WatchMeGrow
Anywhere.

WHITE PAPER

Is Your Childcare Streaming Video System Secure?

PRIVACY & SECURITY FOR VIDEO IN CHILDCARE CENTERS

Table of Contents

Executive Summary

Streaming video has evolved into a feature that is in high demand by today's target consumer of childcare services, and industry forecasters predict it will continue to be the norm. Millennial parents are digital natives who prioritize transparency and connectivity in their purchase decisions, making streaming video a standard feature in today's childcare industry. While essential, this connectivity can open a business to serious risk and requires careful consideration when selecting a provider.

Connected devices, including streaming cameras, are part of the Internet of Things (IoT) that has exposed vulnerabilities in network systems, data security, and privacy. This threat carries extra weight in the childcare industry, where privacy and security are paramount.

This threat carries extra weight in the childcare industry where privacy and security are paramount.

Data breaches in the U.S. are growing: the total number of exposed records increased by a staggering 126% from 2017 to 2018 and included major companies like Target, Sony, and Adidas. Small businesses are vulnerable too, and a data breach could cause irreparable harm.

Threats include ransomware, data mining, and public access to private video feeds. The effects of breaches like these have been far-reaching and include victims ranging from major Fortune 500 brands to individual households with streaming devices.

In order to avoid these threats, there are many key factors to consider when installing streaming video in a childcare business. The absolute minimum requirement to protect your business is to choose a built-for-childcare custom software provider with data that is encrypted in both storage and transmission and has been audited by a credible third-party IT firm. The system you select should use a secure cloud service, proper password management, and have qualified technical support for your staff and families to ensure privacy is always the priority.

State of the Childcare Industry

The childcare industry is a reliably strong sector, projected to contribute $57 billion in revenue to the U.S. economy in 2019 alone. With more than 65% of this sector categorized as "center-based" care, these businesses have evolved into learning centers that focus on education, nurturing, and preparation for the academic journeys of children beyond care.[1]

Daycare is part of a service economy because it relies on labor rather than capital to earn revenue. Labor of teachers and staff cannot be outsourced; businesses grow

by adding new technology and services. More childcare centers than ever before are offering streaming video camera systems that enable parents to see their child throughout the day. In 2019, the IBIS Worldwide report, Daycare in the U.S., asserted that this offering is expected to become even more common in the coming years.[2]

The turn toward technology as a differentiator is also a direct response to the wants and needs of today's parents of children who are under five years old. This target market is made up almost entirely of Millennials (born between 1980 and 1998) and this group has an inherent expectation of connectivity and transparency, especially when it comes to their children. In fact, 73 percent of Millennial consumers are willing to pay more for products that guarantee total transparency.[3] Childcare centers that respond positively to these consumer needs are gaining an edge in revenues and in the strength of their brand.

Camera Systems Used in Childcare

Childcare businesses turn to varied products and systems to bring this transparency to the markets they serve. Many of these businesses open with high-end camera systems and streaming video in place as core offerings of their school. Others retrofit simple streaming camera systems into mature operations as part of a concerted strategy to improve the business with a competitive edge.

There are three categories of camera systems typically used in childcare business settings. Each category has unique features and limitations for childcare businesses.

1. **Camera systems designed for childcare centers** are the premium offering in this category, and number few in the industry. These systems are designed with the operations of a daycare business in mind. The unique needs and requirements for childcare as a business are unlike other small businesses with video monitoring, and necessitate features for timed access to spaces, privacy controls, visibility into customer viewing habits, and most importantly data security.

2. **Camera systems from security companies** can do an adequate job, however the software that allows family to view video is often generic and developed by third parties for a range of businesses including gas stations and retailers. These systems don't offer childcare-specific features that limit camera access to only hours a child is in the school's care and only the hours the school is open. Most require special software to watch video that parents often can't download at the office due to IT restrictions. These systems are designed for one end user to stream video at a time and can't handle family members who simultaneously stream video from your center.

3

Off-the-shelf, DIY camera systems with streaming capabilities can be an attractive low-budget option for childcare businesses. However, risks with these systems loom large, ranging from security and privacy breaches to a potentially exorbitant cost of system maintenance and customer support – in both dollars and staff time. These camera systems don't offer secure logins or encrypted data, making the video streams and your school's data vulnerable to exposure.[4] The hardware is not warrantied, and system maintenance and upgrades fall on the shoulders of the business owner.

When childcare centers add third-party technology to improve their customer experience, it's important that they support their customers in using the technology. Using DIY or security company camera systems means that when a childcare center customer has a problem using the technology, the center owner or admin staff is left to provide technical support to the families who need it. This is not only an interruption of their daily responsibilities, but it's a job for which they may not have sufficient technical knowledge to handle. This often results in negative customer experiences and unnecessary staff fatigue.

Streaming Video Camera Systems: The Internet of Things

A streaming video camera, no matter who manufactures or installs it, is part of the "Internet of Things" or IoT. This term describes the rapidly growing network of physical objects that include an IP address for internet connectivity, and the communication that occurs between these objects and other Internet-enabled devices and systems. Thermostats, home appliances, automobiles and even vending machines are now connected to the internet. Market research firm Gartner forecasts that 14.2 billion connected things will be in use in 2019, and that the total will reach 25 billion by 2021.[5]

Half of all businesses cannot detect if any of their IoT devices suffers a breach.

That growing number makes the Internet of Things vulnerable to threats from outside attacks. Research conducted by global security expert Gemalto found that half of all businesses cannot detect if any of their IoT devices suffers a breach.[6] Adding a virus scanner to your PC is simply not enough to protect your network and your business from the latest malware, hacking and other online threats.

HOW BIG IS THE THREAT?

According to the 2018 End-Of-Year Data Breach Report by the Identity Theft Resource Center, the total number of U.S. breaches in 2018 (1,244) fell 23% vs. 2017 (1,632). This may seem like good news, but in fact is not when you look a little deeper. The total number of exposed sensitive records in the U.S. increased by a staggering 126% year over year (446,515,334 in 2018 versus 197,612,748 in 2017).[7] An additional 1.68 billion records were also exposed, including email-related credentials, that were classified by this study as non-sensitive.[8] As most consumers use the same username, email and password combinations across multiple platforms, giving attackers this information can lead to serious digital threats to individuals.

Well-known brands including Adidas (2 million compromised records), Facebook (2 billion accounts scraped) and Marriott (383 million records exposed) have been impacted by data breaches.[9]

In the business of childcare, a data breach can expose extremely sensitive information about your customers well beyond email addresses and credit card information. Your digital files may include each child's date of birth, private medical information, home address and more. The families you serve rely on you to protect this information as part of your agreement to safeguard their children. Using an insecure video streaming system can provide criminals with easy access to this private data.

RANSOMWARE

Data mining is just one of the threats faced by organizations that rely on Internet-enabled devices. Businesses, individuals, and governments are also vulnerable to the use of ransomware. This malicious software or "malware" program is designed to deny access to a computer system or data until a ransom is paid – often demanded in the form of bitcoin digital currency. Recovery from such an attack can be extremely difficult and may require the services of an outside data recovery specialist. Some victims choose to pay to recover their files; however, as with any criminal activity, there is no guarantee that the files will be restored.

> *Adding a virus scanner is simply not enough to protect your network.*

A childcare business could be debilitated if blocked from using their network to access family records, issue invoices, or even send an email, costing them time and money.

Examples of how devastating a ransomware attack can be have been in national headlines this year. The City of Baltimore was recently crippled when digital extortionists froze thousands of computers, shut down email and disrupted real estate sales, water bills, health alerts and many other services for weeks. Criminals utilized a WannaCry ransomware variant to infect the city's computer network. Allentown, Pennsylvania and San Antonio, Texas have been targets of similar attacks, and the New York Times reports

malware attacks cost FedEx more than $400 million and pharmaceutical company Merck, $670 million.[10]

Information security experts at We Live Security confirm that the WannaCry malware threat is ongoing. In a recent report, the firm said that even though two years have passed since the first use of the WannaCry virus, the number of attempts to use the malware and its variants has continued to grow. In fact, as of May 2019, WannaCry-based attacks are at the peak of the program's popularity, with users bombarded with hundreds of thousands of attacks every day.[11]

UNSECURED VIDEO FEEDS

A streaming video camera system is often high on a family's list of requirements for choosing a childcare center. However, if the camera system is not properly secured, the feed can be easily viewed by anyone who cares to look for it. In fact, sites like Insecam.org offer a directory of online surveillance security cameras. Users can select a country to watch live street, traffic, parking, office, road, beach and home webcams. Feeds are available that show medical facilities, inside homes, and inside childcare centers. In the United States alone, over 4,000 live IP (Internet Protocol) video cameras are available for instant viewing via Insecam – no passwords required.

An insecure video streaming system can provide access to private data.

In 2017, the *Huffington Post* reported that cameras from several childcare facilities across Canada were compromised, allowing their live streaming video to appear on publicly available websites that stream footage from unsecured webcams.[12] In a similar incident, a school in North Carolina unknowingly used a system that was not secure, resulting in alarmed parents and a negative story on their local news station.[13]

Many DIY camera systems feature the same default password that users never change. Others have passwords that are built into the system that users never see and aren't easy to change. It's often difficult, if not impossible, for consumers to determine if the camera system they purchased is putting their business at risk.

For example, Hangzhou Xiongmai Technology Co., Ltd. is one of the largest manufacturers of video cameras, digital video recorders (DVRs), and network video recorders (NVRs) in the world. They function as an Original Equipment Manufacturer or OEM, meaning their brand is not shown on the products. Rather, they produce cameras and recorders for other companies. Cybersecurity experts at SEC Consult found more than 100 vendors that sell branded devices with Xiongmai hardware/firmware inside.[14] The problem? Hackers using Mirai malware are able to exploit critical vulnerabilities in Xiongmai devices that offer high-privileged shell access over TCP (Transmission Control Protocol) ports 23 (Telnet) and 9527 (a Telnet-like console interface) using hard-coded credentials. SEC Consult reports that hundreds of thousands of Xiongmai-manufactured devices were infected and used as part of one of the largest distributed denial of service

(DDoS) attacks to date.[15] Your business could be using one of these compromised cameras without even knowing it.

WHO'S CONTROLLING YOUR STREAMING VIDEO?

In the last year, several families reported that hackers have infiltrated their home's baby monitoring camera systems, often using previously compromised passwords. In one case, the hacker used an unsecured Nest camera to speak to a toddler and his parents, who were shocked to discover the breach inside their home.[16] In another, the attacker frightened parents with kidnapping threats using their Nest baby monitor camera system.[17]

WHO'S RESPONSIBLE FOR DATA SECURITY?

Compromised data is a very serious threat to a company's reputation. Loss of trust is the biggest risk a childcare provider can face. The first thing on every parent's list of requirements when choosing a preschool is safety and security. If the streaming video system a school uses to provide an extra level of accountability is not constantly monitored for security breaches, your business can unknowingly provide public access to your customers' personal information.

> *It is often difficult for consumers to determine if their camera system is putting their business at risk.*

With regular headlines revealing the latest security breaches, consumers are more aware than ever of the responsibility businesses have to protect their personal information. Protection from identity theft is big business – with companies like LifeLock, Experian and McAfee earning millions to provide security to individuals. Customers expect your business will safeguard the sensitive data they share with you.

Ten Elements of a Secure Streaming Video Camera System

Your business can safely and responsibly offer streaming video as a service to parents without these fears. Given the potential risks to your business and your customers, it's critical to carefully evaluate potential streaming video providers before signing a contract. Below is a list of ten must-haves the vendor should be able to provide. Beware any camera systems or providers that aren't able to fully meet all of these elements.

1	**Third-Party Security Audit**	Simply adding an antivirus program to your network or asking your vendor to run a software scan is not enough to secure your streaming video service. Reputable childcare video providers have a system that is reviewed and certified by an unbiased third-party internet security firm. Ask to review the report that accompanies a security audit to verify the results.
2	**Software Created for Childcare**	Use a company with software that was built for the business of childcare. Some camera providers simply put their brand on third-party software and some use software that was created for all businesses: retail, gas stations, and others that don't have the same need to protect privacy. Security begins with the developers who create the software. If unknown people can write code for inevitable updates, then they can also, intentionally or unintentionally, create holes in the security of your system.
3	**Restricted Access to Streaming Video**	Video gathered at your childcare center should never be publicly available online without a unique, encrypted password. The feed should be protected by a firewall that protects the information from unauthorized users.
4	**Encrypted Data**	Usernames and passwords should always be encrypted to ensure your data stays secure. All video and user data streaming through the cameras and servers to end users should be encrypted using Transport Layer Security (TLS), the standard in internet data transfer security.
5	**Secure Cloud Services**	All user data related to your streaming video system that is stored in the cloud should be encrypted and protected by a reputable provider, such as Amazon Web Services (AWS).

6	**Separate Network for Cameras**	You want to avoid granting access to your business network when you offer a streaming video service to parents. Use a dedicated, separate network for cameras to protect other data, such as family records and financial information. This restricts possible access to customer data and reduces your exposure should parents experience a breach of their personal network.
7	**Proper Password Management**	Your roster is constantly changing. In order to keep your streaming video system secure, you'll need a strong system in place to add new users, update passwords and revoke access to parents who leave the center. If your solution is to provide the same username and password to everyone, you're taking a significant security risk.
8	**Ongoing Security Monitoring**	Enterprise systems are constantly under attack. Work with a provider who can and will constantly monitor your camera system for data breaches and new threats. Security measures should be part of the standard operating procedure for the system from day one, not an afterthought that's only considered after a breach has happened.
9	**Regular Software Updates**	Browsers and operating systems are constantly changing. Your system requires regular updates to the streaming software to ensure it works with every new version and delivers a secure and quality experience to parents. Ensure your provider takes care of this automatically and without added cost to you.
10	**Technical Support**	From the initial hardware installation throughout the entire lifetime of a camera system, businesses need qualified, live technical support for all users of the system. Childcare centers constantly add new families to the roster and that means a steady stream of users who need support. A professional service provider designed for the business of childcare can handle those issues for you.

Ensure Data Security: The WatchMeGrow Approach

WatchMeGrow was built for the business of childcare, and privacy is the single most important driver of our business. In more than 20 years of operation, we've never had a case of unauthorized video access.

Our software has been reviewed and vetted by a dedicated team at Leviathan Security Group, a respected IT security firm. After a detailed evaluation, Leviathan determined that WatchMeGrow security protocols are the industry standard.

All data and personal information for centers using WatchMeGrow is stored securely in the cloud with Amazon Web Services (AWS), one of the world's most secure, powerful and trusted cloud-based data solutions. AWS uses KMS (Key Management Service) to encrypt your data with validated cryptographic modules.

Our in-house development team manages every inch of our software. That means we alone control our security and optimize our functions for schools' needs.

We are proud to offer the industry's leading and most secure multi-user platform, so that you can deliver the best user experience to an unlimited number of concurrent users.

Compare Before You Invest

Finding the right streaming solution means knowing the right questions to ask. We can help you answer them to be sure you're offering the most secure streaming video camera system available.

Call us toll free: 1-800-483-5597

Email us: grow@watchmegrow.com

References

1 IBISWorld Industry Report 64221, Day Care in the U.S., March 2019

2 IBISWorld Industry Report 64221, Day Care in the U.S., March 2019

3 Sprout Social Report, Social Media and the Evolution of Transparency, August 2018

4 Over nine million cameras and DVRs open to APTs, botnet herders, and voyeurs: ZDnet, 10/9/2018

5 Gartner Identifies Top 10 Strategic IoT Technologies and Trends: Gartner, November 2018

6 Almost half of companies still can't detect IoT device breaches, reveals Gemalto study: Gemalto, January 2019

7 2018 End-Of-Year Data Breach Report: Identity Theft Resource Center

8 2018 End of Year Data Breach Report: Identity Theft Resource Center

9 2018 End-Of-Year Data Breach Report: Identity Theft Resource Center

10 In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc: New York Times, 5/25/2019

11 EternalBlue reaching new heights since WannaCryptor outbreak: We Live Security, 5/17/2019

12 Unsecured Webcams Are Broadcasting Canadian Daycares, Schools Online: Huffington Post, 5/4/2017

13 WTVD video

14 Millions of Xiongmai Video Surveillance Devices Can Be Hacked via Cloud Feature (XMEYE P2P Cloud): SEC Consult, 10/9/2018

15 Millions of Xiongmai Video Surveillance Devices Can Be Hacked via Cloud Feature (XMEYE P2P Cloud): SEC Consult, 10/9/2018

16 Hacker spoke to baby, hurled obscenities at couple using Nest camera, dad says: Big Country 2/1/2019

17 Nest camera hacker threatens to kidnap baby, spooks parents: Big Country 12/18/2018