WHITE PAPER

5 steps to make live production workflows cyber-secure

A guide to how broadcasters & live production companies can build a secure global framework to protect content, services & brand integrity

Contents

Introduction

The transition to IP is undoubtedly delivering significant benefits to broadcasters and media organisations worldwide. Today, sports and live production companies – the early adopters driven by fierce market demand for high-quality coverage anywhere and anytime - successfully showcase the flexibility, scalability and speed provided by IP infrastructure and accelerated by the pandemic, the agility remote IP production offers.

Across industries where IP infrastructure is mature, cyber-security is a business priority with enterprise-scale threat protection technologies deployed to mitigate risks to operations. For media organisations new to IP and with prime-time coverage and huge global audiences to protect, security must now be considered a critical component in their supply chains.

However, the dynamic nature of live broadcast environments - where the focus is on high-performance and low latency and where no production is the same - makes implementing security measures particularly complex.

In this paper, we explore the steps broadcasters and media organisations should take to protect themselves from the disruption of cyber-attacks and how to keep their live services safe and on-air.

Navigating a challenging landscape

Firstly, let's take a look at the threat landscape through which broadcasters and live production companies need to navigate.

To provide the optimum live viewing experiences that audiences demand, fast-paced IP production environments harness multivendor broadcast hardware and software applications, generic IT technologies, physical infrastructure and increasingly private and public cloud services to deliver from glass to glass. From venue to viewing device, this creates an expansive attack surface, exposing vulnerabilities across the broadcast chain that cyber criminals are all too ready to exploit.

Add remote production into the mix, the potential for creative and technical staff to be targeted and made vulnerable by human-error, security can be compromised at a user-level deep in the workflow.

From malware, ransomware, distributed denial of service to phishing, attacks are increasing in complexity, frequency and duration across all industry sectors, including broadcast media where recent attacks on high-profile broadcasters are well-documented. In live production environments, with such a large attack surface, the potential for multiple attacks to occur simultaneously, is an unwelcome reality that needs to be addressed.

Enterprise-scale threat protection technologies are well-proven in IP environments and are now increasingly deployed by media organisations on a corporate level to protect business systems. Solutions such as Web Application Firewalls (WAF), Intrusion Detection Systems (IDS) and Elasticsearch engines to index alerts and metadata, are now being rolled-out into live IP production environments to protect key areas of the workflow.

However, the threat landscape is ever evolving, with attacks growing in sophistication, frequency and duration, so security should not be seen as a "set it and forget" technology solution. Security policy is a moving target and the deployment of enterprise threat protection technologies alongside broadcast technology is not enough in itself to protect workflows. Expertise to balance performance and protection, alongside good and continuous security governance, is also vital.

As we become more dependent on digital IP infrastructure, what steps can broadcasters and media organisations take to make their live production operations cyber-secure and mitigate risks to critical assets, data and applications?

WHETHER MOTIVATED BY FINANCIAL GAIN OR POLITICAL AGITATION, CYBER-ATTACKS CAN UNDERMINE CONFIDENTIALITY, INTEGRITY AND AVAILABILITY ACROSS THE PRODUCTION CHAIN:

- **Malware:** Malicious software or a program code designed to harm a computer or its data
- **Ransomware:** A form of malware in which the user's files are encrypted and a ransom is demanded to restore the system to normal use
- **Phishing:** direct communication to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords
- **Distributed Denial of Service:** An attack that occurs when multiple systems flood the bandwidth of the targeted system with traffic and disrupt services

5 essential steps to become cyber-secure

1. Good housekeeping is fundamental

The first step in gaining control of your infrastructure is to know what equipment you have to protect. And that means all hardware and virtual (VM and cloud) assets on your networks - from the humble office printer to the latest high-spec super slomo camera equipment. Keeping an inventory may seem obvious but given the amount of kit used in live production environments and stored ready for deployment, it can seem a daunting task. However, by closely managing all hardware on the network – both IT and broadcast devices - it is easier to spot rogue assets and remove or isolate them.

Just as you need to keep track of your hardware assets, it's necessary to maintain an up-to-date list of all authorized software required across business operations. That includes both broadcast and typical IT solutions. Ensure that only software applications or operating systems currently supported and receiving vendor updates are added to your authorized software inventory.

Whether you rely on manual lists or use asset discovery and software inventory tools, the core security principle is simplicity. If software is unauthorized, it should not be installed. If an asset is not needed, that asset should not present on the network. If it is not present, it can't cause a security risk. Make sure to sync your software and hardware asset inventories, so that all devices and associated application are tracked from a single location for tight control.

Once you understand the kit and software you need to protect, it's essential to know who has access to and uses those systems and applications. The most common attacker techniques take advantage of uncontrolled administrative privileges, so keep access in check. Maintain an inventory of all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges. And for greater peace of mind, change all default passwords before deploying an asset into a production.

> "If software is unauthorized, it should not be installed. If an asset is not needed, that asset should not present on the network."

2. Identify & manage your vulnerabilities

When security researchers report new vulnerabilities, a game starts between all actors in the loop. The vendor will develop a patch asap, the security engineers will assess the risk and put all the counter measures in place and finally, the hacker will study, understand, stabilize the vulnerability and weaponize it by creating an exploit. We have to admit that in real life, the hacker is the winner in 99% of the cases. If an organization doesn't scan the network and proactively search for vulnerabilities, their assets will soon be compromised.

Whether using manual audits or authenticated vulnerability scanning with local agents or remote scanners, make it a priority to perform regular assessments of your assets to identify vulnerabilities, remediate and minimize the attack surface. Couple this with logging events and you'll be better placed to detect malicious software and activities and recover from an attack.

If logging and analysis of events is not present, it allows attackers to hide their location, malicious software, and activities on victim machines. Even if the victims know that their systems have been compromised, without complete logging records they are blind to the details of the attack and to subsequent actions taken by the attackers. Without solid audit logs, an attack may go unnoticed indefinitely and the particular damages done may be irreversible. In some cases, an effective audit logging program can be the difference between a low impact security incident which is detected before covered data is stolen or a severe data breach where attackers download large volume of covered data over a prolonged period of time.

The latest Security Information & Event Management (SIEM) software supports various log sources such as OSs, security software, application servers and even physical security control devices such as badge readers. Teamed with a Broadcast Control System (BCS), SIEM can provide you with granular detail to monitor the most critical broadcast operations.

3. Protect your network to keep workflows & content secure

Today's broadcast IP architectures are complex. Workflows rely on ethernet networks to provide the scalability and bandwidth to manage devices, assets, data, applications, users and locations – all interconnected and communicating with the external world. To protect your valuable assets and content, you need to start by protecting your network.

Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers installed by default on a variety of different device types, often without a business need for the given service. Many software packages automatically install services and turn them on as part of the installation of the main software package without informing a user or administrator that the services have been enabled. Attackers scan for such services and attempt to exploit these services, default user IDs and passwords or widely available exploitation codes.

To protect your network, you must consider access and usage:

- **Network ports:** It is vital that the operational use of ports, protocols, and services on networked devices are limited and rigorously controlled. Only those associated with your assets inventory should be open and they should only be running when you need them. When not in use, close them.
- **Firewalls:** Employ robust host and perimeter firewall architecture, scaled to meet your throughput requirements. Firewalls will control access to your domains and drop all traffic except those services and ports that are explicitly allowed to keep the network safe. Add in Web Application Firewall (WAF) to protect internet-facing applications from web protocols misuse, SQL injection and Denial of Service attacks.
- **Encryption:** For greater protection of your most valuable assets and to comply with regulations, encrypt your data in both transit and rest, using proper key management systems. Ensure stringent policies to control how master keys are stored, used and who has access to them.

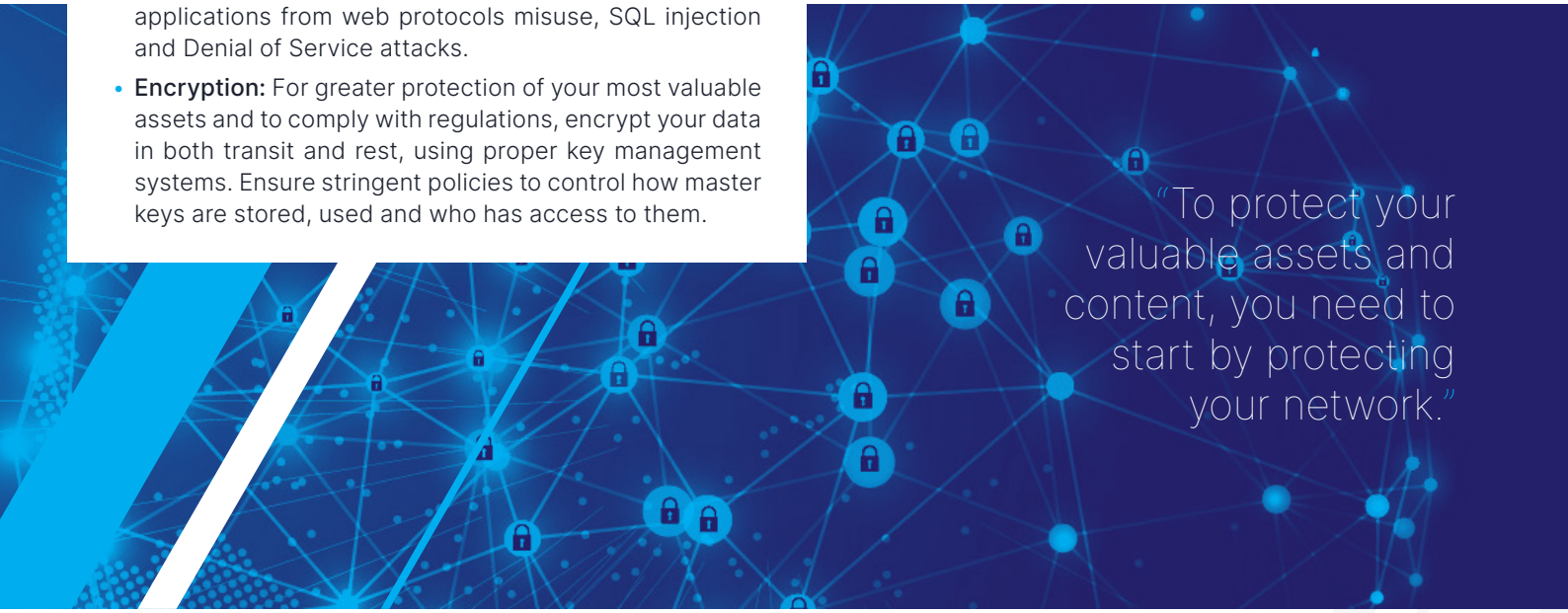
4. Follow industry due diligence

Whilst each organisation must take responsibility for its own security policies, the burden of cyber-threats is one that is shared across the broadcast and media community, so you're not facing it alone. Broadcasters are working together with industry bodies such as the Society of Motion Pictures & Television Engineers (SMPTE) and the European Broadcast Union (EBU) to push cyber security due diligence to the top of the agenda for manufacturers, services providers, systems integrators and users alike.

Through the exchange of knowledge, experience on security topics and extensive testing, organisations are collaborating to ensure systems, software and services used throughout production workflows do not create security breaches that could lead to impactful attacks.

This extends well beyond the rollout of enterprise threat protection technologies into development of good security policies, governance and training - all necessary to reduce vulnerabilities, build resilience, counter malicious actors and make the entire broadcast ecosystem secure.

For example, the world's major broadcasters firmly support the latest EBU directives such as EBU R-143 and R-148, which provide a framework for vendors to safeguard systems and services. These directives provide clear guidance on effective cyber security organisation, audits, analysis and vulnerability management, incident management, product lifecycle and development, maintenance and training, physical and cloud security, supply chain management and business continuity. When you engage with vendors ensure they follow and comply with these industry standards and can demonstrate that they are cyber-ready.



5. Partner with vendors who take security seriously

Broadcasters and media organisations expect vendor partners to deliver efficiencies and innovation across their workflows. Increasingly they also expect vendors to fully understand the challenges and risks of the security landscape and to provide the right skills to help them prevent and recover from cyber-attacks.

Compliance to industry standards is key but the customer's trust will increase if the vendor can demonstrate that they are implementing their own safeguarding measures. To build a cyber-secure framework, focus on working with vendors who are:

- attentive to the integration of enterprise security tools in your workflows and are experienced with balancing the high-performance required for live production with essential protection measures. It's not necessary for vendors to reinvent the wheel when it comes to security technology, but they should keep abreast of latest technologies and best practice - bridging the gap between IT and broadcast with a common language.
- able to undertake detection and prevention practices and deliver security measures from firewall management, network micro-segregation and micro-segmentation, redundancy and fallback plans in case of breach.
- primed to support you with a dedicated Incident Response team should an attack occur, minimising disruption and providing feedback to address issues for the future.
- and who consider cyber-security as early as possible in the development and lifecycle of their products and solutions so that they are inherently secure by design.

Organisations who take these steps to understand and implement security measures across their operations, who take advantage of the latest enterprise threat protection technologies, follow industry best practice and work with vendors who demonstrate proven security expertise and compliance, will survive and thrive in this emerging all-connected world.

Working with you to become cyber-secure

As a leading provider and architect of IP infrastructure solutions for the broadcast industry, EVS takes security seriously. Serving a growing customer-base of high-profile broadcasters and production companies delivering news and major sporting events worldwide, we are committed to meticulously safeguarding our clients from malicious parties and the disruption that their attacks can unleash.

We're building a security-first culture across our business: employing dedicated security experts to assess and prevent threats at a product and workflow level; using the latest security tools, complying with industry standards and best practice, and building a roadmap of solutions secure by design.

Contact us today to find out how EVS supports customers to be cyber-ready.