EAGLE EYE NETWORKS

SECURE CLOUD VIDEO SURVEILLANCE

Eagle Eye Networks Cybersecurity Guide

TABLE OF CONTENTS

Video surveillance system security can and should be more fully addressed within the industry, so that cybersecurity is not left as a problem for system integrators, installers, or customers to solve.

Eagle Eye Networks is a leader in this respect, mitigating security concerns starting with system design and extending to continuous cybersecurity management on the cloud. The Eagle Eye Cloud VMS (video management system) is designed to protect against system vulnerabilities and provides automatic system security updates via the cloud.

Introduction

Cybercriminals can attack an organization of any size at any time. Criminals target any potential weakness to breach a company's network to access identity, payroll, credit card, and other critical data information. The frequency of both attacks and security breaches rises each year, and the associated costs rise, too. According to IBM's annual report on data breach costs, which analyzed security breaches on businesses of all sizes, the global average cost of a data breach is now over $4 million.

Organizations of all sizes rely on a network of interconnected systems to operate, and any of those individual systems can present security weaknesses. A secure networked system eliminates as many risks as possible to protect the confidentiality, integrity, and availability (CIA) of the system and the data it contains.

Network-connected video surveillance systems are not immune to cyberthreats. For years, surveillance cameras and recorders have been weaponized by hackers to create Distributed Denial of Service (DDoS) attacks on targeted systems, impacting businesses of all sizes.

Figure 1 outlines several of the most notable cyber attacks and vulnerabilities that have affected Internet-connected security cameras and digital video recorders (DVRs) in recent years. These and other similar incidents highlight the ongoing threat to video surveillance systems.

2021	MAR	Massive breach of security company Verkada exposed live feeds of 150,000 surveillance cameras inside hospitals, companies, police departments, schools, and other institutions, compromising privacy for customers, patients, and others — and exposing organizations to legal and regulatory risk.
	JUL	Serious, exploitable firmware vulnerabilities discovered in IP camera firmware from UDP Technology, used in dozens of vendors' surveillance products, exposing the security footing of internet-exposed camera infrastructure.
2022	APR	BotenaGo malware variant targets Lilin DVRs for infection with Mirai botnet, reducing their functionality and turning these DVRs into sources of attacks on other networks.
	JUN	Record-breaking DDoS abused HTTP/2 multiplexing (from devices including security cameras of an unnamed Chinese telecommunications company) to send 25.3 billion requests, disrupting camera networks and impacting network bandwidth.
	AUG	Despite available security updates, many of 80,000 unpatched Hikvision cameras across 20,000 organizations were used as part of a Mirai-based botnet.
2023	FEB	Vulnerability allows hackers to remotely tamper with Dahua security cameras, compromising the security and availability of affected cameras

Figure 1. Timeline: Continuing cyberattacks on security video cameras and DVRs.

VIDEO SYSTEM CYBER VULNERABILITIES

Modern video surveillance systems are useful because they incorporate powerful processors and extensive networking capabilities, both wired and wireless. For many video systems, however, internet connectivity puts confidentiality, integrity, and availability (CIA) at risk because many systems do not have built-in protection against cyberattacks. The continuing escalation of attacks makes it more important than ever for video systems to be cyber secure.

Misconfiguration errors, exploits by cybercriminals, and bugs in conventionally installed camera infrastructure can expose valuable video information and other data.

Many cyber attacks work by gaining access through phishing attempts or user login credentials, and then exploiting device and system vulnerabilities to obtain a high level of access that gives attackers full control. Factory-default passwords, easily- guessed passwords, and passwords transmitted in plain text that allow access privileges to be escalated are how most automated and manual cyber attacks succeed.

DVRs (digital video recorders) and NVRs (network video recorders) typically need manual system security updates, often involving a scheduled site visit from a technician. These security patches are often overlooked, or in some cases not provided by the manufacturer, creating a weakness in the system.

IS YOUR CAMERA INFRASTRUCTURE SECURE?

Here are some resources you can use to check your existing camera security system for potential flaws:

- Search for vulnerability information at security-focused sites such as **Krebsonsecurity.com** Use search terms such as "camera vulnerability" or "NVR DDoS" to find detailed articles about security vulnerabilities.
- **General internet search:** Look up your camera's manufacturer for general information, or search product name or model for specific security alerts.
- **Monitor the manufacturer's website** for security alerts or firmware updates, or sign up for direct notifications.
- Visit public sites such as the U.S. government's **Cybersecurity and Infrastructure Security Agency (CISA),** where you can search for broad terms (such as "video surveillance") for more detailed information.

VIDEO SYSTEM CYBERSECURITY

Traditionally, video surveillance systems are built from general-purpose computers, network switches, routers, and firewalls that require highly technical configuration and ongoing, manual software and firmware security updates to operate as a cyber-secure system. Configuring a secure video surveillance system from general-purpose equipment is a lot to ask of video system installers and customers—especially when there is an easier solution.

Manufacturers of purpose-built video surveillance products, rather than leaving cybersecurity as a problem for system integrators, installers, or customers, can and should provide secure, 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 updates that effective cybersecurity protection requires.

The Eagle Eye Networks Cloud VMS (video management system) provides a purpose-built cloud video surveillance solution designed to reduce the risk of known vulnerabilities to surveillance systems. The subscription-based VSaaS model delivers automatic security updates, and a team of experts are responsible for the ongoing cybersecurity of the cloud, helping achieve the highest levels of confidentiality, integrity, and availability (CIA) for surveillance video.

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

Eagle Eye Cybersecurity Benefits

Eagle Eye Networks is committed to cybersecurity and has completed SOC 2 Type 2 compliance, considered the gold standard of independent security audits. The company has also completed conformance with the comprehensive ISO 27001:2013 security standards. Eagle Eye applies strict privacy and information security standards in the handling of customer information. Our employees undergo thorough background checks, sign confidentiality agreements, and are trained on and follow our information privacy and security policies and procedures.

SYSTEM OVERVIEW AND ARCHITECTURE

The Eagle Eye Cloud VMS is a secure, fully managed cloud video surveillance solution, delivering an end-to-end video management system with hardware and software designed to provide unmatched security and accessibility. The Eagle Eye Cloud VMS provides authorized users access to live and recorded video and is used to install, configure, and manage the system.

The Eagle Eye Cloud VMS is built and maintained by physical and cybersecurity experts to protect the CIA of your data. The software and firmware supporting the platform are managed and updated by Eagle Eye Networks. Additionally, Eagle Eye performs penetration testing and scanning to ensure the cybersecurity of the platform.

EAGLE EYE ARCHITECTURE

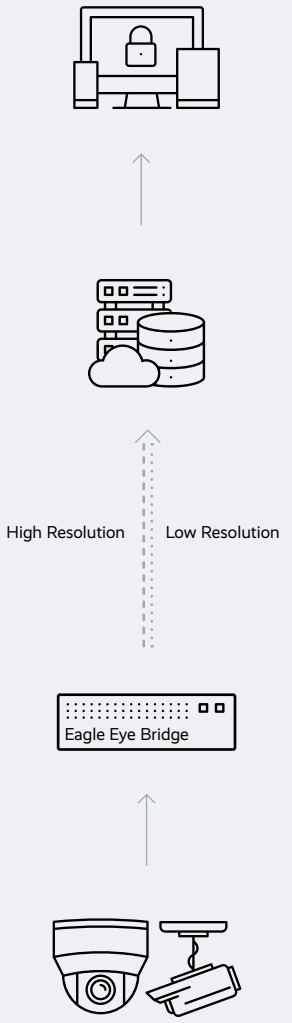

Figure 2. Eagle Eye Video Management System Architecture

The Eagle Eye Cloud VMS uses an on-premise appliance to establish a secure connection between the cameras and cloud; the Eagle Eye Bridge or the Eagle Eye Cloud Managed Video Recorder (CMVR). Eagle Eye Bridges and CMVRs transmit encrypted video and metadata to the Eagle Eye Cloud Data Centers while isolating cameras from the internet.

Video can be retained entirely in the cloud, entirely on-prem, or with a hybrid approach that combines both options. The Eagle Eye system is completely based on a modern redundant cloud architecture that provides both mobile and web browser-based interfaces.. **Figure 2** depicts the system architecture.

The Eagle Eye Cloud VMS replaces traditional DVRs and NVRs with a cyber-secure cloud-based solution:

Secure on-premise Eagle Eye Bridges/CMVRs:

- Eagle Eye Bridges, which buffer video and send it to the cloud, perform encryption, video data deduplication, bandwidth management, motion analysis, and video compression.
- Eagle Eye CMVRs, which perform all Bridge functions, plus record video locally and optionally send it to the cloud for hybrid retention.

Secure off-premise Eagle Eye data center equipment (the cloud):

- The Eagle Eye Video Platform and Video API Platform application servers, system data, and video data, are all located in the Eagle Eye Cloud Data Center.

EAGLE EYE BRIDGES/CMVRS

Eagle Eye Bridges and CMVRs connect cameras to the cloud VMS. These on-site appliances are designed as “locked down” devices and eliminate the weakness of a camera/internet connection by blocking inbound communications to the cameras.

Each Bridge/CMVR has at least two network ports: one for the camera network, and one for connecting to the internet. The Bridge/CMVR assigns a unique address using DHCP to each camera via its camera network-facing port; there is no way to access cameras directly from the internet, so camera password vulnerabilities cannot be exploited by internet-based botnet malware or manual remote hacking attempts. Similarly, cameras cannot reach out to connect to the internet.

Eagle Eye Bridges/CMVRs buffer video locally and send it to the Eagle Eye cloud using Eagle Eye Intelligent Bandwidth Management, which adjusts data transmission and bandwidth utilization dynamically, and prioritizes transmissions to optimally utilize the existing internet connection.

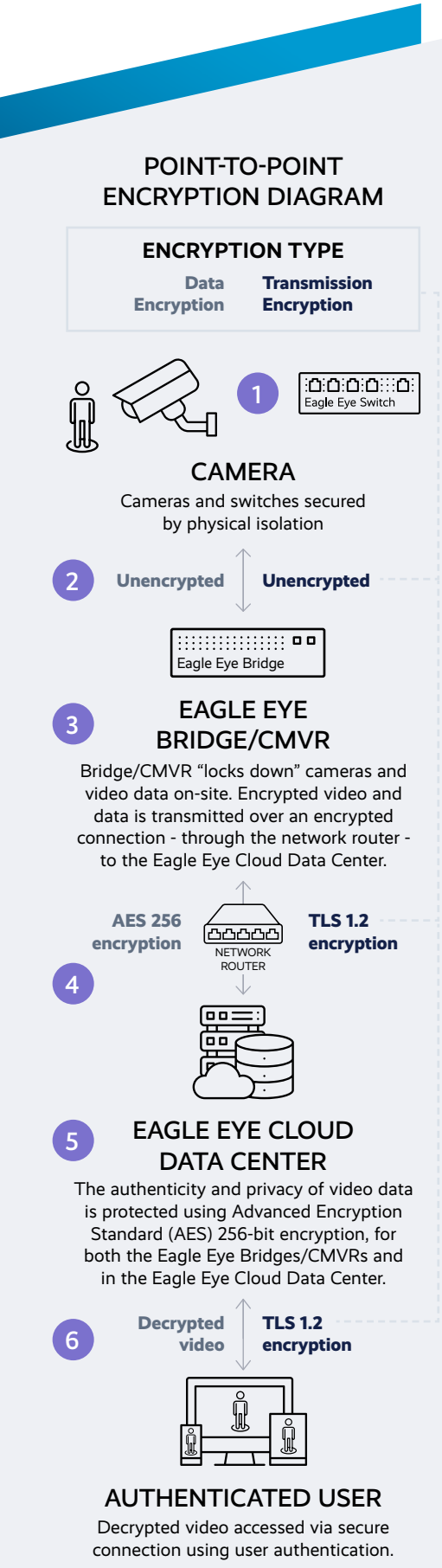

Figure 3. How Eagle Eye Networks Protects Customer Data

EAGLE EYE CLOUD DATA CENTER

At the center of the Eagle Eye Cloud Security Camera System is a set of highly secure data centers. These global data centers are collectively referred to as the Eagle Eye Cloud Data Center. Each customer's video and data is assigned to a data center closest to their region and stored in triple redundancy to reduce the likelihood of disruption or loss of recorded video.

Eagle Eye data center locations incorporate fault tolerance in components and connections. Redundancy in network connections and power supplies as well as in server hardware eliminates any single point of failure, maximizing hardware availability.

The Eagle Eye Cloud Data Center's multilayered approach to security ensures video data is not visible to the public. Customer data is encrypted at rest using a unique encryption key for each customer. Also, data centers are both logically and physically separate from the Eagle Eye corporate office network.

System Security: Encryption and Authentication

In addition to the physical security features already discussed, the Eagle Eye Cloud VMS uses multiple forms of encryption and authentication to ensure the highest levels of CIA. The VMS uses bank-level security to transmit video from the camera to the cloud and the cloud to the customer. The operating system, web server, and application software are continuously maintained and automatically updated with the safest available software, eliminating the need for manual security patches by a system technician or the customer.

Eagle Eye protects systems and data with authentication technologies that allow access for verified users and deny it to others. Eagle Eye also ensures a secure connection through two layers of encryption: one for the data itself, and another for the transmission of data from the Eagle Eye Bridge/CMVR to the Eagle Eye Cloud Data Center. Authenticated users can access decrypted video and data from the Cloud Data Center via a secure connection.

Figure 3 and **Figure 4** diagram and detail how both video data and data transmission channels are encrypted across the Eagle Eye VMS.

POINT-TO-POINT ENCRYPTION TABLE

DATA LOCATION	ENCRYPTION TYPE	
	Data encryption	Transmission encryption
1 Between camera and switch	Unencrypted, over physically isolated link	Unencrypted, over physically isolated link
2 Between switch and Eagle Eye Bridge/CMVR	Unencrypted, over physically isolated link	Unencrypted, over physically isolated link
3 Between Eagle Eye Bridge/CMVR and router	AES-256 encryption	TLS 1.2 (or higher)
4 Between router and data center	AES-256 encryption	TLS 1.2 (or higher)
5 On data center servers	AES-256 encryption	N/A
6 Between data center and end user	Unencrypted	TLS 1.2 (or higher)

Figure 4. Point-to-point encryption description

DATA TRANSMISSION SECURITY

The Eagle Eye Cloud Data Center servers use a digital certificate to establish a secure connection to each Eagle Eye Bridge/CMVR using Transport Layer Security (TLS) 1.2 or higher, thereby providing privacy and data integrity in three ways:

1. Authenticating the communicating applications using digital certificates.
2. Ensuring the connection is private by using strong data encryption.
3. Preventing alteration of the data during transmission with a message integrity check.

The Eagle Eye mobile app, web application, and APIs also utilize TLS version 1.2 or higher.

DATA ENCRYPTION

The privacy of video data is protected using Advanced Encryption Standard (AES) 256-bit encryption, the most secure encryption algorithm available, both on the Eagle Eye Bridges/CMVRs and in the Eagle Eye Cloud Data Center. AES-256 is the same level of encryption used in banking, government, and military applications.

Eagle Eye uses digital certificates, the equivalent of an electronic ID card, to authenticate users and provide access to their unencrypted video data.

A recognized third-party Certificate Authority (CA) manages the digital certificates to authenticate connections to the Eagle Eye Cloud VMS. This same CA is used and trusted by the major web browsers. For Eagle Eye Bridges/CMVRs, Eagle Eye issues its own certificates, because it can guarantee a trustworthy physical chain of custody during the installation of certificates into the appliances as part of the manufacturing process.

USER AUTHENTICATION

End users must be added to the system by an administrator before they are able to access the VMS. Administrators are either a designated person or persons within the account organization, or in some cases the security integrator/reseller will be the account administrator. Administrators specify each user's access to the system. Some of the user permissions include:

Ability to view live or recorded video	Ability to download video	Limits to what cameras or locations can be viewed
When a user can access the system by day or time	Authorization to change camera analytics and settings	Access to account settings or Audit Logs

Two available types of secure authentication protect users' access to the Eagle Eye Cloud VMS via mobile apps or web browser:

Multi-factor user authentication (MFA) - Eagle Eye offers MFA for all accounts to provide strong security by allowing system access only from trusted devices. A trusted device is a mobile device or a browser on a specific computer that has been previously authenticated using a phone number or email associated with that Eagle Eye user. The user receives a text or email verification code to authorize the device.

Single Sign On (SSO) - Using SSO, system administrators can easily add or revoke access to the Eagle Eye Cloud VMS via their Active Directory or LDAP to simplify access for authorized users. When a user logs into the SSO solution, the SSO checks the user's credentials in an identity management system and creates a digital certificate that verifies their identity. This digital certificate is stored either in the browser or the SSO's server, and checked by the application before granting the user access. SSO is available as part of the Professional and Enterprise Editions of the VMS.

Eagle Eye also offers IP whitelisting, which allows organizations to restrict camera and system access to approved networks. This feature is available as part of the Eagle Eye VMS Enterprise Edition.

CUSTOMER DATA PROTECTION

In addition to the security and privacy provided through advanced encryption, extra security measures ensure that video and data is protected and only available to authorized users. No customer has access to any other customer's system or data. By default Eagle Eye Networks does not have access to customer video, data, and system settings.

There is a mechanism for Eagle Eye Networks to gain access to account settings and video with appropriate permissions. This includes the combination of a required Support PIN and the optional Privacy Mode.

Support PIN: If a user calls our technical support department, the user must supply a personal identification number (PIN) available through that user's account profile. Every new user is assigned an initial Support PIN, and users can change the PIN at any time. The Support PIN authenticates the caller's credentials to stop cybercriminals posing as customers and also prevents unauthorized access to Eagle Eye employees. The Support PIN acts as a key to the front door of the user's account. Once inside, Eagle Eye can access customer settings, account logs, and cameras, but not necessarily the live or recorded video.

Privacy Mode: Privacy Mode creates another level of video security for customers. While the Support PIN is the front door to the account, Privacy Mode acts as the "light switch" to the video. If Privacy Mode is enabled, Eagle Eye employees do not have access to video. Privacy Mode is a standard feature

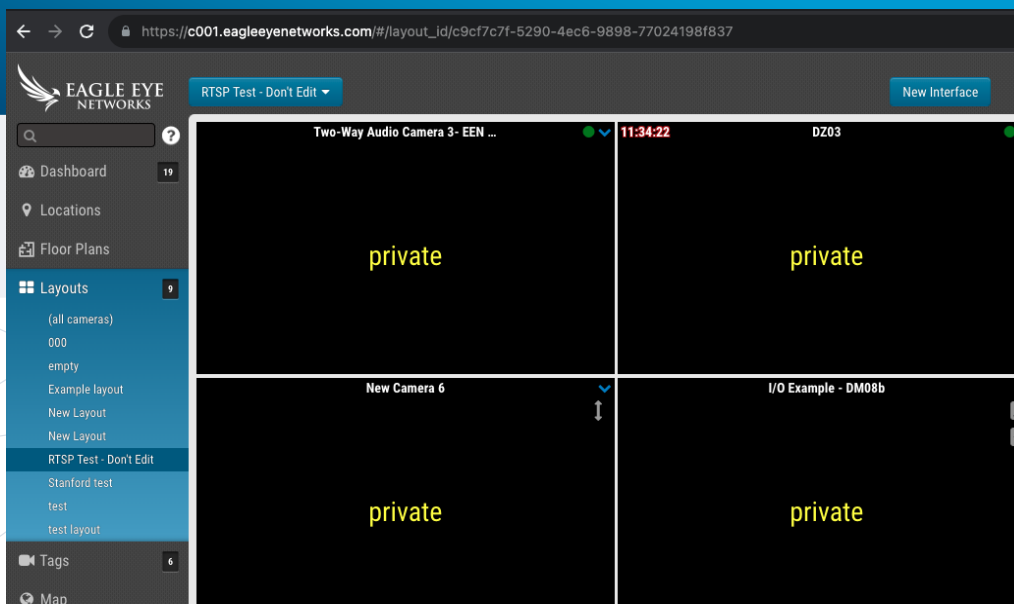

Figure 5. Eagle Eye Networks VMS dashboard with Privacy Mode enabled.

which allows Eagle Eye VMS users to block access to video streams, while still allowing necessary technical access. If video stream access is required (such as to verify a camera's exact field of view), Privacy Mode can be temporarily disabled by the user.

Audit Logs: To provide additional assurance, Audit Logs track every action in the VMS by end users, administrators, or Eagle Eye Networks personnel. Audit Logs are saved within the account for a year. Actions logged include:

- Login information
- Video views and downloads
- Setting changes

Conclusion

The Eagle Eye Networks Cloud VMS is a purpose-built cloud video surveillance solution designed to reduce the risk of cybersecurity vulnerabilities. Eagle Eye's continually managed subscription-based service provides automatic system security updates to achieve the highest levels of confidentiality, integrity, and availability for surveillance video.

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

- Designing and building a highly secure application based on modern redundant cloud architecture
- Developing a cyber-secure cloud-based Security Camera Video Management System with standards-based encryption of video data and transmission and strong authentication of users and mobile devices
- Manufacturing purpose-built secure video appliances that isolate cameras from internet cyber threats
- Managing and updating Eagle Eye appliance security and feature updates automatically, with no installer or end user action required

Summary of Technical Cybersecurity Measures

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

ON-PREMISE EQUIPMENT CYBERSECURITY

- Cameras are isolated from the Internet
- Appliances have no open inbound network ports
- Appliances are protected against pre-installed camera malware
- Appliances use TLS 1.2 connections to Eagle Eye Cloud Security Camera VMS
- AES-256 encryption is applied to buffered and locally recorded video
- Appliances are authenticated via digital certificates

DATA CENTER PHYSICAL SECURITY

- Facility intrusion detection and alarm system
- Biometric facility area access control
- 24/7 on-site live and recorded video monitoring
- Security desk visitor identity verification and visitor log

DATA CENTER NETWORK SECURITY

- Network address translation (NAT)
- Customer data encrypted at rest using unique encryption keys
- Logical and physical separation of data center environments from Eagle Eye corporate network

REDUNDANCY

- Eagle Eye Cloud Security Camera VMS components are redundant (either active/active or active/passive)
- Triple-redundant video data retention, power provision, and internet connectivity

APPLICATION AND DATA SECURITY

- Regular server vulnerability scanning
- Regular penetration testing
- API level security
- Multi-factor authentication for web and mobile access
- TLS 1.2 connections to Eagle Eye Cloud Security Camera VMS for web and mobile access
- AES-256 encryption of recorded video
- Multi-tenant data security controls

Eagle Eye's continually managed subscription-based service provides automatic system security updates to achieve the highest levels of confidentiality, integrity, and availability for surveillance video.

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 TM, 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."

LEARN MORE
Visit our website
EEN.COM

UNITED STATES
+1-512-473-0500
sales@een.com

LATIN AMERICA/CARIBBEAN
+52 55 8526 4926
LATAMsales@een.com

EUROPE
+31 20 26 10 460
EMEAsales@een.com

ASIA-PACIFIC
+81-3-6868-5527
APACsales@een.com