Cyber Security and Cloud Video Surveillance

August 2018

Eagle Eye Networks | 4611 Bee Caves Rd, #200 | Austin, TX 78746
www.een.com | +1-512-473-0500 | sales@een.com

This paper explains why video surveillance system security can and should be more fully addressed within the industry, so that cyber security is not left as a problem for installers or customers to solve. Eagle Eye Networks is a leader in this respect, mitigating security concerns from the point of product research, development and deployment.

Introduction

Today's networked video surveillance systems are vulnerable in many ways, and their cameras have been weaponized by hackers to create massive Distributed Denial of Service (DDoS) attacks on targeted systems. **Figure 1** presents a timeline of recent cyber attacks and threats affecting Internet-connected security cameras and digital video recorders (DVRs).

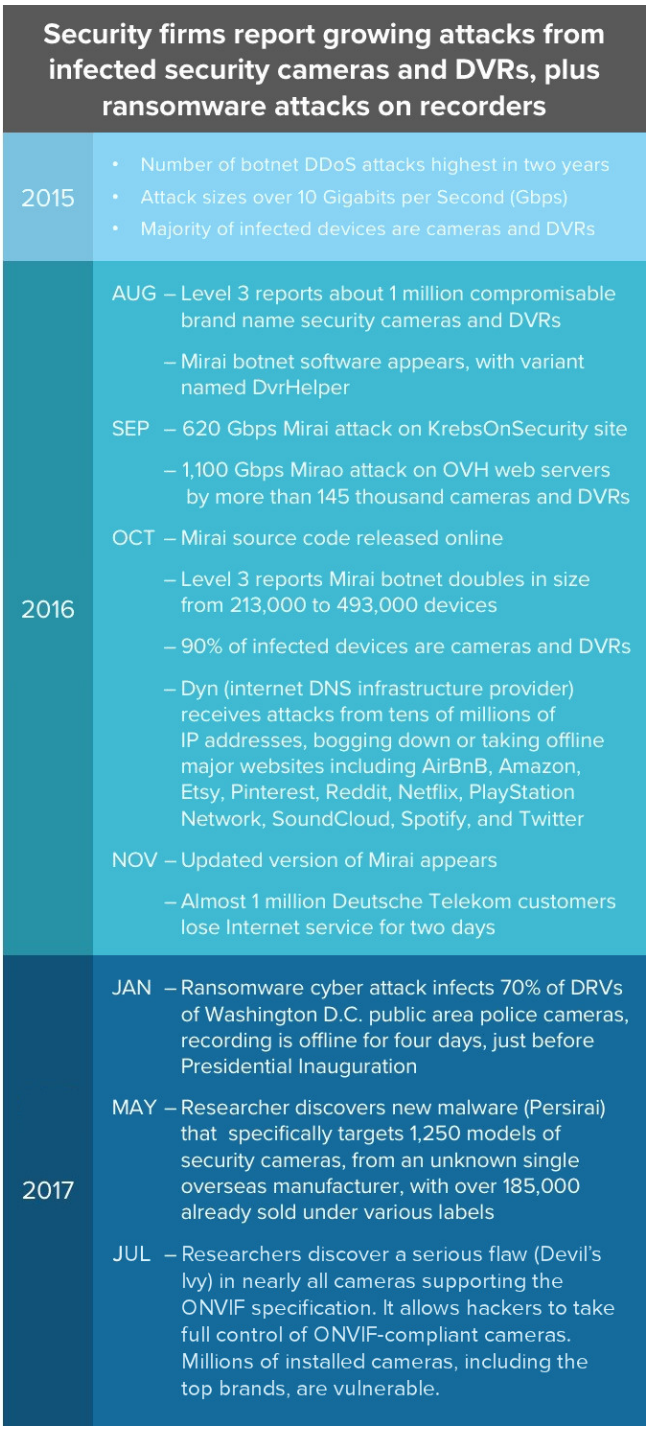
Securing today's networked video systems can be a complex and difficult technical challenge. However, especially for small and medium size businesses, it doesn't have to be that way. Video systems and equipment can be purpose-built to constitute a pre-hardened and more easily securable system, in contrast to the current installed base of networked video technology.

In September of 2016, a large French web-hosting provider reported a record-breaking 1-terabit-per-second DDoS attack against their web servers, unleashed by a collection of more than 145 thousand hacked Internet-connected video cameras and digital video recorders.

In October of 2016, DDoS attacks were launched from tens of millions of IP addresses against Dyn, an Internet infrastructure company headquartered in New Hampshire. The attacks bogged down or took offline dozens of major websites including AirBnB, Amazon, Etsy, GitHub, Netflix, Pinterest, Reddit, PlayStation Network, SoundCloud, Spotify, and Twitter.

Researchers have reported that over 90% of the attacking devices were compromised network security cameras and DVRs, and that most of the compromised devices are in the U.S. In August 2016, researchers

Figure 1. Timeline: escalating cyber attacks on security video cameras and DVRs.



reported that about one million web-connected video cameras and DVRs were infected with malware. Most of the camera and DVR owners are unaware that their devices are infected.

In January 2017, in a ransomware cyber attack, cyber criminals infected 70 percent of the 187 video storage devices that record data from federal surveillance cameras in Washington D.C., taking video recording offline for about four days, just prior to the presidential inauguration.

These and other similar incidents are proof that securing video systems should be of paramount concern to security video equipment manufacturers, to installing security integrators, and to their end-user customers. However, hacker defense is just one part of ensuring that security video systems live up to their purpose – to faithfully monitor and record the activity within their cameras' fields of view.

Video System Cyber Security

Computer and network security focuses on protecting the *confidentiality*, *integrity*, and *availability* (CIA) of the networked systems and the data they contain. These three factors are paramount for video systems, given the potential for any camera's recorded video to become critical legal evidence. Additionally, today's video systems have become operationally important to many types of businesses, both for the instant oversight capability they provide, and for the business insights enabled by a wide variety of video analytics. Anywhere, anytime availability of video via mobile devices is a basic business expectation these days.

However, for most video systems, Internet connectivity puts confidentiality, integrity, and availability at risk because most systems don't have built-in protection against cyber attacks. Thus, many video systems are defenseless against cyber attacks, even though the continuing escalation of such attacks makes it more important than ever for video systems to be cyber secure.

General-Purpose vs. Purpose-Built Equipment

Traditionally, networked video management systems were built from general-purpose computers, network switches, routers and firewalls that require a significant amount of highly technical configuration to operate as a cyber-secure system. Leading manufacturers provide system or device hardening guides about how to set up appropriate cyber security controls. Even then, security hardening remains an ongoing project that requires continuing attention and updating, as products are improved and as new cyber threats emerge.

Configuring a secure VMS from general-purpose equipment is a lot to ask of video system installers and customers, especially because it's not necessary. Manufacturers of purpose-built video surveillance products can and should provide security pre-configured systems, because they designed and built the equipment and wrote the software that needs to be hardened. Furthermore, a cloud-based video surveillance system, provided as a service, can and should include the continuing attention and updating that effective cyber security protection requires.

The remainder of this paper explains how Eagle Eye Networks addresses cyber security protection and simplifies video system deployments using purpose-built design.

Video System Cyber Vulnerabilities

Most cyber attacks work by gaining access via user login credentials, and then exploiting device and systems vulnerabilities to obtain a high level of access that gives attackers full control. Factory default passwords, easily-guessed passwords, passwords transmitted in plain text, and weaknesses that allow access privileges to be escalated, are how most automated and manual cyber attacks succeed. A search for “cameras DVRs DDoS” (without quotes) on the website krebsonsecurity.com lists many detailed articles about vulnerable name brand security cameras and recorders. These are the makes and models of cameras that were compromised and made to join the botnets that created the DDoS attacks described earlier.

Large scale botnet attacks manifest themselves quickly, due to their size and impact, and garner significant media attention. However, undetected small-scale manual attacks on video systems can be deadlier to a business, for example, by allowing a would-be thief to remotely “case” a store by viewing in-store activity such as cash handling and the stocking of merchandise.

Preventing Unauthorized Access

Eagle Eye Networks’ self-configuring system design eliminates the need for installers to log onto on-premises Eagle Eye video appliances, thus the appliances don’t have the typical username and password vulnerabilities. The appliances automatically connect themselves to the Eagle Eye Cloud Security Camera Video Management System (VMS), and ignore any inbound connection requests from the Internet.

Eagle Eye appliances isolate the cameras from the Internet. Because there is no way to access cameras directly from the Internet, camera password vulnerabilities cannot be exploited by Internet-based botnet malware or remote manual hacking attempts.

The Eagle Eye appliances use digital certificates to establish encrypted data connections and authenticate themselves to the Cloud Security Camera VMS in the Eagle Eye Cloud Data Center. Live and recorded video are accessed securely via the Cloud Security Camera VMS, which offers a choice between two-factor or biometric user authentication to grant user access to cameras and recorded video.

Eagle Eye Cyber Security Benefits

Eagle Eye’s well-architected cloud-based video management system provides several important cyber security benefits lacking in fully premises-based systems:

- **Strong Security Profiles.** The strong physical and cyber security profiles of Eagle Eye’s highly secure cloud data centers are too difficult and costly to implement for fully on-premise video surveillance systems, especially for small offices, shops, service centers and production facilities. With a cloud-based system, all customers affordably share in the strong security provided for live and recorded video access.
- **Managed Systems.** Eagle Eye on-premises video appliances are managed from the Eagle Eye Cloud Data Center and are automatically kept up to date with security and feature updates. Installers and customers are relieved of that burden.

- **System and Data Redundancy.** Eagle Eye's servers and databases reside in multiple cloud data centers, so that continuous system uptime is maintained regardless of the state of any individual server or data storage device. Local video storage can provide additional redundancy.

Thanks to mobile computing, the Eagle Eye Cloud Camera Security VMS can securely extend its always-on availability to any location from which the Internet can be accessed. The Eagle Eye cloud-based video management system software, combined with Eagle Eye purpose-built on-premises equipment and provided through an as-a-service model, constitute the most affordable way to achieve the highest levels of confidentiality, integrity, and availability for surveillance video.

System Architecture

The Eagle Eye *Cloud Security Camera* VMS is a cyber-secure cloud-based system that replaces traditional DVRs (digital video recorders) and NVRs (network video recorders) with:

- **On-premises Eagle Eye custom-built appliances.** *Bridges*, for receiving and buffering video, audio, alarm and event data from cameras and video encoders, and sending it to the Eagle Eye cloud data center, and *Cloud-Managed Video Recorders (CMVRs)*, which perform all the Bridge functions plus locally store video on-premises. The required networking, routing and firewall functionality is built into the appliances to ensure the integrity of the on-premise components.
- **Off-premises Eagle Eye custom-built data center equipment.** *Eagle Eye Cloud Security Camera VMS Platform* and *Video API Platform* application servers, system data storage, and video data storage, all located in the Eagle Eye Cloud Data Center.

The Eagle Eye system is completely based on a modern redundant cloud architecture that provides a web browser-based interface and comprehensive mobile applications for iOS and Android smartphone and tablet devices. **Figure 2** depicts the system architecture.

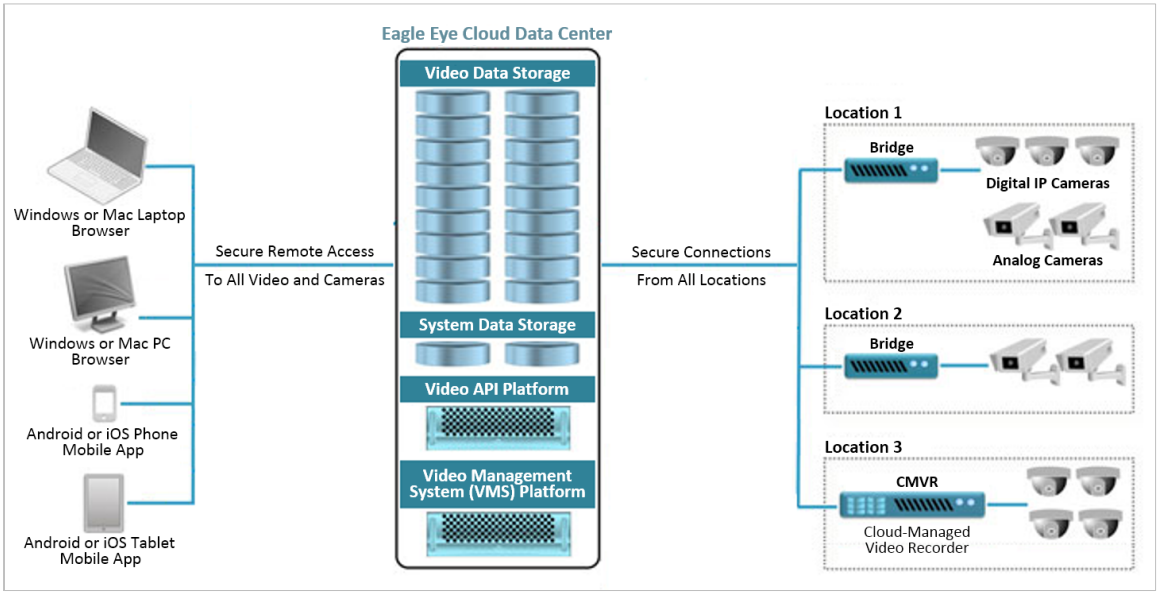


Figure 2. Eagle Eye Video Management System Architecture

Recording is typically performed off-premises in the Eagle Eye Cloud Data Center, though at the user's request can also be performed on-premises where the cameras are located, or using a combination of the two storage locations on a per-camera basis. When recording is performed off-premises, the Eagle Eye on-premises equipment buffers the data locally, so that no video is lost in the event the Internet connection is severed.

Camera and Data Isolation

For both on- and off-premises recording, cameras are never directly connected to the internet. For off-premises recording, Eagle Eye Bridge appliances aggregate and buffer the video data for secure encrypted transmission to the Eagle Eye Networks Cloud Data Center. For on-premises recording, Eagle Eye CMVRs record locally and continue to ensure that cameras have no direct link to the Internet. This ensures a high level of confidentiality.

Eagle Eye Cloud Data Center

At the center of the system architecture is a set of highly secure data centers, which cooperate with each other and maintain secure connections to customer-premise appliances. The data centers implement a redundant data storage scheme under which customers' video data is stored on three different archivers, making the loss of any recorded video highly unlikely. For simplicity's sake, these data centers are collectively referred to as the Eagle Eye Cloud Data Center.

Data center design includes compartmentalized security zones that have biometric access controls. All data center components are fully fault-tolerant including redundant network uplinks, application servers, data storage, chillers, HVAC systems, power panels and power distribution. Network distribution is redundant, including dual network cards in servers. Electrical power is provided from two different sources, such as two different utility substations, and two backup generators are utilized (one for each power source). There is no single point of failure. These requirements establish 99.999% hardware availability.

Eagle Eye Cloud Data Center locations are outfitted with biometric scanners and secure card access to the collocation services areas of the data center. On-site security personnel monitor hosting facilities 24/7 via indoor and outdoor video surveillance. Data center access requires security desk check-in and is managed 24/7. Local key management is enforced for racks and cabinets.

The Eagle Eye Cloud Data Center's multi-layered approach to network security includes perimeter firewalls, network intrusion prevention systems, network address translation (NAT), and network segmentation whereby database servers are not visible to the public. Also, data center environments are both logically and physically separate from the Eagle Eye corporate office network. Internet access is provided through redundant Internet backbones.
Eagle Eye utilizes extensive screening and background checks for Eagle Eye personnel who have data center physical access or privileged logical access to the Eagle Eye Cloud Data Center platform.

Eagle Eye On-Premises Appliances

Eagle Eye appliances buffer video locally and send it to the Eagle Eye cloud using Eagle Eye's *Intelligent Bandwidth Management*™ technology, which is designed to deal with the reality of limited bandwidth. Intelligent Bandwidth

Management adjusts data transmission and bandwidth utilization dynamically, and prioritizes transmissions to optimally utilize the existing Internet connection. As shown earlier in **Figure 2** there are two categories of Eagle Eye appliances:

- *Bridges*, which buffer video and send it to the cloud, performing encryption, video data de-duplication, bandwidth management, motion analysis, and video compression; and
- *Cloud-Managed Video Recorders* (CMVRs), which perform all the functions of a *Bridge* plus record video locally and optionally send it to the cloud.

Both standalone and rackmount versions of the Eagle Eye appliances do not require a third-party network switch or router to keep cameras isolated on their own network, and to encrypt and send their video data to the Eagle Eye Cloud Data Center. Each appliance has at least two network ports, one for the camera network and one for connecting to the Internet. The appliances contain the required networking, routing and firewall functionality. Some appliances have additional POE network ports for connecting to individual cameras, to enable remote power cycling for each camera.

Simple Secure Deployment

Securely deploying Eagle Eye appliances is simple because they are all designed as “locked down” devices, have no open ports, accept no inbound communications, and are pre-configured to automatically authenticate and connect to the Eagle Eye Cloud Security Camera VMS. No configuration is required to establish network connections. Cameras are auto-discovered, and must be manually approved before they are enrolled in the system. Bridges and CMVRs act as DHCP servers for network cameras, so that it is not necessary to manually set camera IP addresses.

Cyber Security Features

Eagle Eye’s cloud-based, purpose-built VMS infrastructure provides high assurance of confidentiality, integrity and availability for surveillance video using a variety of standards-based cyber security best practices. The sections below describe how Encryption and Digital Certificates are used by the Eagle Eye Cloud Security Camera VMS infrastructure. Additional security measures of the Eagle Eye organization and its technology infrastructure are also described.

Eagle Eye Data Encryption

Encryption is the process of changing data so it is unreadable (encrypting), in a way that it can be changed back into its readable form (decrypting). The simplest kind of encryption uses a single set of characters (numbers, letters and/or symbols) – the encryption key – to both encrypt and decrypt the data.

Eagle Eye uses a technique called *public key encryption,* which works because of a mathematical fact that a pair of very large numbers can have a special relationship to each other, whereby what you encrypt with one number (using special methods) you can decrypt only with the other number, and vice versa. Yet if you have one of the numbers, you cannot figure out the other number. This simple but unbreakable relationship between the numbers

enables many types of trust relationships and data secrecy capabilities.

Public key encryption is the short name for *public/private key encryption.* By keeping one key private and only sharing the other key (the public key), two important capabilities are established:

- Source Authenticity. Information that is encrypted using a private key, can be shared and decoding using the corresponding public key, thus verifying its source—the holder of the private key.
- Information Privacy. Encrypting information using a public key ensures that only one person (or system) can decrypt it—the holder of the private key.

Whenever we see the term “public key”, we know that there is also a private key also involved.

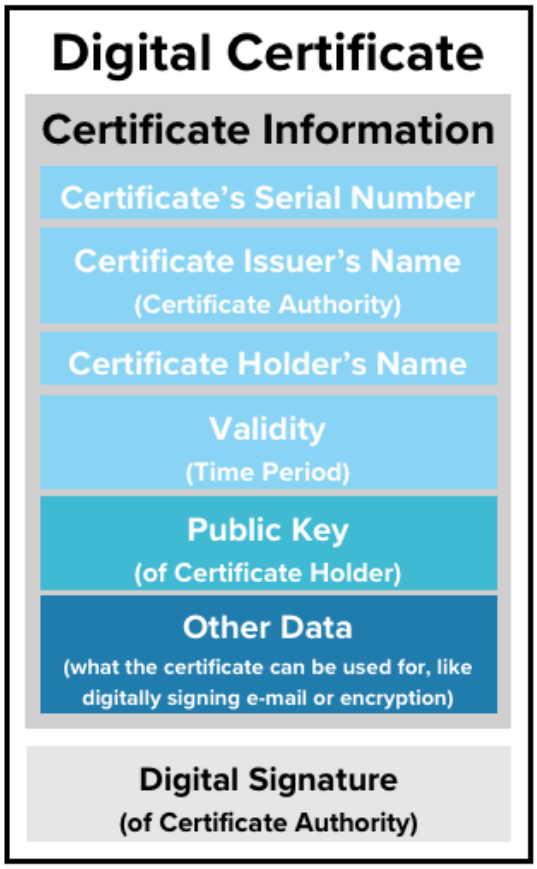
Managing Public and Private Keys

Where do public/private key pairs come from? How are keys distributed securely? These and other issues are addressed by the ANSI X.509 standard for a public key infrastructure (PKI) for digital certificates, public-key encryption and public key management.

Digital Certificates

Digital Certificates are small electronic document files. Each file contains information that can be used to prove the authenticity and integrity of the digital certificate file and its data. Public keys are part of the information in a digital certificate, as shown in **Figure 3.**

Figure 3. Example of Digital Certificate



Digital Certificate Uses

A digital certificate lists the uses that the certificate holder intends for it, such as:

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Ensures software came from software publisher
- Protects software from alteration after publication
- Protects e-mail messages
- Allows data to be signed with the current time
- Allows data on disk to be encrypted
- Allows secure communication on the Internet

Eagle Eye uses digital certificates to encrypt stored data, and to establish secure connections between users and the Eagle Eye Cloud Security Camera VMS, and between Eagle Eye appliances and the VMS.

Eagle Eye's Use of Digital Certificates

Eagle Eye uses digital certificates described by the ANSI X.509 standard, which calls for a Certificate Authority (CA) – a trusted party that can externally validate the identity of certificate holders prior to their issuance – to manage the creation, management, and revocation of certificates.

For authentication of connections to the Eagle Eye Cloud Security Camera VMS, Eagle Eye uses digital certificates issued by a recognized third-party Certificate Authority, whose certificates are trusted by the major web browsers. For authentication of connections to Eagle Eye appliances, Eagle Eye acts as its own Certificate Authority and issues its own certificates, which Eagle Eye knows it can trust, because it can guarantee a physical chain of custody during the installation of certificates into the appliances as part of the manufacturing process. This works because only Eagle Eye systems and devices can be part of the authentication processes that use the Eagle Eye digital certificates.

Eagle Eye Cloud Data Center Authentication

For browser and mobile app communications, as mentioned earlier, Eagle Eye Cloud Data Center servers use a third-party digital certificate to establish the secure TLS connection. Most browsers allow viewing the contents of the certificate used to establish the connection, enabling users to verify that they are indeed connected to an actual Eagle Eye Cloud Data Center server.

Eagle Eye Appliance Authentication

As mentioned earlier, Eagle Eye appliances use self-signed digital certificates to authenticate themselves to the Eagle Eye Cloud Data Center.

Transmitted Data Encryption

The Eagle Eye web application, mobile apps, and APIs communicate via HTTPS, using Transport Layer Security (TLS). The TLS protocol aims primarily to provide *privacy* and *data integrity* between two communicating computer applications. TLS accomplishes this in three ways:

- Authenticating the communicating applications using digital certificates.
- Ensuring the connection is private by using strong data encryption.
- Including a message integrity check using a *message authentication code* to prevent undetected loss or alteration of the data during transmission.

The Eagle Eye web application, mobile apps, and APIs utilize TLS version 1.1 or higher, using the SHA-256 secure hash algorithm with a 2048-bit RSA key.

Stored Data Encryption

Stored data is protected using Advanced Encryption Standard (AES) 256-bit encryption, both on the Bridges and in the Eagle Eye Cloud Data Center. Encryption keys are stored and exchanged using Eagle Eye digital certificates.

User Authentication

The Eagle Eye Camera Security VMS provides several types of secure sign-in user access:

- User two-factor authentication
- Apple Touch ID fingerprint authentication
- First responder real-time video access

User Two-Factor Authentication

Users are Eagle Eye customer personnel with assigned privileges to sign into Eagle Eye applications (mobile apps or browser apps) to access video or manage cameras. *Two Factor Authentication* is used to provide strong security by establishing trusted user devices (PCs, laptops, tablets and smartphones) and only allowing camera and video access from those trusted devices. Attempts to sign in using a non-trusted device result in access being denied. Two-factor authentication utilizes the following mechanisms:

- **Trusted Device.** A trusted device is a mobile device or a browser on a specific computer that has previously registered using two-factor authentication. It's a device that is known to be associated with that Eagle Eye User.
- **Security Code.** A security code is a one-time-use code sent to a trusted device or phone number when the user logs in for the first time using a new device or browser.

Apple Touch ID Fingerprint Authentication

The Eagle Eye VMS supports Apple Touch ID fingerprint biometrics, to minimize the chance of a third party observing password entry, and additionally, to make login more secure and convenient. The mechanism utilizes the iOS Keychain password storage, and allows the user's fingerprint to be used for login.

First Responder Real-Time Video Access

The Eagle Eye Cloud Security Camera VMS allows customers to pre-designate first responders who are able receive immediate real-time security camera access during emergency situations, via the free Eagle Eye Viewer mobile app or any major web browser. Customers also specify which of their own personnel are authorized to activate emergency responder access when an incident is occurring.

First responder permission can be restricted to specific groups of cameras; for example, to outdoor cameras and public lobby areas only. The cameras are kept private and are only shared when an authorized user activates first responder access. When first responder access is activated, the first responders are sent an email that contains links to specific cameras they are authorized to view. The links will open camera views in the app or web browser.

Application Security

The operating system, web server and application software are kept updated with the latest and safest available

software. API security is implemented both for Eagle Eye applications and for third-party API integrations. Eagle Eye performs penetration testing and application scanning as part of the development process. Additionally, regular penetration testing is performed on the Eagle Eye Cloud Security Camera VMS. Periodically prospective customers who have in-house penetration testing capability will request permission to perform penetration on the Eagle Eye Cloud Security Camera VMS.

Customer Data Protection

Hardware and software configurations and multitenant security controls keep customer data separate. Each customer can view only its own live and recorded video, and system information. When connected to the Eagle Eye Cloud Security Camera VMS, each customer has no visibility into any other customer's system and cannot access anyone other customer's data.

Advanced Networking Requirements

Some facilities, especially critical infrastructure facilities, are maintained by highly capable IT departments who prefer to provide their own network infrastructure for security camera video networking. In such cases, Eagle Eye collaborates regarding networking requirements to ensure that customer network standards and practices are appropriately applied to the deployment of the Eagle Eye Cloud Security Camera VMS.

Eagle Eye Security Practices

Eagle Eye applies strict privacy and information security standards in the handling of customer information. Our customer contracts include confidentiality provisions that prohibit our disclosing the confidential information of our customers, except under specifically defined circumstances, such as when legally required. Our employees sign confidentiality agreements, are trained on and follow our information privacy and security policies and procedures. For example, password management policy requires that that strong, not-easily-guessed passwords are used, that passwords are changed frequently, that passwords are not written down anywhere.

Eagle Eye has published, and strongly encourages all users of any type of security camera system to adopt, security camera system best practices for cyber security.

Summary of Technical Cyber Security Measures

The lists below summarize the cyber security technical measures described in this paper:

On-Premises Equipment Cyber Security

- No inbound internet connections accepted
- Cameras are isolated from the Internet
- Appliances have no open network ports
- Appliances are protected against pre-installed camera malware

- Appliances use TLS connections to Eagle Eye Cloud Security Camera VMS
- Encryption applied to buffered and locally recorded video
- Appliance authentication via digital certificates
- Collaboration regarding customer advanced networking requirements

Data Center Physical Security

- Facility alarmed intrusion detection system
- Biometric facility area access control
- 24/7 on-site security personnel
- 24/7 on-site live and recorded video monitoring
- Security desk visitor identity verification and visitor log
- Biometric physical access control
- Local key management is enforced for racks and cabinets
- Extensive screening and background checks for Eagle Eye personnel with data center or Eagle Eye Cloud Security Camera VMS access.
- Data Center Network Security
- Network perimeter firewalls
- Network intrusion prevention systems
- Network address translation (NAT)
- Network segmentation to isolate database servers
- Logical and physical separation of data center environments from Eagle Eye corporate network

Redundancy

- Eagle Eye Cloud Security Camera VMS components are redundant (active/active or active/passive)
- Triple-redundant video data storage

Application and Data Security

- Regular server vulnerability scanning
- Regular penetration testing
- API level security
- Web and mobile application use two-factor authentication
- Use mobile device fingerprint authentication
- Web and mobile application TLS connections to Eagle Eye Cloud Security Camera VMS
- AES encryption of recorded video
- Multi-tenant data security controls

Conclusion

Eagle Eye Networks has significantly reduced video surveillance system cyber security risks by:

- Designing and building highly secure data centers based on a modern redundant cloud architecture

- Developing a cyber-secure cloud-based Security Camera Video Management System with standards-based encryption of video data and strong authentication of users and mobile devices
- Manufacturing purpose-built self-configuring secure video appliances that isolate cameras from Internet cyber threats
- Managing Eagle Eye appliance security and feature updates automatically, with no installer or end user action required.

Thus, Eagle Eye provides the most affordable way to achieve *the highest levels of confidentiality*, *integrity*, and *availability* for surveillance video as a well-managed subscription-based service.

About Eagle Eye Networks

Founded in 2012, Eagle Eye Networks, Inc., ('Eagle Eye') is the leading global provider of cloud-based video surveillance solutions addressing the needs of businesses, alarm companies, security integrators, and individuals. Eagle Eye's 100% cloud managed solutions provides cloud and on-premise recording, bank level security and encryption, and broad analog and digital camera support - all accessed via the web or mobile applications. Businesses of all sizes and types utilize Eagle Eye solutions for operational optimization and security. All Eagle Eye products benefit from Eagle Eye's developer friendly RESTful API platform and Big Data Video Framework ™, which allow for indexing, search, retrieval, and analysis of live and archived video. Eagle Eye's open Video API has been widely adopted for integration in alarm monitoring, third party analytics, security dashboards, and point of sale system integrations.

Eagle Eye sells its products through authorized global resellers and installation partners. Headquartered in Austin, Texas, USA, Eagle Eye has offices in Europe and Asia.

About Dean Drako

Founded by Dean, Eagle Eye Networks is the first cloud-based video surveillance company to provide both cloud and on-premise recording.

Dean has led, and continues to lead, remarkable security related firms throughout his impressive career. Concurrently with Eagle Eye Networks, Dean is the owner and Chairman of Brivo, a cloud access control company. Previously, as founder, president and CEO of Barracuda Networks, Dean created the industry's first email security appliance. Prior to Barracuda Networks, Dean founded Boldfish, a leading provider of enterprise outbound email solutions that was acquired by Siebel Systems in 2003. Dean was founder, President and CEO of Design Acceleration, Inc. (DAI), a maker of superior design analysis and verification tools, which was acquired by Cadence Design Systems in 1998.

Dean was founder, Dean received his BSEE from the University of Michigan, Ann Arbor and MSEE from the University of California, Berkeley.

Goldman Sachs named Dean as one of the "100 Most Intriguing Entrepreneurs of 2014."

Headquarters

Eagle Eye Networks
4611 Bee Caves Rd.
Suite 200
Austin, TX 7874
Tel: +1-512-473-0500
Web: www.een.com
Sales: sales@een.com

EMEA Office

Eagle Eye Networks B.V.
Hogehilweg 19
1101 CB
Amsterdam
The Netherlands
Tel: +31 (0) 88 00 68 450
Sales: EMEAsales@een.com