SWEAR™

SWEAR Case Study: Houston First

Ensuring Video Authenticity in a New Era of Digital Risk

CASE STUDY

About Houston First

Houston First Corporation operates at the center of one of the nation's most dynamic metropolitan areas, managing convention centers, entertainment venues, and tourism assets that welcome millions of visitors each year. From large-scale conferences to high-profile public events, the organization plays a crucial role in shaping the city's experience and its reputation.

As Director of Security, Ben Williams oversees the strategies, systems, and operations that protect Houston First's expansive portfolio, because large-scale events, public access, and high visibility demand a security approach that goes beyond the basics. To meet those expectations, the organization relies heavily on advanced technologies to enhance situational awareness, streamline response, and strengthen overall security.

From high-resolution video surveillance systems to integrated security platforms, technology plays a central role in ensuring operations are effective and resilient in the face of evolving threats.

But as reliance on technology grows, so does a new and more complex challenge.

We are now operating in an age of misinformation, where manipulated content, deepfakes, and altered videos are becoming more sophisticated and, in some cases, more convincing than reality itself. In this environment, video can no longer be assumed to be a definitive source of truth.

For organizations like Houston First, where video surveillance is critical to understanding incidents, guiding decisions, and supporting investigations, this shift raises an urgent question: How can you trust what you see?

That's where authentication becomes essential. It is not just a safeguard but a foundation for modern security.

THE SWEAR SOLUTION

Defensive/forensic analysis has traditionally been the tech industry's go-to strategy for identifying manipulated content. However, this reactive approach is locked in a never-ending arms race against increasingly sophisticated forgeries, making it insufficient in today's rapidly evolving digital landscape.

The future of information security demands a paradigm shift from after-the-fact detection to the creation of permanently verifiable records of reality at the moment of recording. SWEAR has pioneered this groundbreaking approach, offering real-time authentication instead of fragmented analysis. Our patented "Digital DNA Mapping" technology, powered by blockchain, ensures that any manipulation is instantly detectable while preserving the integrity of every pixel, sound, and frame. Designed to withstand even the most advanced AI and quantum exploits, this methodology transcends traditional forensics, delivering an unprecedented level of tamper-proof protection.

The Challenge: When Trust in Video Can No Longer By Assumed

The rise of artificial intelligence and digital editing tools has fundamentally changed the nature of risk. Today, video content — once considered a reliable source of truth and data — can be manipulated, altered, or fabricated with increasing sophistication.

For security leaders like Williams, this shift introduces an urgent challenge: how to ensure that video evidence remains credible in an era where "seeing is believing" is no longer guaranteed. "We're at a point where digital content can be changed so easily that you have to question everything," Williams explains. "From a security and legal standpoint, that creates real risk. If a video is challenged, you have to be able to prove it's authentic."

At Houston First, video footage plays a central role in incident response, internal reviews, and potential legal proceedings. Without a reliable method to validate that footage, even the most critical evidence can be called into question — undermining investigations, delaying resolution, and exposing the organization to reputational and legal consequences.

Equally important is the broader brand impact. In a public-facing organization, the circulation of altered or misleading video content can create confusion, erode trust, and damage credibility.

"We have to think about how content could be used outside of our control," Williams adds. "If something is altered and shared, it can quickly become a much bigger issue."

The Solution: Verifiable, Tamper-Evident Video

Houston First has made a deliberate commitment to adopting technologies that lead the way in modern security. At the core of its infrastructure is Milestone's XProtect video management software, a platform that enables the organization to manage and leverage video intelligence across its operations. It was through this ecosystem that Ben Williams was introduced to SWEAR.

Recognizing the growing risks tied to manipulated media and the need to validate digital evidence, Williams saw immediate value in SWEAR's integration with Milestone. Rather than disrupting existing workflows, the technology seamlessly adds a critical layer focused on video authentication and integrity.

What stood out was how easily it could integrate into what we were already using," Williams says. "It wasn't about replacing anything; it was about strengthening it."

The integration offered a compelling advantage by enhancing Houston First's existing video infrastructure with a solution designed to ensure that video data remains verified, authentic, and defensible.

SWEAR takes a fundamentally different approach to video integrity. Rather than embedding watermarks or altering the original file, the platform maps the unique digital DNA of each recording. It analyzes pixels, frames, and sound, and anchors that fingerprint securely to SWEAR's databases, where each unique hash is secured by blockchain technology. This creates an immutable, time-stamped record that can be used to validate the authenticity of the video at any point in the future.

This method ensures the original content remains untouched while providing a trusted, independent way to verify whether video footage has been altered. "With SWEAR, we're able to confirm that our video hasn't been manipulated," Williams says. "That level of verification is critical for us — especially when the footage may be used in an investigation or presented externally."

Once deployed, SWEAR became an essential layer within Houston First's security ecosystem. It has protected video as it is exported, shared, and reviewed. If any modification occurs, even at the most granular level, the system detects the change immediately by comparing it to the original digital fingerprint.

"It's essentially a digital fingerprint for the video," Williams explains. "If anything changes, that fingerprint changes. That gives us a clear indication of whether the content is still authentic."

By leveraging SWEAR, Houston First has strengthened its ability to independently verify the authenticity of video evidence across both legal and investigative scenarios. The technology enables the team to have confidence in every frame of video, while also preserving a secure and defensible chain of trust as content is exported and shared. Just as importantly, it helps safeguard the organization's reputation by reducing the risk of altered or misleading video content circulating beyond its control.

The Future: From Optional Capability to Industry Standard

While Houston First has not yet faced a direct incident involving manipulated video, Williams is focused on what lies ahead. As synthetic media and deepfake technologies continue to evolve, the ability to verify digital content is quickly shifting from a forward-looking capability to a core requirement.

"This is where things are going," he says. "The technology to manipulate content is only going to get better. We have to be prepared for that." For Williams, adopting SWEAR represents a proactive step toward future-proofing the organization's security operations — ensuring that video remains a defensible source of truth, regardless of how the threat landscape evolves.

"This isn't going to be a 'nice-to-have' for long," he adds. "Being able to prove authenticity is going to be essential, especially in legal environments."

As the line between real and manipulated content continues to blur, Houston First is setting a new standard where trust is not assumed, but verified.

In an increasingly complex digital world, that distinction may prove to be one of the most important safeguards of all.

What Makes SWEAR Different?

AI-Resistant by Design

Cryptographic fingerprints for every second of media —recorded, hashed, and verified in real-time.

Blockchain Backed Authenticity

Decentralized and tamper-proof. Every second of a recording is mapped, in real-time into an independent chain of custody.

Enterprise Ready at Scale

SWEAR integrates across devices and platforms — with minimal friction and maximum protection.