White Paper: The Importance of Surveillance System Resilience and System Health Monitoring

Though never officially codified, security managers are very familiar with Murphy's Law of Security, stating, "... an incident is more likely to occur near a PTZ camera pointed in the opposite direction or in view of a broken camera."

An unrecorded incident can leave a business liable for large damage settlements, risk a bad public reputation, or lose employee confidence. Many things can cause an IP camera to stop streaming video, from a firmware hiccup to a botnet creating performance issues. Regardless of the actual reason, the responsible parties must be immediately aware of any system health issues to remedy the situation. Resilience in a system is related to how quickly an issue is realized and addressed as much as it is relevant to have engineered failover or redundant components in the final design. Backup measures are meant to temporarily be in place, motivating the urgency to correct issues with the primary components.

With one billion surveillance cameras being installed worldwide by 2021, the businesses and agencies that rely on the continued operation and integrity of their investments, require assurance that they are operational and performing the tasks for which they are deployed. A single camera losing video could have helped avoid a massive lawsuit, a single drive failure could permanently lose video for dozens of cameras, and a server outage could leave entire systems inoperable when security can afford zero downtime.

WHY MONITOR?

Often, Security Operators monitor the system's outputs; however, they may not be the team responsible for fixing any of the technical issues. Having instructions coded into a Standard Operating Procedure with a calling tree is undoubtedly a way to handle occasional outages. Still, it is time-consuming and sometimes contains out-of-date contact information. A security system with built-in monitoring and tagged alerts can drive resilience by minimizing downtime and mitigating the amount of overall data lost during an outage by monitoring critical aspects of the complete system. From video stream integrity to cyber-attack

and operating system uptime, having 24/7/365 coverage of the essential elements of a surveillance system should be a vital part of any security operation.

NOT ALL ISSUES ARE CREATED EQUAL

Not all surveillance system components carry the same amount of risk and incur the same losses should they fail. For example, a single camera outage will only impact the area the camera was covering at the time of the disruption. The fix for an IP camera is often the same as the time-tested computer fix of "turning it off and on again." It is crucial that responsible parties are notified immediately, or better yet, the PoE switch can detect a loss of video streams and automatically power cycling the affected camera while notifying responsible parties like IT or the Service Provider.

As you move away from the edge of the system, a single component can be responsible for a small group of components, like a separate network switch. It will typically power and connect anywhere from 1 to 48 cameras or devices. If that switch is the single connection point for other switches, even more devices are at risk of failure from a single source. The loss faced with this type of issue impacts the present ability to power cameras or transmit and record videos during the outage. The group managing the switch, be it the corporate IT department or the Service Provider, needs to be aware of the failure and defining characteristics, such as its location to troubleshoot and fix any issues quickly.

MONITORING YOUR SYSTEM'S HEART

At the heart of the system is the most significant potential risk with the highest number of points of failure, the management/recording server itself. Without any redundancy in power, storage, or system drives, a single drive failure could cause the loss of present and past video evidence. In some cases, hundreds of cameras accounting for thousands of video hours could potentially be lost. Smart engineering, with redundancy in storage using RAID, is one of the easiest ways to ensure resilience in a recording. It is just as critical that hard drive health and RAID health are closely monitored and any issues are reported to responsible parties for immediate resolution.

Hard drives get the lion's share of attention since it is a moving part, subject to wear over time, and easily one of the most common component failures. The "silent killers" of security solutions are the hidden software issues or temperature spikes that can bring a system to a full stop. For example, when a Windows background service stops running, and video is still streaming to viewing clients but is not being recorded, this leaves a false sense of certainty that systems are working. Or, the CPU overheats, triggering an emergency shutdown, stopping the entire system from operating. With temperature issues, problems in one device may point to concerns in others. Non-monitored devices that are sharing the same physical space, potentially revealing HVAC or similar issues.

MORE SYSTEM HEALTH RISKS

Aside from a system component failure, the other significant health risks facing security systems is the ever-present and persistent threat of malware and hackers. The Mirai Botnet, released in 2016 heavily impacted CCTV cameras, is still crawling the internet. Newer variants like Dark Nexus seek high powered computational devices exposed to the internet, like IP Cameras and routers. In 2020, it was discovered the IoT well was poisoned when Ripple20 was exposed, impacting billions of IoT devices. There are ever more sophisticated phishing attempts that seek to unleash ransomware and malware from inside the castle walls. These attempts could potentially bring down the entire enterprise, including security and life-safety systems.

With so many cyber threats posing a risk, a health monitoring platform must assess the cybersecurity posture of the system and provide the details at a glance and answer the following questions: Do all servers and clients have an anti-virus installed? Are all devices adhering to cybersecurity best practices, and are they using easy to guess username and password combinations? Are any devices attempting to communicate out to unknown sites? Each of these best practices, when enabled, makes a system more resilient to exploits from malware and ransomware, and a monitoring platform allows the appropriate stakeholder to identify what and where the vulnerability lies and address it immediately.

MAKING YOUR SYSTEM WORK FOR YOU

With the health of a surveillance system being directly responsible for a security program's overall effectiveness, it stands to reason that monitoring those systems is vital to have a comprehensive and reliable security program. A carpenter is no good if his hammer is broken, so a security program is ineffective if its systems fail. Treating system health and cybersecurity alerts, like a security sensor alarm, is the next logical step. The best way to visualize a system's health and cybersecurity posture is with dashboards and reporting, and to leverage text messaging for critical failures and moderate issues being communicated via email to the appropriate parties.

A best in breed monitoring solution would stand alone as its visually-driven view into managing security systems and their assets across the enterprise, with visibility to anyone with a browser and a login. On its own, the solution will have a customizable dashboard to display the information most relevant to the viewer. Additionally, the monitoring solution can export customized reports to review historical data and schedule those reports to be delivered at a predetermined time to the right people.

The monitoring solution would also integrate those alerts into existing systems used by security departments and IT managers. For security personnel, the monitoring solution would integrate into their preferred pane of glass, like a Video Management System that is digesting and displaying video, access control, and intrusion alarm data. The health alert data is treated as a system-based alert, and various actions can be assigned to that alert. For example, if Camera Y goes offline, PTZ X can move to a preprogrammed position, while sending an email to the Security

Manager, IT Manager, or the Service Provider. For the IT department, the alert data can be sent to industry-standard tools like Syslog, Splunk, and SolarWinds®, where similar actions can be prescribed.

The daily benefit of issue alerting is evident, but the other, less distinct advantage of having a monitoring solution is historical reporting. Looking at alerts or other conditions over time can reveal problems in other systems by correlating data internally amongst the security system and other data points generated by the enterprise. Seeing a trend of excessive reconnects of a camera during a particular time frame may reveal an unrelated network issue elsewhere that is impacting the stream traffic from the camera to VMS.

A camera being auto rebooted for a single video loss may not be a big deal. However, if that camera was rebooted several times in a day or a week, the trend analysis can identify which devices may need repair or refreshing.

DIRECTING THE FLOOD OF DATA

With an open platform monitoring solution feeding surveillance system health metrics into a data correlation engine like Splunk, the possibilities are exciting. The data points a monitored surveillance system provides can be joined with building system data points and other security sensors to create a data picture to optimize business operations beyond the scope of physical security. For example, maximizing space utilization by correlating motion, video, and lighting usage data.

With the total number of cameras growing steadily and the capabilities of modern security systems consistently expanding, the amount of data being delivered to security operations is incredible. That flood of data must be appropriately prioritized and circulated. Visualizing the data in a simple and meaningful way through dashboards is the first step in managing that flood.

RESILIENCE IS ESSENTIAL

Automatically alerting parties responsible for resolving specific issues deemed critical and bypassing those whose attention is better served in handling actual physical threats are essential components in making a security system and its operation resilient. Resilience makes security operations effective with minimal downtime. The capacity to catch issues early reduces the overall total cost of ownership. The ability to deploy resources where they are needed with what they need reduces trips and overall downtime, which directly translates to lower costs overall. A resilient system, built with appropriate redundant measures in power and storage, being adequately monitored and maintained, will help shield the enterprise from potential substantial liability costs; thereby, justifying the investments to protect people, property, and profit.

Americas: 469-828-3380
UK/EMEA: 0203 773 3689
salesinfo@razberi.net
wphm20200716