A Focus on Video Surveillance Cybersecurity

A MARCH NETWORKS WHITEPAPER

This whitepaper examines threats to IP video surveillance systems, the critical factors in cyber secure product and system design, and how March Networks solutions incorporate these features.

MARCH® networks

Table of Contents

Cybersecurity matters now more than ever

Constant vigilance is required

You want a video surveillance solution you can count on to provide security, prevent loss and improve operations. The question is, what if the solution you choose leaves you exposed to cybersecurity risks that can undermine those very benefits?

High-profile video surveillance breaches are becoming more commonplace.

In March 2021, for example, a hacker exposed photos and video from 150,000 connected security cameras on the Internet. The affected company, a California-based startup, reportedly gave multiple employees super administrator rights to its system, and the password was eventually posted online. The data breach impacted numerous businesses, as well as hospitals, prisons and others using the company's systems.

This is just one example of what can happen when cybersecurity is not taken seriously by a video surveillance provider. With so many Internet-connected devices in networks and so much personal and financial data flowing through systems, it's more vital than ever that your IP video surveillance solution is secure. Both smart product choices and constant vigilance are required.

But what does that look like and how can it be achieved?

Cybersecurity is more than the sum of its parts

Cybersecurity is not just an IT challenge. There is no single off-the-shelf product that can guarantee it. Instead, cybersecurity must be integrated into all aspects of your security solution and practices. It must be taken into account when selecting hardware, like IP cameras and network video recorders (NVRs), as well as software, including video management software (VMS), client software and enterprise management services. You also need to consider things like protocols, procedures and dedicated support resources.

To ensure strong end-to-end cybersecurity, each individual element of your surveillance solution must be strong. It's not only prudent, it's operationally imperative that you choose technology you can trust and manufacturers with a track record of investing in cybersecurity and data protection measures. Both should be backed up by cybersecurity best practices and ongoing support.

What can happen if your security is breached?

As seen in the example above, the potential fallout from a serious data breach can be devastating. While the final bill may take years to calculate, the costs of exposing highly sensitive data and video on the Internet can quickly reach numbers that can cripple large operations — and shutter smaller ones.

Data breaches can result not only in direct financial losses – millions or even billions – but also losses to reputation, consumer confidence and goodwill. If your system is compromised, you could also lose access to video evidence when you need it most. The stakes are high, and it underscores the critical importance of choosing cyber secure video technology.

Threats to video surveillance cybersecurity

Networks come with vulnerabilities

Because data is collected, stored and communicated between devices, clients and services, IP video surveillance systems can have the same potential vulnerabilities as other systems deployed over networks. This data can include video, and in the case of integrated surveillance systems, sensitive personal and financial information such as point-of-sale (POS) and ATM transaction data, as well as GPS, alarm panel data and analytics. Storing and moving this data around presents risks.

Of course, there are many ways to mitigate these risks using technology and best-practices — but there is often a trade-off between security, cost and functionality. The trick is finding the right balance for your organization.

The most common attack strategies

There are many ways a hacker could gain access to your IP video system. Some of these include:

Hijacking access

Password attacks

The simplest way of gaining entry into an IP video system is by exploiting device or client log-in functions.

In password attacks, a threat actor attempts to log into a user's account by figuring out the required credentials. This can involve taking advantage of default passwords that are never reset or phishing attacks to trick users into providing credentials. Or, it can be a brute-force attack which, as the name suggests, attempts to overwhelm your system by systematically trying out password combinations until the right one is eventually identified. This can compromise the confidentiality of data.

Network spoofing

Network spoofing is when a device emulates or "spoofs" a trusted device in your network. Essentially, a malicious computer can pretend to be a camera or NVR in order to gain access to, alter or destroy video and data assets within the network. This can compromise the integrity of data or video evidence.

Intercepting or altering data

Eavesdropping attacks

Eavesdropping (also called network sniffing) is when a threat actor intercepts communications between two devices or systems within the network, between camera and recorder or recorder and client for instance. It can be used to gain access to any data while it is in transit — including video and potentially sensitive financial or personal information. Eavesdropping is hard to detect and can compromise the confidentiality of data.

Man-in-the-middle attacks

A man-in-the-middle attack is a more sophisticated version of eavesdropping in which the threat actor is able to not only intercept, but alter communications during transmission between two parties within a network. The "man-in-the-middle" is able to modify messages or content, hide malicious activity, or further compromise the network by injecting malware — all without being visible to those communicating. The two parties are likely to trust that nothing is out of the ordinary. This poses a serious threat to the integrity of data and video evidence.

Systems attacks

Denial-of-service

Denial-of-service attacks attempt to render IP video surveillance systems ineffective by flooding them with traffic in order to overwhelm network resources or crash the system. At that point, the solution can no longer function as it was intended and physical security can be compromised or other network attacks can slip through.

When multiple compromised devices are used, it is known as a distributed denial-of-service (DDoS) attack.

Malware

Malware (malevolent software) is created by threat actors to damage networks and make systems inoperable. Once deployed, malicious code can replicate and spread quickly across a network — causing chaos while remaining largely undetectable. Malware comes in many forms including spyware, which can access and transmit data, and ransomware, which can cut off access to parts of the network unless the victim pays a ransom to retrieve their data.

Your biggest threat is still human error

Apart from an insider willfully sabotaging your security, the single biggest internal threat to your organization is simple human nature.

Apart from an insider willfully sabotaging your security, the single biggest internal threat to your organization is simple human nature. People can forget to strictly adhere to cybersecurity best practices. People can neglect to create and update strong passwords. People can insert an unverified USB key into your devices and unknowingly install malware or open you up for external attack.

The most common mistake is failing to change default passwords shipped with off-the-shelf devices. Default log-in information can often be found with a simple Internet search, giving threat actors access to use your own devices to, for example, conduct denial-of-service attacks.

This is exactly what happened in a 2016 attack that temporarily disrupted a number of major websites including Twitter, Spotify and the New York Times. Hackers used what we now know as the Mirai botnet to attack a major DNS host. They were able to coordinate the DDoS attack by using the default passwords on unsecure DVRs and IP cameras.

So, what can you do to protect against external and internal threats?

Safeguarding your system with encryption

The three pillars of digital information security

There are three characteristics that an effective IP video solution should have measures in place to address:

Confidentiality

Confidentiality means your video and data has not been seen or accessed by parties who are not authorized to do so. You have safeguards to prevent those without permission from gaining access — and they are working as intended.

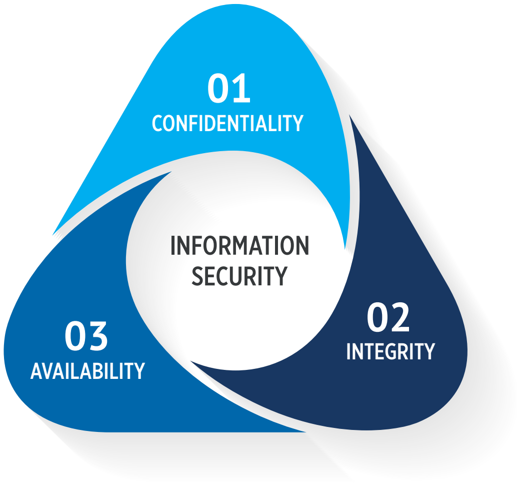
Integrity and non-repudiation

The fundamental principles of information security are confidentiality, integrity, and availability.

Integrity means your video and data can be trusted because you can guarantee it has not been altered in anyway. Non-repudiation means that you cannot deny that something was sent or received — or by whom — and it helps ensure integrity. This is important for video exported to files, which is often essential evidence for legal proceedings. Solid integrity ensures evidence cannot be discredited for the purposes of assigning guilt or awarding damages.

Availability

This means that your video and data, and the systems that store and communicate them, are always accessible and available when you need them. To ensure availability, video surveillance systems need to feature high resiliency, redundancy in case of failure, and tolerance to denial of service attacks.



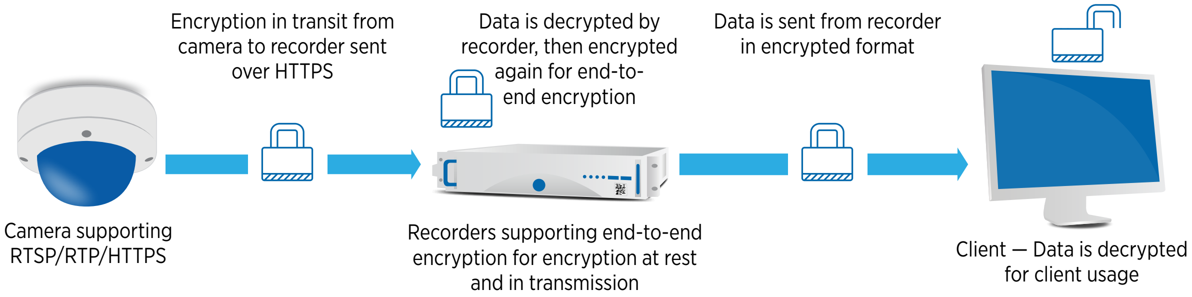
Encryption is a critical component of cybersecurity

Encryption can help ensure the confidentiality and integrity of your video and data remains intact.

Encryption uses algorithms to scramble or obscure your video and data so that it cannot be seen or used by attackers — even if they manage to breach your cybersecurity measures and gain access to them. Encrypted data cannot be decoded without the corresponding decryption key, which contains the information required for decryption. Encryption can protect data intercepted in eavesdropping and man-in-the-middle attacks. Depending where in the system encryption and decryption take place, it can also protect data accessed through password attacks, network spoofing and spyware.

It is an important component in protecting your sensitive data, but encryption is most effective if the data is encrypted at the point where it is actually created, and decrypted where it is actually used — implementing what is formally known as end-to-end encryption. Conversely, systems with multiple decryption and encryption operations across the pipeline presents weak points that can be exploited by hackers.

End-to-end encryption


Encryption in transit from camera to recorder sent over HTTPS
Data is decrypted by recorder, then encrypted again for end-to-end encryption
Data is sent from recorder in encrypted format
Camera supporting RTSP/RTP/HTTPS
Recorders supporting end-to-end encryption for encryption at rest and in transmission
Client — Data is decrypted for client usage

Network protocols and encryption

Network protocols play an important role in video surveillance cybersecurity. As technology has evolved, protocols have become layered in increasingly complex combinations to provide higher levels of functionality and security. What follows is a simplified explanation of the key protocols for each layer.

The network layer: IP, TCP and UDP

Let's start with the simplest and most fundamental network protocol: Internet Protocol (IP). IP models data as packets and establishes a set of rules for addressing and routing these packets. Each packet is "addressed" with IP information to help routers send packets across networks, have them arrive at the right place, and be configured properly when they get there. IP does not provide security or ensure the confidentiality or integrity of data, but does provide a foundation for IP video surveillance networks.

How March Networks protects you

March Networks' next-generation recorders offer end-to-end encryption, from the media received from cameras to the clients connected to our enterprise management system. In addition, they support cameras sending RTP/RTSP over HTTPS — a function March Networks' latest generation of IP cameras support.

March Networks fully leverages HTTPS for communications across all clients and services, supporting TLS 1.2 and ciphers that provide forward secrecy and strong keys. This combination delivers the same security and capability of TLS 1.3.

On top of this, we also support WebRTC and DTLS 1.2, enabling secure remote access to devices and services, from any deployment site, to any client location.

When it comes to streaming video over a network, the most commonly used implementations of IP are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). TCP is a little slower but more reliable because individual packets are delivered, verified and assembled in sequence. This makes TCP more suitable for one-to-one (unicast) communications. UDP is faster, with multiple packets that can be delivered simultaneously, so it may also be used for one-to-many (multicast) communications.

Neither TCP nor UDP provide security or encryption.

The security layer: TLS and DTLS

Transport Layer Security (TLS) is the standard used to encrypt any TCP communication. Different versions of it exist, with each iteration designed to enhance security and extend capability. TLS 1.0 was established in 1999, followed by TLS 1.1 in 2006. TLS 1.2 was defined in 2008, adding support for AES 256 encryption. This version is widely considered the industry standard for today's deployed IP video surveillance solutions. The latest version, TLS 1.3, was defined in 2018 but is not yet well-supported in the field.

The Datagram Transport Layer Security (DTLS) is a protocol based on TLS concepts, and is intended to provide similar security guarantees for UDP multicast applications.

Forward secrecy

Forward secrecy is a characteristic of some TLS ciphers that protects past encrypted communications, even if encryption keys are compromised at some later point. In many cases, forward secrecy limits the amount of information a threat actor is able to access. Even if an attack is successful, only information intercepted from that point forward could be decrypted.

The application layer: HTTP and HTTPS

HyperText Transfer Protocol (HTTP) is a client-server protocol that enables web applications to transfer content when requested by a recipient. It is layered on top of TCP for one-to-one communications, providing the foundation of any data exchange on the Internet, which is why you see HTTP in website URLs. However, HTTP alone does not guarantee the security of that exchange.

Hypertext Transfer Protocol Secure (HTTPS) uses TLS to encrypt data and create a security layer wrapped around an HTTP connection.

In IP video surveillance solutions, HTTPS is used to provide secure network connections between cameras, recorders and clients. While HTTPS is widely used for configuration functions, many devices still manage media using HTTP, due to the computing power needed to encrypt it. This makes the video they capture far less secure in transport.

The real-time streaming layer: RTSP/RTP and WebRTC

Real-time Transmission Protocol (RTP), is a protocol designed to stream media in real-time, from one-to-one or one-to-many connections, across different transport layers (UDP, TCP, HTTP, HTTPS). Think of a birthcam set up at a zoo, allowing anyone who is interested to see a livestream of an anticipated event.

Real-Time Streaming Protocol (RTSP) combines with RTP to include authentication and the concept of streaming sessions. In IP video surveillance solutions, RTSP can be used to stream multiple camera feeds to a public view monitor, like you might see overhead as you walk into a gas station or convenience store.

RTSP/RTP is great for local network usage, but is not ideal for transmitting surveillance video across the Internet. Another protocol, the Web Real-Time Communication (WebRTC), was designed for this. WebRTC uses several other protocols in parallel, to offer real-time media streaming for web applications, while at the same time allowing data to travel across firewalls from private to public networks. You might need this if you wanted to access your business's security cameras while working remotely. Most WebRTC traffic uses RTP and DTLS, while adding encryption to RTP using the Secure Real-time Transmission Protocol (SRTP).

Limiting vulnerabilities with the right OS

The advantages of a Linux-based OS

The truth is, any operating system can potentially be exploited given the right opportunity. The trick is in limiting those opportunities. We believe that a well configured Linux-based OS is inherently more secure than a Windows-based OS, particularly when it has been customized for – and embedded in – a video surveillance recording appliance.

There are several characteristics that help back this claim up:

Smaller target

Windows enjoys a very healthy market share. The sheer number of deployed systems makes Microsoft a much larger and more lucrative target for attackers. As a result, Linux-based systems are far less likely to be the focus of third-party attacks in the first place. It's a numbers game, and it's the same reason Macs were less likely than PCs to be targeted for so long.

Customization

With a customized Linux OS, March Networks can strip out everything our embedded devices and software services don't need. We can remove unnecessary components like file sharing services and desktop applications while locking down or removing non-essential network ports. Both of these hardening actions, along with the corresponding reduction in total volume of code, help to limit vulnerabilities and the likelihood of attack — as well as improve overall system performance and reliability.

The Linux-based Operating Systems (OS) in March Networks' NVRs are customized to help safeguard against vulnerabilities by removing unnecessary services and applications and locking all non-essential network ports, reducing the likelihood of attack. The customized OS also has a reduced volume of code that helps optimize overall system performance and minimize defects.

Tighter control

A customized Linux-based OS provides more direct control over what enters our systems. Our embedded recording devices don't need to interact with updates from third parties. Any direct access to devices is blocked and there are no default users enabled. If remote access for maintenance is needed, the process is managed by March Networks' technical support team, who can generate a one-time password (OTP). March Networks strictly limits and regularly audits who uses OTPs and when. Additionally, OTPs are never used without prior consent from our customers.

In addition, our Linux-based server bundles use commercial distributions that are configured to minimize exposed services and to leverage security measures like Secure Boot, which further harden the security of the system.

All of this makes it more difficult for malicious software to gain access to March Networks' Linux-based recording solutions.

Minimizing cybersecurity risks with security features and best practices

Control access to your system

Limiting who can access your system and what they can do once they are in is critical to cybersecurity. There are a number of ways this can be facilitated:

Password protection and management

A surprising number of breaches can be attributed to shared, stolen or guessed passwords. You should avoid IP cameras and NVRs with fixed or hard-coded passwords. Instead, there should be a mechanism for creating a unique password. You should look for solutions that require, or strongly encourage, password protection. Ideally, there is a simple way to enable password management so you can mandate requirements such as length, complexity and how often they must be changed.

User role management

Clearly defined user rights and privileges are an important part of the overall cybersecurity story. You should look for a solution that offers tight controls over user profiles and restrictions. This can help ensure that new employees or third-parties only have access to what they need to do their jobs — instead of the entire system.

This type of control mitigates the damage that can be caused by breaches to accounts with too many privileges, where one person may have unrestricted access to an entire system.

Look for built-in auditing, anti-tampering and security alerts functions

These capabilities can help ensure the security of your video surveillance system by alerting you in real-time to potential threats:

Auditing

No system is 100% secure, so you need to be able to determine not only when a change has been made on the system, but who made that change, and what exactly was changed. Ideally, your solution will capture a log of this information that your system adminstrator can audit when needed. This would enable you to verify, for example, who exported video from a specific recorder, and when.

How March Networks protects you

Our latest generation of embedded recorders and IP cameras are designed to force users to provision a password at initial set up. This prevents attackers from accessing your system using generic user credentials that can be found online.

March Networks enterprise management solutions have built-in user management capabilities. We enable sophisticated user management that allows administrators to get very granular in how to limit user access. You can, for instance, allow a new hire access to only a few specific cameras, or limit regional managers to viewing video only within their specific territory.

March Networks does not have a Super User or Super Admin role that could allow a single user access to all of our customer's systems. Individual on-premises March Networks products that have this role give access only to a single instance of the product, and the role is completely owned by the customer, not by March Networks.

March Networks provides peace of mind

To enable audits, March Networks' enterprise management system captures robust data on who accesses the system, what changes are made and when.

March Networks also has a dedicated file format (.cme) that allows customers to export video with encryption, with a strong key generated from a password seed. Video, as well as alarms and integrated data from POS receipts and ATM printouts, can all be exported to .cme format. Once in the .cme format, these files can only be viewed by someone with the associated video player.

The player decrypts and plays back the file, and also validates a seal that detects if the data was tampered with in any way.

In addition to the .cme format, March Networks also offers a secure cloud-based platform for sharing video evidence. Video evidence and case files can be exported directly to the cloud and shared only with those given permission to access them.

Finally, March Networks recording solutions have built-in security alerts that detect and notify you in the event of unusual activity. Alerts can be configured to trigger upon a series of failed login attempts, or in the case of a potential DDoS attack.

Anti-tampering

Tampering can make your video or data worthless during legal proceedings. You need a solution with built in anti-tampering features to control access and ensure exported evidence remains unimpeachable. This can include a dedicated video file format with a dedicated player, an export process protected with encryption, and a way to validate that exported information has not been tampered with in any way — at any point in the evidenciary chain.

Security and health alerts

You also need to be notified right away when something out of the ordinary occurs. You want a solution that provides real-time security alerts in the event of any suspicious activity. Multiple failed login attempts, for instance, may indicate a brute-force attack. Or, if an NVR is not functioning properly, it may be the target of a denial-of-service attack. Look for a system with robust security and health monitoring features, as this too can also alert you to device issues in real-time.

Maintain secure infrastructure and connections

There are a variety of other security features you can look for to ensure the integrity of your network and connections:

Integration with corporate systems

Given the value of data and video assets, you want your IP video surveillance solution to be able to benefit from as many protections as possible. Chances are, your organization has already put significant resources into safeguarding data — you want your solution to be able to seamlessly work with and benefit from any overarching security measures already in place on the corporate network.

Secure network access

In addition to the network protocols described above, you can control device and client access by requiring authentication at the network port level. 802.1x is the accepted industry standard for port-based network access control (PNAC). When used, it means a device can't connect to the network until an 802.1x authentication server gives it access. In this way, you can eliminate rogue devices from connecting to your secure network and protect from spoofing attacks.

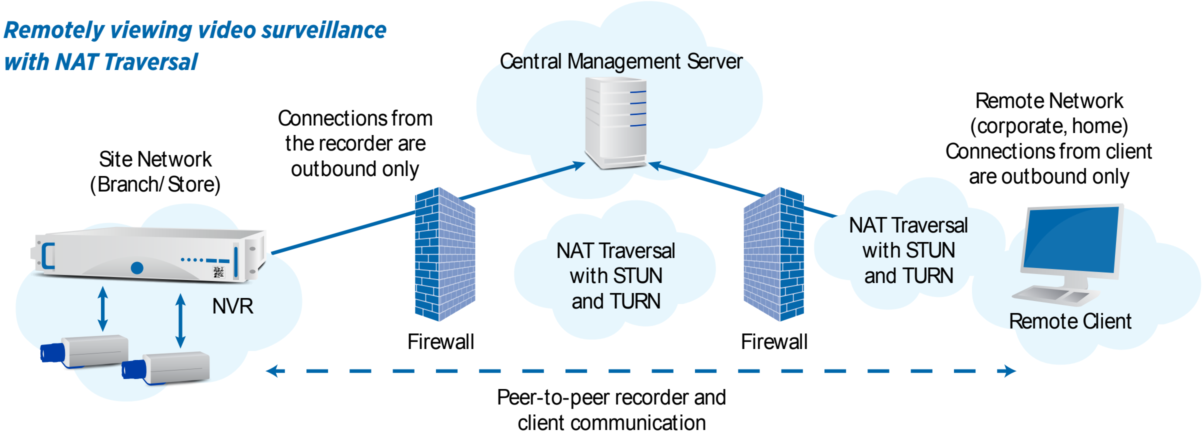
Secure remote access

If you need to view video while you are off premises and operating outside of your secure network's firewall, you will need a way of communicating across the firewall and network address translators (NAT). The most common method is to leave some ports open and configure port forwarding between external and internal addresses. The problem is, these open ports can be exploited by attackers and malware.

For more secure remote access to your video, you need a way of crossing your firewall and NAT without punching holes in them. A secure NAT traversal mechanism will instead be needed to preserve the IP addresses of devices in your network invisible to the public.

WebRTC leveraging Session Traversal Utilities for NAT (STUN) and Traversal Using Relay around NAT (TURN) allows for the creation of peer-to-peer communications, facilitating secure and encrypted connections without the need to compromise firewalls and NAT. The result allows for more secure remote viewing of video surveillance.

Remotely viewing video surveillance with NAT Traversal


Central Management Server
Connections from the recorder are outbound only
Remote Network (corporate, home) Connections from client are outbound only
Site Network (Branch/ Store)
NAT Traversal with STUN and TURN
NAT Traversal with STUN and TURN
NVR
Firewall
Firewall
Remote Client
Peer-to-peer recorder and client communication

March Networks helps ensure network security

Our systems can be fully integrated with LDAP and Microsoft Active Directory, so you can inherit, comply with and take full advantage of overarching corporate security measures.

March Networks recorders and cameras support 802.1x, so you can enable network port device authentication using an 802.1x authentication server.

March Networks uses WebRTC to provide NAT traversal for secure remote viewing. This method allows users with dedicated access rights to initiate encrypted communications between recorders and remote clients. Our enterprise management service coordinates the communication, leveraging standard STUN and TURN services.

Ensure your video manufacturer provides ongoing support

Because cyber threats are constantly evolving, it's important to look for a video surveillance manufacturer that continually evaluates threats and has clear processes in place to safeguard its products and protect its customers.

Here are some supports that March Networks offers our customers and partners that you may want to consider when choosing a provider:

A proven track record

For over 20 years, March Networks has delivered secure video surveillance solutions to customers, including leading banks and credit unions, who demand the highest cybersecurity standards. We have a team of R&D professionals dedicated to ensuring we continue to meet and exceed those standards. Additionally, all March Networks employees undergo annual cybersecurity training to ensure everyone is following best practices at all times.

Scanning for evolving threats

You need a video surveillance provider that constantly monitors for vulnerabilities, assesses how they may affect you, and provides fixes as soon as possible. March Networks' Security Updates and Advisories Program provides these functions on an ongoing basis. Information is posted on the March Networks website and subscribers are notified by email about important cybersecurity updates impacting our products. Software patches are made available on our Partner Portal.

Constant testing and evaluation

March Networks is trusted by Fortune 500 companies who demand nothing less than the best. We are constantly evaluating our security practices, and regularly undergoing security audits that analyze our business policies and practices. All March Networks recorders and cameras pass stringent cybersecurity testing including ethical hacks and independent third-party penetration testing to further confirm security integrity, assess potential cyber weaknesses, and help us resolve them.

Innovative security tools

March Networks certified partners can use our innovative GURU Smartphone App, an industry-first tool that was designed specifically for supporting the installation and maintenance of March Networks products. The GURU app's Security Audit feature can assess how secure the configuration of installed March Networks recorders are against a list of potential weaknesses. It can then provide a list of recommendations on ways to harden the system.

The final word

Cybersecurity is an increasingly important consideration when choosing an IP video surveillance solution — and there really are no shortcuts.

Maintaining a secure system takes a commitment from everyone involved. From the manufacturer to the integrator to the end-user organization, everyone needs to take an active role. It takes a coordinated and sustained effort, but.as we've seen, it's well worth the investment.

If you're looking to partner with a video surveillance manufacturer that is committed to cybersecurity, March Networks can help. Use our video surveillance cybersecurity checklist to evaluate your preferred solution or contact us online.

www.marchnetworks.com/products-services/video-surveillance-cybersecurity/

IP video surveillance solution cybersecurity checklist

Use this list as a guide to evaluate the cybersecurity of an IP video surveillance solution. This list is not intended to be exhaustive, but it can help you determine if a solution delivers key cybersecurity protections.

Network Protocols and Encryption

- ☐ End-to-end encryption
- ☐ Secure network connections over HTTPS
- ☐ Supports TLS 1.2 or higher
- ☐ Forward secrecy support
- ☐ Cameras and recorders support 802.1x authentication
- ☐ WebRTC for remote viewing

Operating System

- ☐ Customized OS removing unnecessary services and apps
- ☐ Linux-based for smaller attack target

Access and Alerts

- ☐ Strong password security and management
- ☐ No fixed or backdoor passwords
- ☐ LDAP/Microsoft Active Directory integration for streamlined corporate security
- ☐ Enables strict and granular controls over user access
- ☐ Enables auditing of all user activities on the system
- ☐ Has anti-tampering features, ensuring the integrity of video evidence
- ☐ Offers security alerts on suspicious system activity (i.e. multiple failed logins)

Manufacturer Support

- ☐ Has a dedicated cybersecurity team
- ☐ Scans for emerging cyber threats and communicates them to customers
- ☐ Runs regular penetration testing on products
- ☐ Provides hardening guides for products
- ☐ Provides patches and ongoing support
- ☐ Employees undergo regular cybersecurity training

North America	1 800 563 5564
Latin America	+5255 5259 9511
Europe	+39 0362 17935
Asia	+65 6818 0963
Australia and New Zealand	+61 1300 089 419
Middle East and Africa	+971 4 399 5525

marchnetworks.com