CHECKVIDEO

ENTERPRISE VIDEO SOLUTIONS

INTRODUCTION

The past decade has seen a shift from older analog cameras, to networked IP cameras, recorders and servers. While the promise of IP was to deliver flexibility in being able to view video remotely and manage it centrally, in practical enterprise installations, that has come at the expense of increased cyber-security risk. In many cases, physical security or facilities teams have procured IP video solutions and IT teams have been tasked after-the-fact with configuring, administering and securing these devices on their networks.

Fortunately, with increased awareness, enterprises are beginning to implement policies and procedures, and creating standards for video camera deployment. However, most enterprises do not have the luxury of starting from scratch given the significant capital expenditure. Therefore, IT leaders face the challenge of securing their existing camera footprint and keeping it protected against known and future threats.

We look at some common themes and strategies adopted by enterprises looking to secure and centrally manage a vast footprint. Many of these are inspired by or extensions of policies used to secure network endpoints such as printers and IP phones. Additionally, there are mature practices to secure servers and desktops and centrally enforce policies, which are applicable to a video rollout. With the number of cameras sometimes approaching the number of desktops across the enterprise, this is a formidable challenge.

DISTRIBUTED LOCATIONS

Video cameras for many enterprises easily include hundreds or even thousands of sites. A common approach is to have the video, security or facility network segregated from the corporate network at each site. In many cases, this security network is isolated and limited to the site alone. This means that access to cameras is only available from single-purpose viewing stations or PCs on site. This is no different from older on-premise analog solutions, which required physical access to the CCTV system to view live video or conduct investigations. While such a premise-only segregated network means lower risk, it fails to deliver on the promise of flexibility with IP for off-site access.

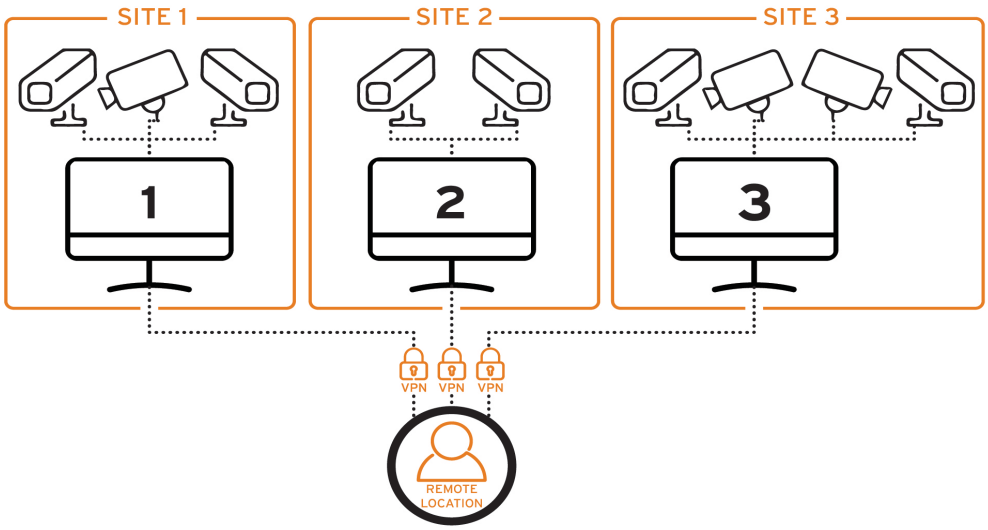
Another challenge with a premise-only solution is the expense of managing it for configuration changes, updates, and health monitoring, all of which cannot be done centrally. This places a large burden on the local IT resource, if available, at each site to keep the system going. It is no surprise that many of these systems are therefore in various states of disrepair.

A step towards remote management is possible by creating VPN connections to the security network at each site and strictly managing administrative access. This does require a VPN endpoint specifically designated for this purpose. It also raises policy questions around who should be authorized to remote into the site over VPN.

Should facilities managers be able to remote it over VPN to view the video? Should there be a separate Internet circuit? Would each user require client software to be installed for VPN and CCTV? How would one limit the scope of which sites, server and/ or cameras such a user could see? How would one enforce a policy for regional managers to view multiple sites, but each site manager to only have access to their site? What may have started off as a remote management tool for IT, rapidly changes to a much larger resource and support challenge.

These challenges have led some organizations to consider a flat, segregated, yet routable security network across sites. Clearly, this requires additional equipment or reconfiguration of existing equipment, both for switching and routing at each site. Given how legacy system is set up, it often means such changes have to be done on site. While well-intentioned, such a change can take years and require significant capital outlays.

This calls for a managed, virtual flat network which can be rapidly deployed with existing segregated on-premise systems. CheckVideo provides such an overlay network-as-a-service which can be deployed simply using a cost-effective gateway device.



HARDWARE VARIATIONS

While every enterprise strives to standardize on a common platform, it is common to have a handful of platforms, and separate models of hardware within each vendor platform. Even if an enterprise were to start with a single platform, business needs as well as acquisitions mean multiple vendor's products are generally deployed across the enterprise. Interoperability of IP cameras with recorders is better than ever with vendor support for standards such as H.264, RTSP and ONVIF.

These standards enable video to be streamed, viewed and recorded across vendors. However, configuration interfaces, support for network protocols, operating systems, web servers, databases and application stacks vary widely across vendors. Such variations are common even among different products or products families from thesame vendor in that the same software or firmware do not work across substantially all of the vendor's products.

Such variability in products as well as software/ firmware stacks does not lend itself to an enterprise standard. With video cameras and recorders being distributed across sites, it is not unusual for an enterprise to not be aware of the number of devices, their software version and patch status.

A splintered platform further complicates usage of the CCTV system across the enterprise because users may need to use different versions of client software as they look at cameras from sites having different platforms or models of NVRs.

One way to mitigate the fragmentation of the platform is the use of federation servers to standardize directory services and recorders. In a federated model, cameras can be heterogenous as long as they support a standard for video streaming. Video Management System (VMS) software is installed on a server at each site, which performs recording functions and maintains a directory of cameras and users. In order to enroll multiple sites and configure/manage them centrally, a federation server is added and on-premise recorders and directories are enrolled in the federation.

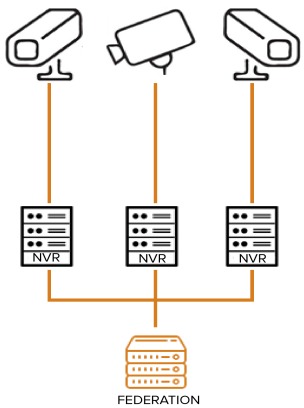
A user or client software logs into the federation server which then does the lookup to the appropriate on-premise recorder.

Migrating to a new VMS can be expensive because hardware, software and servers are required. It also has a scaling challenge in that a federation server can only support a finite number of sites. Of course, additional federation servers can be added and a hierarchy of federation built up, which consumes ever more resources.

Again, the use of virtual machines alleviates some of the concern regarding additional servers. However, video loads work best on native hardware because they exploit the Graphics Processing Unit (GPU), and some efficiency is lost in a virtual environment.

Today, managed services and platform-as-a- service models are being adopted by enterprises for everything from email, Office, CRM and even firewalls. Managed service providers specialize in their application stack, ensuring uptime and cyber-security and delivering a high-availability solution while dramatically cutting down on IT resources required by roll-your-own solutions.

CheckVideo offers a managed VMS, which is fully federated and infinitely scalable. It does not require any software provisioning and is able to harmonize disparate hardware at multiple sites, enabling centralized management, health monitoring, patch management and user access though an enterprise policy.



SECURING THE NETWORK LAYER

The explosive growth of Internet connected devices and the Internet of Things (IOT) revolution hascreated additional vulnerabilities which are prone to attacks by hackers. Owing to competitive pressure, multiple camera vendors source their cameras, and more importantly, the firmware for their camera from a handful of large OEM vendors in China. Unfortunately, these firmware stacks leave vulnerabilities and backdoors exposed and run versions of software with known exploits. These shortcomings have been exploited by hackers that used botnets such as Mirai to stage massive distributed denial of service (DDoS) attacks.

In reaction to this, some progressive vendors have started publishing guidelines and best practices to secure their cameras against attack. Several also provide patches and firmware upgrades as vulnerabilities are discovered. While these efforts are laudable, it creates additional burden for theenterprise IT team to watch out for new firmware version and apply patches when they become available. There is also a lack of SLAs and strict timelines from vendors to ensure timely patches are published.

As IT teams continue to be under siege, it makes sense to contain and block nefarious agents from taking control of cameras or from exploiting thenetwork.
The most common approach is to isolate the security network as described earlier, but that limits access to video and does not facilitate centralized management.

Additional measures can be adopted at the network layer such as static IP addresses and MAC address reservation to ensure other third-party devices cannot inadvertently be plugged into the security network. UPnP and broadcast must be disabled on the network. Some network administrators go a step further and disable multicast and IGMP, which has the adverse effect of making ONVIF discovery impossible. Another common practice is the use of VLANs for cameras. Stricter measures such as encrypted communications from cameras using certificates and port-level MAC filtering can also be employed. Lastly, whitelisting servers and/or disabling out bound access to services on Internet such as P2P and DDNS can also ensure that any malware on the camera iscontained.

Today's IP cameras, NVRs and VMS servers advertise a host of network services and listen on a number of ports. While this is meant to appeal to the broadest audience for every use case, it presents a big and ever changing threat keeping network administrators on their toes.

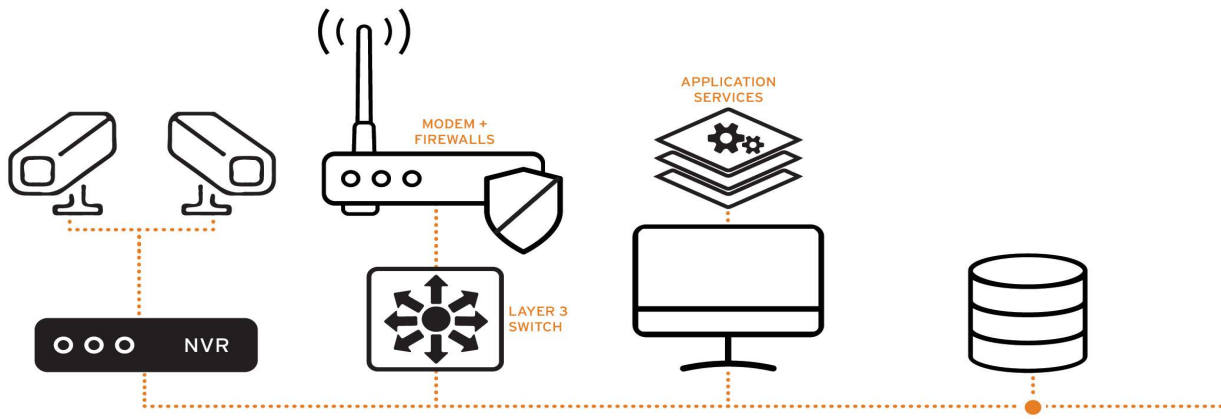
A managed approach with CheckVideo gateways isolates and contains IP cameras. The CheckVideo gateway advertises no services and all ports are locked down with an internal firewall, which can be supplemented with additional MAC filtering and reservations to ensure the highest level of network security. Even better, since the gateway is managed through the VMS, there is no web server, logins or passwords to secure and rotate for on-premise devices. They only way to access and configure the device is to be authenticated through the managed VMS, which then passes down all configuration to on-premise devices over an encrypted (TLS 1.2) connection.

THE OS & APPLICATION STACK

Hardware fragmentation can mostly be addressed by using an enterprise VMS. The VMS is a complex set of interacting software components such as the Operating System (OS), multiple Databases (DB), services and daemons, web servers, recorders and plugins.

While it is possible to standardize on a OS version with the correct update/patch level, the application services and software need to be compatible with changes to the OS, database and web server. While it is good practice to qualify application software on an OS and web server version, such standardization is difficult to keep up over an extended period of time. VMS software vendors do not qualify their software on every permutation of OS/DB/web server release chosen by enterprises. This creates a burden on the enterprise IT team to test and qualify the entire stack. With the amount of effort such qualification requires, and the ever moving target of OS patches that continue to roll out, it is virtually impossible for enterprises to keep up. This results in enterprises continuing to deploy possibly outdated version of OS,possibly with known vulnerabilities, or possibly having a fragmented and functionally incompatiblesystem as some but not all parts of the VMS stack are updated.

A managed VMS changes this by placing the onus for applying patches, and certifying that these work with the application stack on theVMS provider. CheckVideo automatically pushes out full updates including OS, DB, application stacks, etc, and provides a SLA for critical security patches. These updated stacks are subjected to vulnerability scans as well as penetration testing, and customized testing and certification per customer needs and standards available.

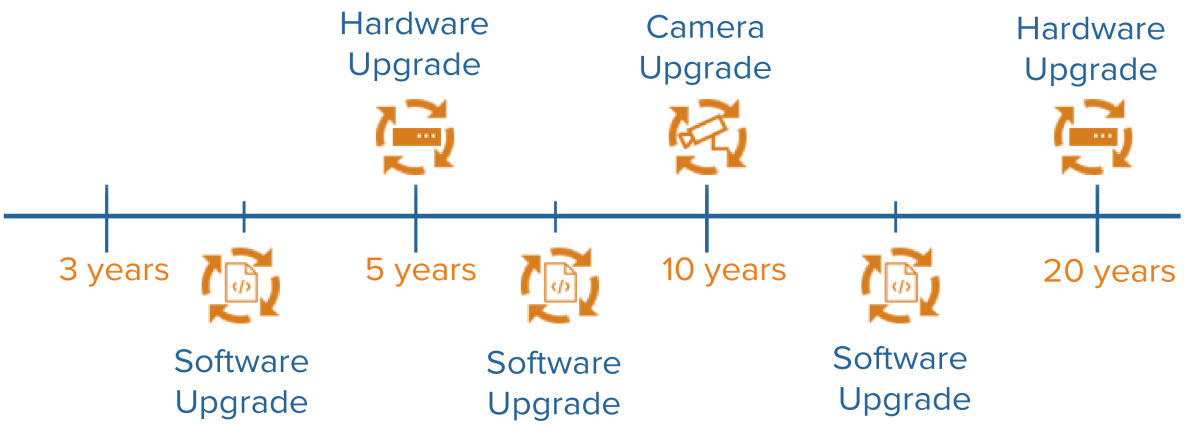


LIFECYCLE MANAGEMENT

Thousands of cameras, recorders and servers across the enterprise over time will comprise of tens or hundreds of different hardware models, firmware revisions and configuration. A key vulnerability exists in the use of passwords for each IP cameras, with newer cameras having three or more passwords for administration, video streaming, ONVIF configuration and other services. While all factory default passwords should be changed at the time of installation, unfortunately it is not common practice to use unique passwords for each device or to rotate them regularly. Changes to passwords also need to be propagated to the video recorders and viewers so they can continue to stream video from cameras. The sheer effort required to do this makes it impractical to update camera passwords on a regular basis.

As devices fail and are replaced, they may be replaced with a newer model or perhaps a different vendor's camera, and settings for the camera have to be re-programmed. Variations across models and vendors in settings mean that a common standard is virtually impossible to achieve. As new firmware is released by vendors, the process of applying this firmware is cumbersome and requires significant handholding with access to the security network on site. Should firmware be incompatible, it may fail to be applied, or worse, may render the camera inoperable which requires on- site intervention and troubleshooting.

Vendors of cameras, NVRs and VMS software must be able to provide and commit to long term support that goes beyond a statement that software and firmware updates will be provided. It is imperative that long- term support and backward compatibility be ensured for all hardware, software and services. For enterprise customers, it is important to truly understand in detail the effort that would be required on their part to keep a distributed system running over a decade or longer without requiring a forklift upgrade or a large investment in resources. A 5 year software update and firmware update guarantee with at least two updates a year should be mandatory and the ability to run older hardware/firmware concurrently with newer replacement hardware on a common VMS platform with no degradation.



CONCLUSION

Enterprise IT tools and processes that have historically worked to manage desktop and server infrastructure do not easily translate to the management of video surveillance, which tends to have its own unique set of challenges. Fortunately, managed video surveillance can serve as a force multiplier for stretched resources and budgets, while ensuring full lifecycle support in the long run. With companies beginning to embrace managed services in other parts of the enterprise, such as VoIP and hosted Exchange, there are precedents and best practices that can be applied to video surveillance and other physical security challenges.

About the Author: Nik Gagvani, Ph.D. is President and founder of CheckVideo, based in Falls Church, VA. A technology entrepreneur, Dr. Gagvani has started and grown four companies in the video security space. He is credited with launching the first DIY security camera with machine learning. At CheckVideo, his team is combining enterprise grade security with smart, managed video surveillance which serves as a force multiplier for security and IT teams.