelligence investment arm In-Q-Tel, 3VR is the first company to provide the complete range of analysis required by today's security professionals in one system.

A single, affordable appliance that supports industry-leading hardware and storage options, the 3VR system has been recognized as the best digital video surveillance system by the Security Industry Association and Frost & Sullivan. In addition to a variety of government installations, 3VR systems are the first such products to gain real traction in the commercial market; the system is deployed at several Fortune 500 companies, national retail chains, world-renowned hotels, and top national banks.

Tel: 415.495.5790 • **Fax:** 415.495.5797

Sales: 415.513.4611 • **Email:** info@3VR.com

Website: www.3VR.com

3VR Security, Inc.

475 Brannan Street, Suite 430,
San Francisco, CA 941071

