VERKADA

How Secure is your Video Surveillance System?

Security Whitepaper

Verkada Inc. 210 South B Street, San Mateo, California, 94401 • sales@verkada.com

Table of Contents

EXECUTIVE SUMMARY

Everywhere you look, video surveillance plays a growing role in the protection of people, property and assets. In 2014, there were nearly 250 million professionally installed security cameras worldwide.[1] Through 2021, security camera sales are expected to grow over 7% annually.[2]

Unfortunately, many security camera systems have software security weaknesses, making them an increasingly popular target of malicious actors. In the two-year period of 2015-2016, for instance, hackers mounted 458% more vulnerability scans of connected IoT devices—many of them CCTV cameras.[3] In 2016, attackers exploited an IP camera vulnerability to execute one of the largest distributed denial of service attacks in history.[4] These are just two recent examples of many: a Google search for "security camera vulnerabilities" returns about 1.1 billion results—nearly 250,000 more than are returned for "iphone vulnerabilities."

This whitepaper outlines vulnerabilities common to conventional video security systems, flags issues to watch out for, and offers suggestions on a better way to enhance the security of your organization.

[1] HS Markit, 2014.

[2] http://www.securityinfowatch.com/news/12362388/report-us-surveillance-camera-sales-to-grow-72-percent-annually-through-2021

[3] https://www.business.att.com/cybersecurity/archives/v2/iot/

[4] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

RISKS OF THE OLD WAY	BENEFITS OF THE NEW WAY
Out-of-date software & firmware	✓ Update all devices automatically & continuously; redundant firmware banks for failsafe updates
Insecure video storage	✓ Replace DVRs and NVRs with on-camera, solid-state storage; encrypt all data, all the time; cloud backup for added redundancy
Insecure video transmission	✓ Transmit all data over HTTPS; don't rely on physical security of wiring or VLAN-security
Open ports & inbound device access	✓ Outbound connections only; no open ports and no openly accessible servers running on each device
No redundancy; single point of failure	✓ Distribute video storage across many nodes (cameras and cloud); eliminate reliance on DVRs/NVRs at each location
Insecure user access controls	✓ Granular user access controls; fully auditable logs
Unsafe remote access	✓ Two-factor authentication; powerful user access controls; single sign-on integration
No way to tell if a camera is operational	✓ Active system health monitoring; tamper detection; image clarity verification; automated alerts

ABOUT VERKADA

Verkada builds enterprise video security systems that combine cutting-edge camera technology with intelligent, web-based software—all in a secure, user-friendly solution. Unlike existing systems, Verkada's technology eliminates outdated equipment such as network video recorders (NVRs) and offers the protection of full encryption with no special configuration required. Verkada systems are easy to install, update and expand.

Founded in 2016 by computer scientists and information security experts from Stanford University and MIT, Verkada is headquartered in San Mateo, California.

A NOTE ON SYSTEM DESIGN

Traditionally, closed-circuit television (CCTV) systems were exactly that—closed. Video cameras were wired to broadcast locally to a set number of monitors. The only way to breach the system was to gain physical access to the monitors while the broadcast was in progress.

We've come a long way—there now exist a number of approaches to enabling video surveillance of physical sites. The biggest change in recent years has been growing demand for remote access—the ability to manage security camera footage via connected devices such as laptops, tablets, smartphones.

To meet this new demand, security system providers have developed a number of different system designs. At a high-level, we describe these approaches as follows:

TRADITIONAL ON-PREM + INTERNET ENABLED REMOTE ACCESS

Many of the world's largest providers of security cameras and related equipment have adopted this system design to meet new demands of their connected clients. This approach retains the original system architecture—essentially video cameras plus an on-premise storage device—but adds an Internet connection to enable remote access.

Pros:

- Works with your existing system architecture
- Available from established brands

Cons:

- Difficult to keep up to date with the latest security patches and software
- Lots of configuration and manual updates required
- Requires complex VPN configuration and/or port forwarding to enable remote access

VIDEO SURVEILLANCE AS A SERVICE (VSaaS)

Several years ago, a new group of providers entered the market to provide cloud-based storage and access. Generally speaking, VSaaS comes in two varieties:

- **Hosted video surveillance:** Video is recorded, managed, and stored off site at the VSaaS provider's data center
- **Managed video surveillance:** Video is recorded and stored at the customer's site, but the provider manages it remotely

VSaaS providers typically do not manufacture their own hardware. Rather, they configure existing equipment to connect to their cloud-based services, which are typically powered by third-party storage and computing providers. While VSaaS providers often handle system management and upkeep, the systems themselves are not immune to the risks associated with outdated software and other vulnerabilities.

Pros:

- Turn-key managed service

Cons:

- Systems require provider to keep system updated and maintained; typically relies on manual updates
- If storage is hosted in the cloud, the system may hinder bandwidth
- Likely relies on VPN configuration and/or port forwarding to enable remote access

CLOUD-BASED ADD ONS

A third group of providers has developed physical adaptors that plug into DVRs and NVRs from established security equipment manufacturers. We describe these providers as "cloud-based add-ons," given that they are designed to add capabilities to an existing system. Once connected, these devices enable functionality such as remote access, encoding of digital video, cloud storage and video analytics.

Pros:

- Works with your existing system; don't need to get rid of existing equipment

Cons:

- May consume significant bandwidth because the system is constantly uploading footage to the cloud
- Often requires its own high-speed network to function properly, adding cost
- Updating software is not automatic—it typically requires intervention of the VSaaS provider to ensure success
- There are frequently interoperability challenges between components from different manufacturers

TRADEOFFS: INFORMATION SECURITY AND REMOTE ACCESS

Historically, any video security system designed for businesses has presented a set of tradeoffs. Systems that rely on centralized on-premise storage—via NVRs or DVRs—typically face complexities when it comes to enabling remote access. These complexities are known to introduce vulnerabilities that may be exploited by malicious actors.

On the other hand, systems that rely purely on cloud-based storage remove the need for DVRs and NVRs, but this configuration comes at a cost: sending 100% of your recorded footage to the cloud can dramatically hinder the bandwidth of your local area network. Poorly designed cloud-based systems may also come with their own set of vulnerabilities.

The purpose of this white paper is not to dive deep into the details of each system type. Rather, we aim to highlight the most common software-related security shortcomings that arise from existing system designs. As with any investment for your business, it's important to consult with your provider to fully understand the benefits and limitations of their proposed system design.

At the end of this whitepaper, you'll find a questionnaire that you may find helpful in identifying the right questions to ask during your vendor selection process.

Verkada offers a new, differentiated approach to achieving information security and enabling user-friendly remote access. If you're interested in learning how this approach is different—and why we believe it is better suited to meeting today's business needs—visit verkada.com or contact Verkada Sales at sales@verkada.com.

OUT OF DATE SOFTWARE

New malware and other threats are constantly emerging and evolving. In order to ensure system security, it's critical that your hardware's operating system and firmware are updated regularly. In the ideal vulnerability response scenario, system providers quickly develop and release software security patches, which are then installed across all deployed devices, everywhere.

In reality, however, it can be weeks—sometimes months and even years—before a given video security system receives an update. There are a number of causes. In some cases, manufacturers don't develop software patches fast enough, or they develop a security patch that's just a partial fix. In other cases, the patch is developed but it's installed only across a small subset of all the systems in operation. Finally, many vendors rely on third party operating systems, frequently Microsoft Windows, over which they have limited control. A number of other factors contribute to low patch rates, including:

- System administrators may be unaware that their system requires an update
- The device's operating system isn't compatible with the firmware update
- It's difficult or time-consuming to properly install the security patch—in some cases, the patch must be installed manually to each camera separately, adding cost and delays to the update process

Patch rates are difficult to measure broadly. But in recent years the high number of incidents where manufacturers have failed to respond quickly—or administrators have been slow to fully adopt updates—suggest that many systems continue to run on outdated software. The longer a system goes without an update, the higher the risk that it will become a target of an attack or security breach.

NOT JUST FOR IT ADMINISTRATORS

In many organizations, the physical security system is used and maintained by the operations, loss prevention, or facilities teams. These groups need a system that "just works" and stays secure without requiring specialized IT skills.

Avoid systems that only IT can effectively keep secure, including ones that require manual firmware updates, operating system patches, complex network storage or backup devices, and sophisticated networking infrastructure.

Ideally, the team responsible for the camera system should be able to plug in a new camera, see a green light, and not have to think about the security of the camera again.

DVRs & NVRs

Conventional video security systems store footage on what are essentially centralized, on-premise servers called digital video recorders (DVRs) or network video recorders (NVRs). Despite the fact that these devices add cost, complexity, and risk, the vast majority of ordinary video security systems today use them.

Here are a few of the top ways in which NVRs and DVRs introduce complexity and risk.

PORT FORWARDING & FIREWALLS

Most DVRs these days enable remote access, allowing users to watch live or recorded video using a web browser or application. This is most commonly achieved by "port forwarding," which enables external devices to penetrate through the organization's firewall and communicate directly with the DVR. Once opened, however, this connection creates the possibility that external actors can enter the previously firewalled network.

Machines that are connected to the Internet are typically scanned thousands of times a day. And firewalls are often highly complex, requiring hundreds or even thousands of rules. If not managed correctly, DVRs can compromise the security of your entire system. Even if managed by a qualified professional, port-forwarding can introduce risk and complexity that should be avoided if possible.

SHARED PASSWORDS & FACTORY DEFAULTS

DVRs and NVRs are often shipped with login credentials that are set at the factory. Since the user interface on these devices is notoriously unfriendly (many don't have keyboards) it's not uncommon for administrators to simply use the factory defaults when configuring the system.

In some cases, the default username has been identified as “admin” and the password is blank.[5]

By some estimates, as many as 70% of NVRs and DVRs operating today are still running on unchanged passwords.[6] Even if you discount this estimate by 50%, that still suggests that over a third of systems have not had their factory defaults changed.

SINGLE POINT OF FAILURE

By centralizing the storage of video data, NVRs and DVRs may represent a single point of failure in your system. Unless you are storing all of your video data in the cloud, which can greatly hinder the bandwidth of your local area network, you risk losing all of your footage if the device is tampered with or stolen. It is not unheard of for a disgruntled employee or savvy outside operator to deliberately target the video recorder when perpetrating a malicious act.

INCOMPLETE ENCRYPTION

A surprising number of NVRs, DVRs and other equipment are shipped without encryption enabled by default—more often than not, it’s a setting that must be actively configured by a person with technical knowledge.

Even when encryption is enabled, it typically applies only at rest—that is, the system offers protection only when footage is stored on the DVR/NVR drive. Any time the footage is viewed, it’s played back over an unsecured connection—most often, this is achieved over real time streaming protocol (RTSP). Result: though your footage is protected in storage, it’s not in any way encrypted during playback. Anyone who’s able to take advantage of the insecure elements of your system architecture may be able to intercept the video stream during playback, gaining access to all of your video data.

[5] https://www.pentestpartners.com/security-blog/pwning-cctv-cameras/

[6] https://blog.gdssecurity.com/labs/2012/5/15/using-metasploit-to-access-standalone-cctv-video-surveillanc.html

NO ACTIVE MONITORING

It’s a fairly common tale: faced with a recent theft or other security incident, a business owner asks video footage to be retrieved only to hear that the camera with the best vantage has been offline for an undetermined period of time. The very system that they had invested in is rendered useless right when they need it most.

Fortunately, this scenario can be avoided if you select a vendor that offers active monitoring of system health. The best providers will offer automated alerts for both system health—whether a camera is operating as normal or has gone offline—and if tampering is detected.

WEAK USER ACCESS CONTROLS

As noted previously, traditional systems make it difficult to grant or revoke user access permissions—so much so that it’s not uncommon to see users opting to share login credentials rather than configuring individual logins appropriately. It’s not uncommon for multiple users at an organization to share the same log-in credentials—often via spreadsheets or other insecure means. While in a pinch it may be easier to copy/paste your login rather than to configure a new user account, this practice clearly compromises the security of the overall system and should absolutely be avoided.

A BETTER WAY TO ENHANCE SECURITY: VERKADA'S APPROACH

At Verkada, we're on a mission to modernize the world of physical security. Our approach to video surveillance system design is different from what's out there. As a result, we're able to ship all of our systems with network security best practices enabled by default—with no special configuration required.

Verkada eliminates local servers and network video recorders (NVRs). Each camera stores video footage on industrial-grade, solid-state storage. This footage is encrypted at rest via public key infrastructure (PKI), which prevents unauthorized access—even in the unlikely event that the camera itself falls into the wrong hands. For added redundancy, on-camera footage may optionally be backed up in encrypted cloud storage. Eliminating the NVR not only reduces the overall complexity and cost of ownership of the system, it also removes the single point of failure common to traditional systems.

HTTPS/SSL encryption comes enabled by default, meaning no additional configuration is required to protect video data when it's in transit. And because each Verkada camera only communicates via outbound protocols and is automatically self-firewalled when it first connects to the network, our systems avoid the vulnerabilities associated with open ports.

When it comes to controlling access, Verkada makes it easy to manage access permissions across your organization. Quickly grant, edit or revoke access rights for any user—right from Verkada's cloud software. You can also easily control accessibility by user, site and organization. Provision access for a set period of time with time-restricted access. For added protection against unauthorized user access, two-factor authentication is offered as a standard feature.

Finally, software updates and upgrades occur automatically, with security patches being rolled out in as little as 24 hours. This ensures the system is always running the latest software version.

VERKADA SYSTEM HIGHLIGHTS

SYSTEM DESIGN

- No NVR or DVR
- On-camera, industrial-grade solid-state storage
- Regular, automated software updates
- Redundant firmware banks for failsafe updates
- Remove reliance on physical security of wiring and/or VLANs

ENCRYPTION

- 128-bit AES encryption + 2048-bit RSA encryption (two layer) + 256-bit SHA2 HMAC cryptographic integrity checking (to ensure that only authentic and authorized software is uploaded to the camera system)
- Full HTTPS/SSL encryption

USER PERMISSIONS & ACCESS CONTROLS

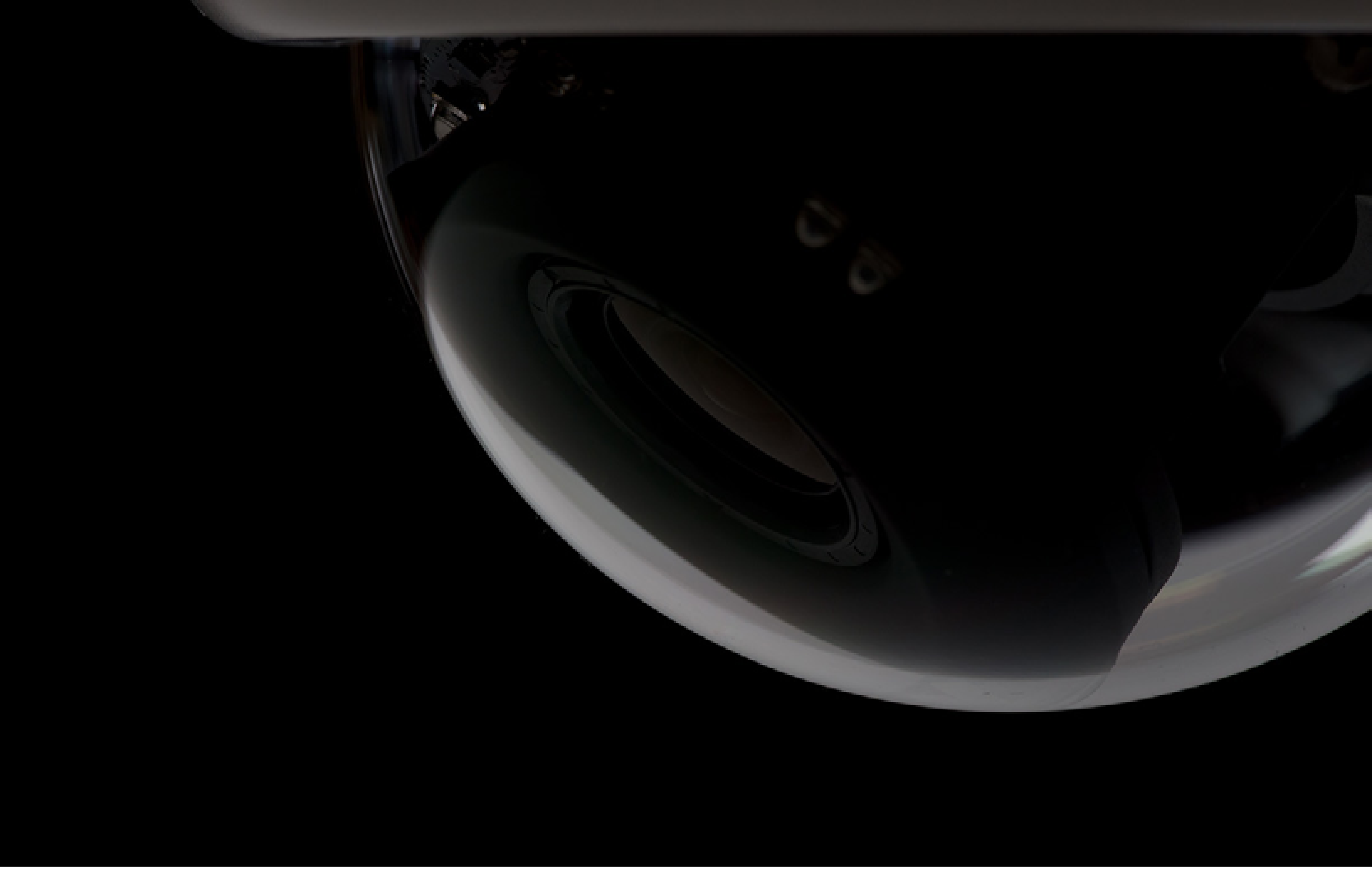
- 2-factor authentication
- Granular controls for user, site and organization
- Easily assign/revoke different permission roles
- Time-restricted access sharing: automatically expire access after set time period
- Detailed access logs

MONITORING & ALERTS

- Active system health monitoring
- Tamper detection
- Automated alerts
- Subscription controls for managing alerts

CAMERA HARDWARE

- Vandal resistant: IK08 for the Verkada D30 (indoor camera); IK10 for the Verkada D50 (outdoor camera)



WANT TO LEARN MORE?

We'd be happy to speak with you about your particular needs and answer any questions you may have about video security systems for your organization.

Toll-free: (833) 837-5232 // (833) VER-KADA
Email: sales@verkada.com

Global Headquarters
210 South B Street
San Mateo, California 94401

APPENDIX: VENDOR SELECTION WORKSHEET

When selecting a vendor, use these questions to better understand the security protocols and best practices that underpin their recommended system. These questions are intended for reference only—be sure to consult with your company's physical and IT security teams before selecting a security system partner.

QUESTION	YES	NO	NOTES
Do you support two-factor authentication?			
As part of the system install and configuration process, do you require setting up a VPN connection?			
Do you require port forwarding and/or open firewall ports to enable remote camera access?			
Is video encrypted during transfer?			
Is stored video encrypted? If so, how?			
Can video be played back without third-party software or plugins?			
Are software updates and patches validated for integrity using a secure hash or checksum to ensure only authentic software can be downloaded to the device?			
Does your system enable control of user permissions associated with live & archival video access?			
Can you audit who has accessed live and stored video footage, or where they've done it?			
Do your cameras require inbound connections to stream video?			
Does your system automatically notify me if it goes offline?			
Does your system detect abnormal movements that are associated with tampering? If so, can it send automated alerts?			