

VUNETRIX

The Root of
Cannabis
Security and
Compliance

www.vunetrix.com

INTRODUCTION

Do you, your customers, or state regulators rely on timely responses to security breaches to ensure that criminals do not harm people, damage property, or divert and steal inventory? Can a power disruption or communication breach cause you a loss of data, product, or assets? If you answered yes to either of these questions, then it is time to make sure your security system always operates, functions as designed, and complies with state regulations.

Timely responses to security breaches require reliable data from security and alarm systems. A data loss from your security system leads to security holes that can put you and your cannabis operation at risk. Break-ins cost thousands if not tens of thousands of dollars in asset loss harming both business continuity and your brand. But even worse, non-compliance with security monitoring and reporting requirements can cost you your business license.

Why should you be concerned about security system monitoring?

This eBook discusses how to minimize, if not eliminate, failures found in most security and intrusion detection systems as well as ensure compliance with state regulations. We hope to spark interest in how a tool that integrates your network and devices can combine with accurate, real-time alerts to deliver better monitoring and reporting, and therefore ensure security system reliability and compliance.



Why is this happening?

In many circumstances, criminals work at neutralizing your security system. Thieves and unauthorized individuals often cut the phone lines to the alarm system, disconnect video systems, or damage or block cameras. Monitoring stations can fail to notice these disruptions. And, at the very least, Security professionals might not receive the information in a timely manner. Missed security threats lead to response delays that result in losses for the business and regulatory failures. Neutralizing the security system allows criminals unlimited time to breach safes and vaults, falsify information, divert inventory, and empty the contents of an entire retail, growth, processing, manufacturing, or research facility.

Historically, businesses saw an alarm system as the first line of notification when an criminal breached a property. Alarm systems can delay reporting and generate false alerts. In the current era of network connectivity, real-time monitoring exists and guarantees a superior method for knowing when a breach occurs. Some state regulators require cannabis facilities to notify authorities of security breaches within the hour of its occurrence; else the businesses risk hefty fines or temporary closures as penalties.

The Root: Vunetrix Network Monitor

VNM has facilitated arrests of dozens of criminals in organized gangs, saving tens of thousands of dollars of inventory loss and facility damage.

Why is Vunetrix Network Monitor (VNM) at the root of stopping unauthorized access and proving compliance?

VNM is always on, notifying your Security team the instant any physical or network security device goes offline. Unfortunately, video monitoring can't cure all physical security concerns: devices develop defects over time that most often go unnoticed. Moreover, existing infrastructures sometimes block organizations and their Security teams from discovering anomalies in their facilities and networks.



OUR VALUE

VNM delivers defect and anomaly detection for both security and compliance through device information monitoring. The VNM software inspects network bandwidth, scrutinizes the health of each device, and determines the device's status. For instance, VNM can diagnose the condition of a live streaming video camera, inspect the servers that collect the video streams, check the network connection cards, and ensure that the bandwidth stream is indeed continuous and operates efficiently. With all these functions, VNM monitors baseline control board requirements for video recording, alarm, and personnel access systems.

How does Vunetrix assure protection against unauthorized access and compliance gaps?

VNM software monitors all bandwidth fluctuations and network traffic to assure that the devices and services operate within normal ranges. If an anomaly occurs, VNM promptly alerts monitoring staff and Security teams. 'Know Your Normal' forms the substratum of Vunetrix's excellence. The firm's best-in-class software determines the baseline condition for each physical security appliance and service in your environment and establishes the system's 'normal' state. Then, you can set network bandwidth thresholds and key alerts. Alerts can be prioritized by job function, time of day, and priority.

VNM lays the deployment baseline using device templates.

Vunetrix also delivers device information through a 'single-pane-of-glass': a dashboard aggregates intelligence from all devices, regardless of manufacturer, and displays the health and condition of each using color-coded charts. The software automatically sends real-time email alerts about servers, power supplies, storage drives, and the network to your personnel based on user permissions as defined by your Security team.

Once you determine the severity of any physical or electronic anomaly, VNM's instant notification feature allows you or your alarm company to dispatch local law enforcement and to notify regulatory authorities immediately. VNM software double-checks the security system to assure that it continues to operate and function as designed.

The Benefits of Using Vunetrix Network Monitor for Security and Compliance



1 IMPROVED SECURITY AND EFFICIENCY

VNM automates time-consuming tasks and delivers real-time, holistic visibility to devices that ensure the security of all areas of your premises and accurate record keeping. With the correct alerts, your Security team uses fewer resources to ensure compliance and consistent performance of your security system.

2 CRITICAL INFRASTRUCTURE PROTECTION AND COMPLIANCE

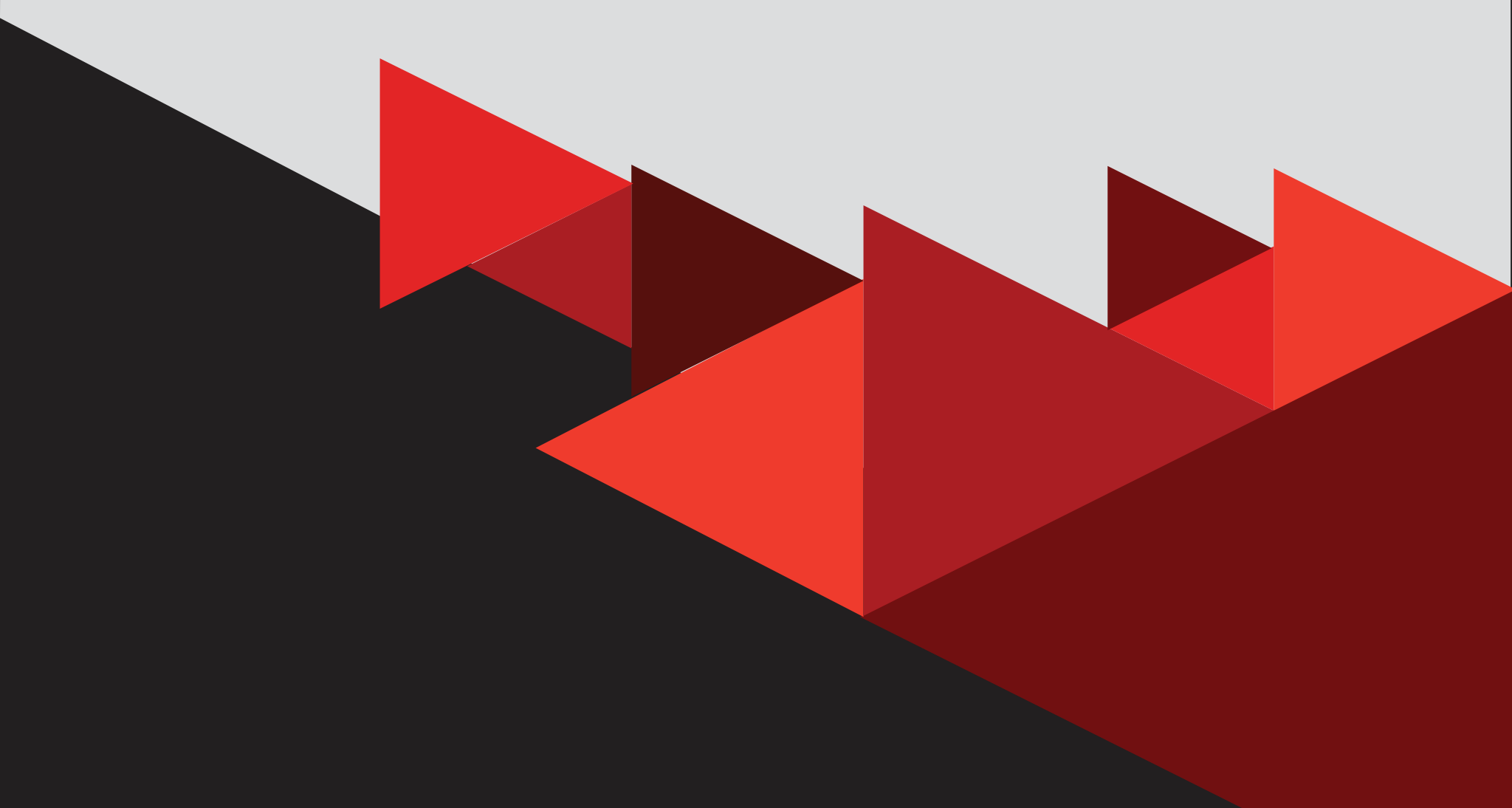
Use VNM to monitor security systems, guarantee uptime, and streamline compliance reporting in real time. Our tool helps you ensure and report compliance as defined by state cannabis control regulations.

3 RAPID TROUBLESHOOTING

Having all data on a single dashboard provides you with instant visibility to assess and correct retail and operations issues, using visual alerts for breaches and failures. VNM delivers the information for quick and appropriate responses, including the deployment of law enforcement and the required notification of regulatory agencies.

4 BUSINESS ANALYTICS

VNM drives better physical security infrastructure and business decisions for capacity planning and system performance, allowing for better filing and reporting of mandated security plans and facility modifications. Your Security team always knows when devices approach the end of their life cycles and need replacing.



Most companies fail to understand the difference between compliance and security. In fact, some organizations think they are the same. Some get so confused about complicated regulations that they stop focusing on security altogether.

SO, WHAT'S THE DIFFERENCE BETWEEN COMPLIANCE AND SECURITY?

Compliance means your business meets state regulations. On the other hand, **security** keeps your money, product, and people safe from theft, intrusion, disruption, and physical harm. Cannabis growers, retailers, and dispensaries need both: a system that keeps facilities, people, and assets secure, and a system that complies with state rules.

If you are curious about the difference between a compliant and secure environment, we've outlined the difference on the next few pages. Keep in mind that these are "must have" yet general recommendations. Each environment is unique and has specific security needs. Also, every state has their own Cannabis Control Board. Be sure to check with your local state regulators and assure that your business follows the specific regulatory mandates for that state in which it operates.

Compliant vs Secure Surveillance Systems

Compliant

- Cameras must cover all areas where cannabis items or waste will be present.
- Cameras must cover all areas where cannabis items or waste is in transit.
- Cameras must cover all areas within 15 feet of all entry points in all directions.
- Cameras must record at a minimum resolution of 1280x720 pixels in all lighting conditions.
- Cameras must record at a minimum of ten frames per second (five frames per second for exterior non-restricted areas).
- Locations must incorporate a dedicated room for surveillance systems, including a list of all personnel with authorized access.
- The surveillance system must include a backup battery that can independently power the system for at least one hour.
- The surveillance system must provide automatic notifications in the event of a camera or other system component failure.
- The surveillance system must include a monitor for viewing video from any camera.
- The surveillance system must contain a digital archiving system and a printer.
- Companies must maintain recordings for 90 days on-site.
- Companies must back up video continuously to a secure off-site location.

Secure

- Camera placement and positions allow for the desired field-of-view.
- Camera programming includes appropriate access permissions with secure usernames and passwords.
- Camera configuration provides uninterrupted data/video image storage.
- Camera function correctly and provide a live image.
- Network and infrastructure handles and supports high-resolution storage and large amounts of data transfer (the most common cause of lost video data).
- IT properly maintains hard drives in good health to store video data.
- Optional but highly recommended: An employee or video monitoring company continually watches live video, strengthening security by scanning for shoplifters and other nefarious individuals who can harm products, people, and facilities.

Compliant vs Secure Alarm Systems

Compliant

- Must operate and activate fully during all non-business hours.
- Must include 24x7 professional monitoring. Must detect unauthorized entry onto premises.
- Must detect unauthorized activity in limited-access areas.
- Must notify authorized personnel of each unauthorized entry.
- Must ensure that authorized personnel can immediately notify law enforcement or security personnel.
- Must feature at least two operational “panic buttons” located on the premises that immediately inform law enforcement or security personnel.

Secure

- 24x7 Monitoring: The alarm system guarantees communications system delivery around the clock. Technology obsolescence or cut lines must not hinder business operations.
- Alarm Response: If an intruder triggers a sensor inside the business, the alarm company responds immediately and contacts the company and the authorities.
- Fast Assistance: The alarm solution contacts and dispatches emergency response services on the spot.

Compliant vs Secure Access Control Systems

Compliant

- Must operate fully 24x7. Must include an electronic lock system. Must connect to the alarm system.
- Must enable a Security manager to set specific requirements on who can enter operations and retail space.
- Must incorporate clearance levels and shift times.
- Must differentiate between authorized users by including employee-specific access codes or fingerprint.
- Must prohibit access by individuals not directly engaged in business.
- Must detect unauthorized entry onto all premises.
- Must catch unauthorized entry into limited access areas.
- Must prevent public access to all areas used in marijuana productions.
- Must prevent public access to the composting area.

Secure

- Installers physically secure door readers with specialty screws.
- Installers tuck away and protect door reader wires.
- Each door contains internal memory. Door readers feature tamper alarms.
- Door readers include credentials with some form of encryption.
- Door readers offer multiple levels of authentication.
- Access control system programmers use proprietary technology instead of open source.
- The access control system features a lock-down mode.
- Lock-down mode accommodates customized scenarios.
- Door hold alarms sound if a door remains open too long.
- A detailed reporting interface permits monitoring staff and equipment to observe a person's movement throughout the building.
- The best systems integrate with surveillance cameras and store records indefinitely.

Take note: you can also customize and individualize VNM alerts per stage in the seed-to-sale process and per functional area. Incident identification gives your Security professionals the opportunity to act before inventory loss or diversion, data tampering, or unauthorized access or breach of your environments.

CONCLUSION

We invite you to contact us about the security and compliance of the video, personnel access, and facility alarm systems on your premises. Call us toll-free in the United States and Canada at 1-855 NET VIEW.

Vunetrix Network Monitoring: our always-on technology alerts you in real time of any system breaches, snags, or failures that could give intruders or unauthorized users time to break in and threaten your company's security and compliance.

VUNETRIX



1325 4th Ave,
Seattle, WA 98101



1-855-NET-VIEW



info@vunetrix.com

www.vunetrix.com