Grass Valley

ARTICLE

Why Trusted & Secure Media Operations Matter

Seven paradoxes shaping the next era of media production, Article 3

By Ronny van Geel, Director Product Marketing at Grass Valley

In this series, we explore the technologies, architectures and operational realities shaping modern media operations. Along the way, we examine how these individual pieces contribute to a larger operational picture and ultimately help organizations build a unified media operation.

In our previous article, we explored why interoperability alone is no longer enough. As software-defined media operations become more distributed and dynamic, preserving meaning and context through the Media eXchange Layer, or MXL, creates something increasingly valuable: freedom.

But freedom introduces a new challenge. As organizations increasingly rely on people, expertise and partners beyond their traditional boundaries, how do they build trust in an operating model designed around openness and continuous change?

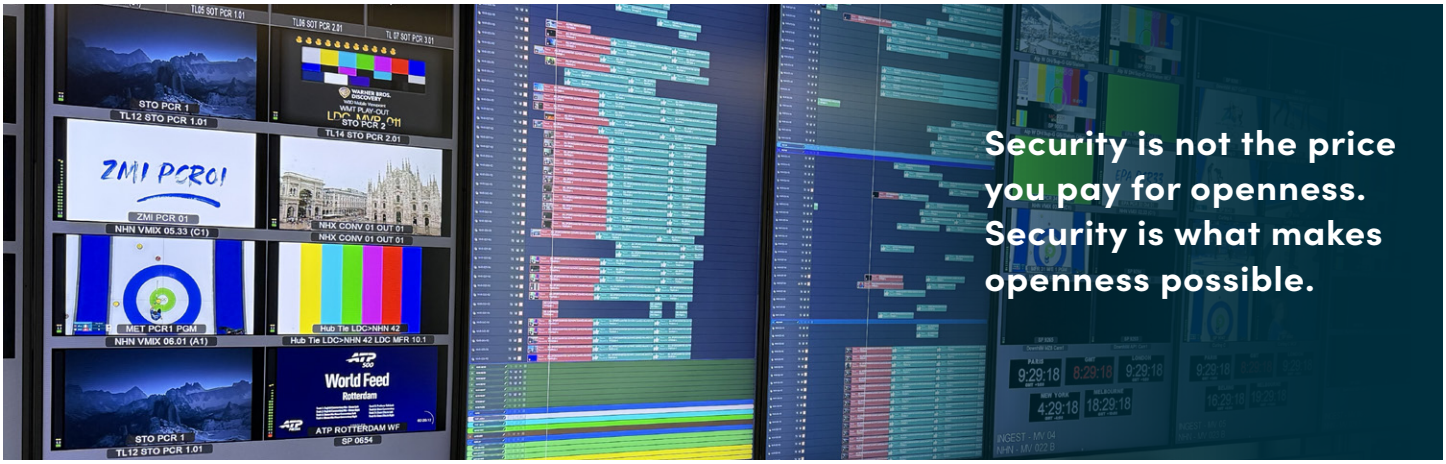
The third paradox: The more we open up, the more we must protect.

Security has always been part of how media organizations build trust. Every media organization understands that the value it creates depends on assets that must be protected. Content, operational systems and audience trust have always been fundamental to the success of the business.

But in an environment increasingly shaped by AI, software dependency chains and rapidly evolving threats, protection cannot be treated as a point-in-time exercise. Security must be continuously assessed, maintained and improved as the operational environment changes.

The evolving risk landscape becomes even more significant as operating models themselves change. The shift to a Dynamic Media Facility does not remove the responsibility to protect, it amplifies the need to do so consistently across a more fluid and distributed environment. It also changes the pace at which risk can emerge. As software, infrastructure and services evolve more frequently, maintaining trust requires the ability to remain continuously aware of vulnerabilities and respond before they become operational issues.

That shift is driven by a changing business reality. Viewers have more choice than ever. Loyalty is harder to earn and easier to lose. Content owners must create more content, serve more audiences and respond faster to changing opportunities while still protecting the quality and distinctiveness of what makes them unique.



To meet those demands, media organizations increasingly rely on remote contributors, regional hubs, partner ecosystems and software-defined workflows. Expertise can contribute from anywhere. Dynamic Media Facilities allow resources to be deployed where they create the most value rather than where they happen to reside — not because technology allows it, because the business demands it.

For decades, media operations were largely built on infrastructure that remained under direct control. The signal paths, the facilities, the equipment and the operational boundaries were all carefully managed because they formed the foundation upon which trust was built.

Today, many of the capabilities that create value no longer sit neatly within those boundaries. And that is exactly where the paradox emerges: the more people, workflows and capabilities contribute to an operation, the less trust can depend on traditional boundaries.

The Real Challenge Is Not Locking Everything Down

The traditional operating model created a straightforward trust equation. Access was often linked to presence. Being inside the operational boundary carried implicit trust because the boundary itself was tightly controlled.

That model still has value in many contexts. Dedicated infrastructure, private networks and controlled facilities continue to play essential roles across the industry. The point is not that one model has replaced another. The point is that software-defined and distributed workflows introduce a different trust equation.

When teams work across locations, when applications run on shared compute, when contribution happens over less controlled networks, and when partners become part of the operational chain, the old assumptions no longer hold. Access can no longer be trusted simply because it originates inside a familiar boundary. Identity can no longer be assumed because someone is inside the facility.

And the challenge is no longer only deciding who gets in. The challenge is knowing who is there, what they are allowed to do and whether that access remains appropriate as the operation evolves.

In traditional operating models, those questions were often easier to answer. If systems, people and workflows remained within clearly defined boundaries, much of that trust could be inherited from the environment itself.

Software-defined operations change that equation. Trust must be deliberately established, governed and maintained. It increasingly becomes an operational capability in its own right. That shift sits at the heart of modern media security.

Organizations want the best creative talent to contribute regardless of location. They want to create more content without moving every person and every resource to every venue. They want to combine internal capabilities with partner services and software-defined workflows.

All of those ambitions require participation. The question is how to make that participation safe enough to build upon.

Enter Zero Trust

Zero Trust is sometimes discussed as if it were a security product or a technical architecture. In reality, its most important contribution is a mindset.

At its simplest, Zero Trust means that systems, users and devices are not trusted by default. Access must be authenticated, authorized and limited to what is required. Permissions should reflect roles and responsibilities. Activity should be traceable. Assumptions should be replaced by verification.

That same principle must extend beyond access. The software, services and components that make up an operation cannot be assumed to remain secure simply because they were secure when first deployed.

This is where the traditional trade-off between openness and security begins to break down. Security is often perceived as friction, something that slows teams down, restricts creativity or makes new operating models harder to adopt.

Poorly designed security can certainly do that. But well-designed security does the opposite — it creates the conditions under which openness becomes practical.

Security is not the price you pay for openness. Security is what makes openness possible.

The Industry Perspective

The importance of this perspective is reflected strongly in conversations across the industry.

Through the GVx Council, we asked media leaders to share their perspectives on the operational realities shaping the transition toward more dynamic and software-defined environments. One theme emerged clearly: Security cannot be added at the end.

As Emili Planas observed, "Security designed from the start, governance, identity management and business continuity must all be part of the conversation."

That sentence is important because it does not frame security as a single layer, tool or feature. It frames trust as a system property. Security, governance, identity and continuity are connected because they all answer different parts of the same question: can this operation be depended upon when it matters?

This is why trust in software-defined operations must extend beyond cybersecurity alone.

Trust depends on governance, ownership, accountability and continuity just as much as it depends on technical security controls. Organizations need to know not only that systems are protected, but also who is responsible, how decisions are made and whether the operation can be depended upon when circumstances change.

That broader view of trust is increasingly shaping both industry practices and regulatory expectations. Frameworks such as the Cyber Resilience Act reflect a growing recognition that resilience, accountability and security must be designed into the operation itself rather than added later. They also reinforce an increasingly important expectation: organizations must be able to identify vulnerabilities, manage change and apply remediation on an ongoing basis, rather than relying on infrequent review cycles.

A CSO, Head of Operations or CTO is not simply evaluating technology. They are protecting something they care deeply about.

Media production has always attracted people who think ahead. They look for weaknesses because they want the operation to succeed. They challenge assumptions because they care about reliability. They ask difficult questions because they understand the value of what they are helping to create and protect.

These are not questions of fear. They are questions of pride, ownership and responsibility.

The Shift Is Already Underway

The shift toward trusted and secure media operations is already visible across the industry. The Dynamic Media Facility Reference Architecture treats security, monitoring, control and orchestration as cross-cutting concerns rather than separate afterthoughts. That matters because it confirms a broader industry recognition: dynamic operations require trust to be designed into every layer of the workload lifecycle.

That lifecycle does not end once a system is deployed. In a world of continuously evolving software and AI-enabled development, the ability to monitor for newly identified Common Vulnerabilities and Exposures, or CVEs, and act quickly where relevant has become part of operating responsibly.

This is also why the work can be difficult.

As Geir Børdalen noted, "We are building IP infrastructure based on Zero Trust. The process is extremely time consuming and constantly challenges timelines."

That honest observation reflects a reality many organizations are experiencing. Building trust into a modern operating model requires more than implementing technology. It requires organizations to rethink assumptions, processes and responsibilities that have often existed for decades.

It also requires change management to evolve. Security updates cannot always wait for a small number of scheduled release windows.

Organizations need disciplined processes that allow important remediation to be assessed, validated, communicated and deployed rapidly, while maintaining control over the operation.

Yes, the effort can be significant, but so are the risks and opportunities. The same foundations that strengthen security also make it possible to embrace more open, flexible and collaborative ways of working.

For Grass Valley, this shift has shaped AMPP OS from the very beginning.

The goal was never simply to make media operations more connected. The challenge was ensuring they could become more connected without losing the trust upon which those operations depend.

That philosophy influences everything from identity and access management to governance, auditability and accountability. Rather than treating security as a separate layer added around the platform, these capabilities are woven into the operating model itself.

AMPP OS reflects a simple belief: participation should be easy, but trust should never be assumed.

For Grass Valley, security is not treated as a phase in the product lifecycle. It is a design and operational principle. That means maintaining continuous awareness across the portfolio, with regular CVE scanning performed weekly and, where required, daily.

Finding a vulnerability is only part of the responsibility. The real test is whether an organization has the culture, processes and delivery capability to act. Our approach is designed to support timely updates where they are needed, ensuring that remediation, compliance and operational confidence remain aligned as conditions change.

This is particularly important in the age of AI. As the pace of software development accelerates and the threat landscape evolves alongside it, trust depends on being able to adapt without compromising the stability and control media operations require.

That approach is reflected in AMPP's SOC 2 compliance, which provides important independent assurance. But compliance is not an endpoint. It is one expression of a broader commitment to continuously identify, assess and address the risks that matter most to customers and their operations.

As media operations become increasingly distributed, dynamic and collaborative, trust must remain consistent regardless of where people, workflows or services participate.

Organizations rarely hesitate because a new operating model lacks capabilities. They hesitate when they are not yet convinced they can depend on it. Trust is what closes that gap.

In The End, It Is About The People

The audience rarely thinks about the trust model behind a production. They only experience whether the story arrives when it should, with the quality, integrity and confidence they expect.

The people responsible for making that happen understand that even the strongest architecture ultimately depends on human behavior. Passwords need to be protected. Credentials need to be managed responsibly. Access rights need to reflect reality. Permissions that are no longer needed must be removed. These are rarely the most exciting parts of media production, but they are often among the most important.

The same discipline applies to how organizations respond to change. Vulnerabilities must be understood. Updates must be prioritized. Decisions must be made with urgency where necessary, but never without accountability.

Media professionals take that responsibility seriously. They challenge assumptions because responsibility requires them to. They look for weaknesses because continuity depends on it. They understand that trust is not something a system creates on its own. It is something an organization maintains through discipline, ownership and attention to detail.

That is not fear. It is professionalism.

What Trust Really Enables

Throughout this article, we have talked about security, governance, identity, permissions and account-ability. It would be easy to conclude that trusted operations are ultimately about protection. They are not.

Trust has always mattered. What has changed is that trust is no longer valuable only because of what it protects. It is valuable because of what it makes possible.

The purpose of trust was never to keep people out. The purpose of trust was to know who could safely come in.

That distinction changes everything. It allows organizations to expand participation without sacrificing accountability. It allows flexibility to grow without losing control. It creates an environment in which people, workflows and capabilities can come together with confidence.

For decades, media organizations built trust by limiting participation. Today, they increasingly create value by expanding it.

For decades, media organizations built trust by limiting participation. Today, they increasingly create value by expanding it.

Closing Thought

As we have seen, the move toward more open media operations is not driven by technology alone. It is driven by the need to create more relevant content, use talent more effectively, collaborate across locations and respond to audiences whose expectations continue to grow.

The trust required to support that shift depends on more than protection at a single moment in time. It depends on identity, governance, accountability and security principles designed into the operating model from the beginning, then continually maintained as the operation evolves.

When those foundations are in place, organizations can involve more people, workflows and capabilities without surrendering control.

And then, another question naturally follows: once an operation can be trusted, how do we keep it running, evolving and improving without disrupting the value it already creates every day?

That is the challenge we will explore in the next article.

This product may be protected by one or more patents. For further information, please visit: **www.grassvalley.com/patents**

WP-PUB-3-1110A-EN

Grass Valley®, GV®, GV Grass Valley®, and the Grass Valley logo are trademarks or registered trademarks of Grass Valley USA, LLC, or its affiliated companies in the United States and other jurisdictions. Grass Valley products listed above are trademarks or registered trademarks of Grass Valley USA, LLC or its affiliated companies, and other parties may also have trademark rights in other terms used herein. Copyright © 2026 Grass Valley Canada. All rights reserved. Specifications subject to change without notice.

www.grassvalley.com Join the Conversation at GrassValleyLive on Facebook, X, YouTube and Grass Valley on LinkedIn