Securing the Integrity of Video Analytics Data

A Parks Associates Whitepaper Developed for

verimatrix®

PARKS ASSOCIATES

Securing the Integrity of Video Analytics Data

As video service providers focus on individual subscriber services, the breadth and depth of the data collected to drive intelligent content services are growing.

Securing video analytics data is a high priority for operators and customers, but the intricacy of data security is a sensitive topic.

This whitepaper on analytics and data security is **informed by a series of in-depth interviews** recently conducted with key decision makers from within the video service operator industry. Their thinking informs discussion on the complexities of strategy in a rapidly changing marketplace for video services and the technologies that drive them.

Interviews with operators and industry executives reveal the following trends:

- Operators face new operating and security risks due to an increasingly connected ecosystem
- Trust is the foundation of the operator-customer relationship in a data-driven economy
- The structure of operator organizations includes C-level positions dedicated to security and privacy of customer information.

Based on this information, this research draws the following conclusions:

- Securing video analytics data must be a constant priority, not a periodic responsibility, to ensure the security and integrity of the data
- With an increased reliance on video analytics data for service-related decisions, ensuring the integrity of the data and trust of the customer has become a board-level responsibility
- Operators understand that security of video analytics data is not their core business and are instead leaning on partners with security-specific expertise

Security: The New Key Performance Indicator

Service providers take protecting customer privacy seriously following increased attention from consumers. As the modern interconnected world has opened humanity to a global society, service providers are faced with new risks of maintaining data privacy and consumer trust.

New Risks for Operators

As video service operators provide content to consumers, they collect video analytics data every step of the way to feed their decision making for value-added services like content recommendation and advertising. They identify several risk factors impacting the security and privacy of this customer data.

Risk Factors

- Cloud connectivity
- Multivendor environment
- Savvy hackers

- **Cloud connectivity:** Rising operational costs and scale issues demand a move from hardware-based service distribution to virtualized cloud-based operations. Regardless of whether data is stored on or off-site, data increasingly flows through potentially vulnerable software-defined networks.
- **Multivendor environment:** Operators require multiple solutions to unique problems that a single vendor cannot necessarily address. Consuming content on unmanaged devices with multiple programming architectures requires a more complex system than ever. Complex operator systems present more opportunities for potential leaks that may initially be undetected.
- **Savvy hackers:** Even when a provider takes all necessary technological steps to protect customers and their video analytics data, the systems are only as effective as the employees who have access to the data. Phishing schemes that exploit the most honest of employees have victimized service providers and customers alike. Staying ahead of hackers is a challenge that operators may not have the dedicated expertise to handle.

Data-based decision making is a valuable component in an operator's arsenal, but the risk of data loss or exposure endangers the provider's credibility in the marketplace.

HIGH-PROFILE BREACHES

Cox Communications

In 2014, Cox Communications experienced a breach of its customer databases by the Lizard Squad hacker group. A hacker using the alias EvilJordie posed as a member of the Cox Communications' IT department and deceived a customer service representative and a contractor, resulting in them entering their account credentials into a false phishing website. The hacker accessed the customer database and obtained personal information, compromising over six million customers' accounts. For the breach, Cox was fined $595,000 by the FCC and forced to provide one year of free credit monitoring to the affected customers.[1] The cost was comparatively minor, as customers' detailed financial information was not exposed.

Target

In 2013, retailer Target experienced a breach that exposed customer credit card information. The company incurred expenses in excess of $260 million in fines, legal settlements, and associated expenses. The potential costs of a breach to both the customer and the company storing their data are palpable.[2]

[1]Lewis, Truman. "Cox fined for getting hacked." Consumer Affairs. 6 Nov 2015. https://www.consumeraffairs.com/news/cox-fined-for-getting-hacked-110615.html

[2]Tabuchi, Hiroko. "$10 Million Settlement in Target Data Breach Gets Preliminary Approval." The New York Times. 19 Mar 2015. http://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html?_r=0

A New Priority around Data Security

Operators report taking more of a big data approach to customer service in an increasingly data-driven economy, collecting vast quantities of information about the network and customers, including viewership data. Databases of personal information shine like beacons to hackers, and publicized security breaches lead to widespread concerns related to personal data.

DATABASES OF PERSONAL INFORMATION SHINE LIKE BEACONS TO HACKERS, AND PUBLICIZED SECURITY BREACHES LEAD TO WIDESPREAD CONCERNS RELATED TO PERSONAL DATA.

Securing content is a familiar function for video service operators, but securing video analytics data is admittedly a new territory for many. Managers within several operating companies report increasing consolidation of regional carriers to national operators and global conglomerates. These large companies require a shift to consolidated security systems. Operators began consolidating the data security functions of disaggregated subsidiaries into a corporate function, employing one of two main strategies:

Existing Chief Information Officer: Providers often roll data security and monitoring functions into the existing IT operations reporting to the CIO. The CIO is then responsible for all corporate information systems, including data security systems.

New position and group: Other providers are creating dedicated security and privacy positions. These may take the form of a Chief Security Officer, or in some cases even a Chief Privacy Officer, who is dedicated to ensuring the privacy of the operator's customers.

The key motivation for more centralized organization is developing a high level of control in the face of an increasingly complex environment.

Operators must consider whether or not their existing infrastructure is sufficient to protect analytics data and determine if reorganization is necessary.

The New Complexity

Operators indicate an expansion of video delivery and viewership analytics systems into the cloud, which has created a complex environment susceptible to a number of threats. In response, regulatory agencies established guidelines intending to protect consumer privacy.

Security Threats

Operators identify the following threats to video analytics data systems driving the need for comprehensive security systems:

Key Security Threats

- Hacking and exposing data
- Tracking viewership on unmanaged devices
- Security and integrity of viewing data

Hacking and exposing data: Hackers are the most publicized threats to the integrity of a data security system and also cause some of the highest financial damage. Operators may not be well-positioned to confront increasingly sophisticated cyber-attacks.

> **Key Implication:** Operators are often held liable in the event of security breaches, and harm to the operator's public image is likely to hinder retention — impacting relationships with suppliers and clients.

Tracking viewership on unmanaged devices: Much of the development in over-the-top (OTT) video delivery has centered on preventing copyright infringement as content is transmitted to consumers' disparate devices. However, as video analytics data flows in the opposite direction, operators now face the obligation of securing data from the device to the server. This data is vital not only to service providers for providing recommendations, but also to advertisers seeking to leverage digital ad inventory. Any use of web beacons or tracking pixels must be secure and conform to Interactive Advertising Bureau (IAB) standards.

> **Key Implication:** Operators must ensure the protection of not only content and entitlements, but also the integrity and security of census-level data provided to partner stakeholders.

Integrity and value of viewing data: As unmanaged devices become a larger part of the content consumption ecosystem and video shifts to an IP-based delivery model, ensuring the integrity and exclusivity of video analytics data will become a measure of the value of an operator's data. Any breach in the transfer of data impacts trust by the customer and the partners that rely on the collected data for decision making.

Key Implication: The ability to monetize video analytics data relies on data exclusivity, which is compromised in the event of a data pathway breach.

Vizio

An incident in 2015 underscored the necessity to secure data pathways on connected devices. Vizio was the subject of a hack that intercepted a viewer's data stream, known as a "man-in-the-middle attack." The smart TV connected with an external server approximately once per second, a connection that researchers from Czech software company Avast were able to exploit by mimicking the server's signed certificate and redirecting the signal. The hackers then received viewership information from the device and, alarmingly, received permission to control functions on the television. The TV function was enabled by default, without the user having to consent to the privacy policy for the connection to be active.[3]

As new devices and services are rapidly introduced to market, the industry is increasingly faced with new and unfamiliar data security challenges.

Any overlooked or neglected portion of the entire data security chain, no matter how seemingly minor, will come back to haunt the operator.

[3]Goodin, Dan. "Man-in-the-middle attack on Visio TVs coughs up owners' viewing habits." Ars Technica. 11 Nov 2015. http://arstechnica.com/security/2015/11/man-in-the-middle-attack-on-vizio-tvs-coughs-up-owners-viewing-habits/

New Regulation

Regulatory agencies in Europe have been proactive in protecting and promoting consumer privacy. In summer of 2016, the European Commission plans to adopt the finalized version of the General Data Protection Regulation (GDPR), which will define how companies can collect and use personal data. Once adopted, there will be a two-year transition period before formal implementation.

The GDPR impacts operators in several key ways:

- Companies must obtain informed consent from all consumers to collect data, including verification that minors have the consent of their parent or custodian.
- Consumers can withdraw consent and erase collected data at any time (i.e., the right to be forgotten).
- Companies cannot export data outside the EU to systems that do not meet GDPR standards.
- Companies must establish a Data Protection Officer (DPO) who reports on the company's security systems.
- Maximum fines for a breach are the greater of €20 million or 4% of annual worldwide revenue.

The DPO position requires executive attention from all companies that collect user data for core operations. In general, representatives from operators in established EU countries of Western Europe believe their companies already meet or exceed the GDPR due to the strictness of local laws. However, new entrants to the EU may have difficulty upgrading systems.

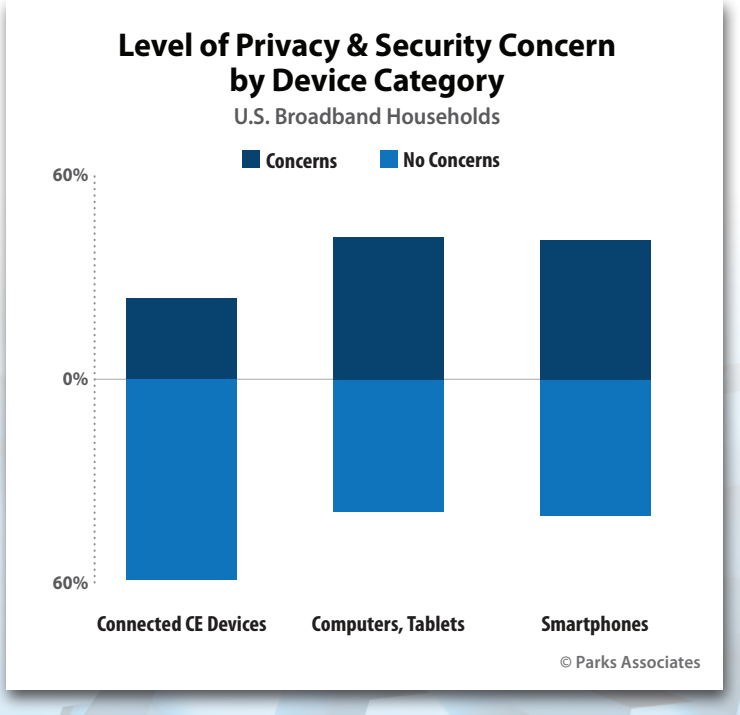
The U.S. stands in contrast to the EU, with privacy for all but the most sensitive data falling under industry self-regulation guided by a series of disparate and complex legal decisions as opposed to legislation. Operators will be bound by regulatory decisions, and implementations may be arduous and expensive.

Consumer Trust

Broadband and pay-TV operators invest significantly to create a trust-based relationship with their customers.

Preserving that trust is a key competitive advantage for operators at a time of heightened competition. On the whole, U.S. consumers are less concerned than their European counterparts with data collection and privacy. That said, Parks Associates' nationwide surveys of U.S. broadband households reveal somewhat high proportions of U.S. consumers who express concern regarding data collection on CE devices.

> PRESERVING TRUST WITH THEIR CUSTOMERS IS A KEY COMPETITIVE ADVANTAGE FOR OPERATORS AT A TIME OF HEIGHTENED COMPETITION.



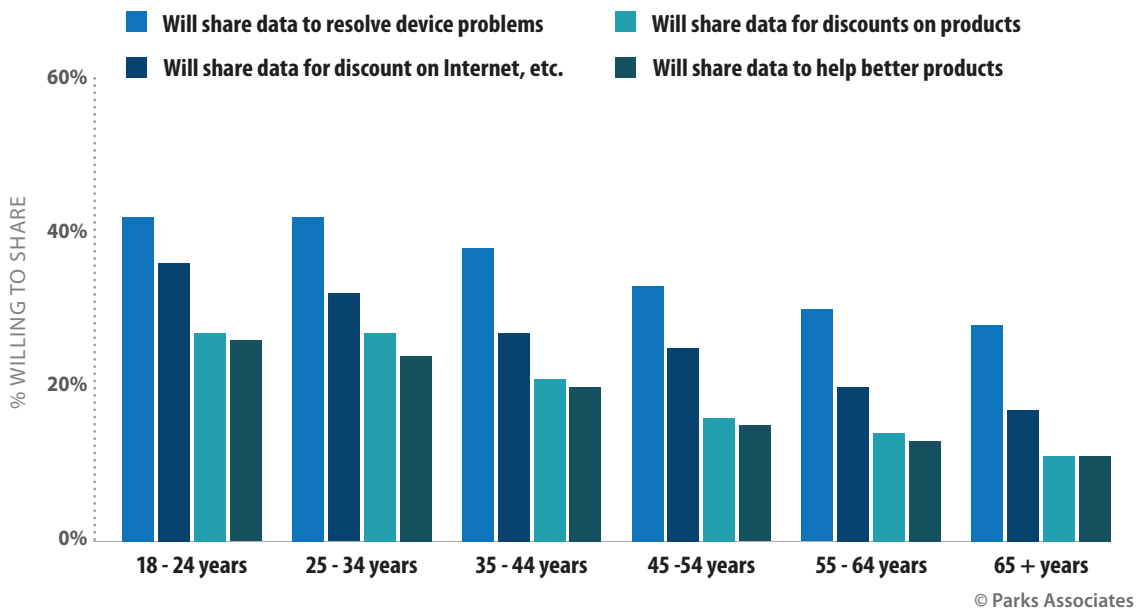
PARKS ASSOCIATES

WILLINGNESS TO SHARE DATA WITH COMPANIES FOR VARIOUS REASONS CORRELATES WITH AGE.

Younger consumers are less apprehensive about sharing their data than older consumers.

Willingness to Share Data from Connected CE Devices

U.S. Broadband Households



Given the tendency for young consumers to spend a disproportionately high amount of time consuming content on alternative devices, their higher willingness to share data is not surprising. However, the willingness of younger consumers to share their data in no way reduces the magnitude of their loss in the event of a breach. Operators have worked hard to build a high level of trust with their customers, with several operators touting this relationship highly. Maintaining this trust will be key to effective analytics implementations. If operators' customers were to perceive a breach of this trust, it would significantly damage their relationship with their operator.

IF OPERATORS' CUSTOMERS WERE TO PERCEIVE A BREACH OF THIS TRUST, IT WOULD SIGNIFICANTLY DAMAGE THEIR RELATIONSHIP WITH THEIR OPERATOR.

Why Focus on Security – Primary Motivators for Operators

Expanding Reliance on Vendor Partnerships

Operators vying for share in competitive markets increasingly rely on video analytics data to forge partnerships with vendors and clients alike. Data is driving content recommendation, advertisement placements, and asset valuation for content providers. Operators must have appropriate security protocols in place to anonymize sensitive and personally identifiable data and ensure compliance with regulatory guidelines. Operators must also ensure that data remains accurate and intact while accommodating both of these requirements. In this environment of complex relationships, operators must be able to compile and deliver actionable insights on the video analytics data they collect. This can be accomplished internally or through a vendor partnership.

In this environment of complex relationships, operators must be able to compile and deliver actionable insights on the video analytics data they collect. This can be accomplished internally or through a vendor partnership.

Development of Rules and Policies

Each module of software running on consumer devices requires a privacy policy agreement between the provider and the customer, most of which are never read in their entirety by the customer. In isolated instances, particularly with trial hardware or services through partnerships, operators report serving customers multiple privacy policies for the same service.

The operator must then reconcile multiple policies into a single policy, or serve multiple policies to an already fatigued customer prior to full launch. Operators may consider offering digestible privacy policy "highlights," like those Google uses for Android services to identify the primary areas of customer concern regarding data storage and use. Rules and policies must also conform to local and sometimes international data privacy regulations.

Achieving Scale

Traditional, well-established operators interviewed report high confidence in their abilities to scale. New entrants to the market, which are more likely to be OTT operators, are not likely to have the resources necessary to scale their operations on their own. Emerging services are more likely to be investor funded and required to achieve fast time to market with low capital investment. In a cloud-based environment, emerging operators can respond to growth by leasing cloud infrastructure rather than building network infrastructure on their own. The challenge then becomes securing a software-based, outsourced virtual network without the control afforded by internally housed hardware-based systems.

Any analytics-based implementation must deploy quickly, scale easily, and comply with regulatory and privacy policies.

Who Has the Keys? Developing Data Security Systems

Service operators are faced with three options when it comes to video analytics data security:

- Develop systems internally
- Outsource systems to third-party solutions providers
- Employ a mixed model approach that blends both internal and external solutions

Internal Development

Developing systems internally requires the operator to house not only the data warehouses themselves, but also to set all rules and policies regarding use of video analytics data, as well as ensure that all policies are compliant with applicable regulations. Additionally, operators must perform frequent threat assessments to defend against the constantly-changing hacker landscape.

Key advantages of internal development:

- High degree of control over security operations
- Ability to become a data security solutions provider or white-label service for other companies in need of security solutions.

Another key challenge for building systems internally is tracking data policies across multiple consumer devices, operating systems, application layers, geographic regions, and technology implementations.

Generally only the largest operators report any likelihood of building all data storage and security systems internally.

Developing systems internally is…

- resource intensive
- requires high capital investment for hardware acquisition and software development
- requires continuous investment and a large staff dedicated to data security

External Outsourcing

Key advantages of external outsourcing:

- Security-specific expertise
- Lower capital investment
- The ability to rapidly adapt systems to emerging threats

Outsourcing to external vendors may involve leasing cloud-based data storage and network systems, as well as contracting a solutions provider to implement video analytics data privacy and security systems. The operator relies on the expertise of the solution provider to develop security rules and policies in accordance with applicable regulatory guidelines.

The solution provider also handles mass implementation of security systems. Operators' representatives generally recognize security solutions providers as seasoned experts in their fields, with staffs dedicated to assessing threats to secure systems, identifying security issues, and reacting rapidly to any security problems.

Mixed Model Approach

Often, operators will opt for a blended system that incorporates internal development, while relying on security solutions providers for implementations. Security strategy is set at the corporate level, while the solutions providers carry out tactical deployments.

In a mixed model approach, the solution provider receives the "best of both worlds."

In many cases, operators understand that solutions providers are the true security experts in the industry, opting for the third-party providers to handle the areas they know best. The solution provider can be highly proactive in assessing and adapting to threats, allowing the operator to focus on its core business of providing video services to its customers.

A mixed model approach is common, according to interviewed operator representatives.

The solution provider can be highly proactive in assessing and adapting to threats, allowing the operator to focus on its core business of providing video services to its customers.

Conclusion

Operators must pay constant attention to data security, not just check in periodically.

Hackers are savvy and organized, and operators indicate their methods evolve too quickly for data security to be a periodic priority. The new complex video ecosystem requires specific knowledge in securing video analytics data over less secure networks. In order to confront threats to data systems, securing those systems must be an ongoing priority, utilizing the latest expertise and most sophisticated tools available.

Consumers take their privacy seriously, and so do operators.

Many operators interviewed are conscious of the importance and at times difficulty of protecting their customers' privacy. With an increased reliance on video analytics data for service-related decisions, ensuring the integrity of the data and trust of the customer has become a board-level responsibility.

Operators understand data security is not necessarily their core business.

With the exception of some of the largest operators, most video service providers opt to lean on external solutions providers to secure their content. Increasingly, operators are also looking to these solutions providers to secure their customers' video analytics data as well.

Ultimately, protecting customer information is not just about protecting the customer but also protecting the operators' investments in video analytics data. **Any security breach reduces customer trust** in their video service provider and reduces the trust of vendors, partners, and advertisers in the ability of an operator to provide valuable analytics information and insight.

Connecting Security to Video Analytics

The value of audience measurement and behavioral data is growing rapidly, as video service providers explore new ways to attract subscribers, increase revenue and differentiate from competitors. Knowing more about subscribers' habits and preferences in close to real-time enables providers to stand out in a highly competitive environment. Aggregated consumption and engagement data can also provide direction and valuable leverage in content licensing negotiations.

Privacy and security are two of the biggest distinct, yet related, topics to consider when implementing an analytics platform because some aspects of the data feeding the analytics can be considered sensitive – and because the more data that is accumulated, the more operators have to consider the implications of breach or loss. Privacy measures will be required to ensure that personal data about user preferences or activities is seen only by people with relevant permissions, which means the data must be effectively anonymized as well as protected from eavesdropping. Security in turn can help enforce privacy rules while also ensuring integrity of the systems involved.

Verimatrix is well placed to meet these challenges through the Verspective™ Intelligence Center, our innovative cloud-based engine designed specifically for pay-TV system deployment, management, monitoring and analytics, with the objective of optimizing performance and reducing operational expenses across the whole video delivery infrastructure.

One very important corollary is that through Verspective, Verimatrix can provide an additional layer of important data that operators and their monitoring systems are otherwise unable to obtain. Because of our "preferred real estate" in the network and devices, our revenue security solutions provide us with a unique capability to gather data—from secure data streams to secure data storage, as well as other infrastructure components. Our solutions are able to see the frame-by-frame experience between the service headend and the client devices.

While other companies that specialize in service analytics have to undertake custom integrations to provide a useful stream of data, Verimatrix provides a complete, extensible infrastructure that is built from the unique position of security in the fabric of service delivery. And as the specialist in video security, Verimatrix is the natural choice to aggregate and curate this potentially sensitive data.

For more information, please visit www.verimatrix.com/verspective

Verimatrix specializes in securing and enhancing revenue for multi-network, multi-screen digital TV services around the globe and is recognized as the global number one in revenue security for connected video devices. The award-winning and independently audited Verimatrix Video Content Authority System (VCAS™) family of solutions enable next-generation video service providers to cost-effectively extend their networks and enable new business models. The company has continued its technical innovation by offering the world's only globally interconnected revenue security platform, Verspective™ Intelligence Center, for automated system optimization and data collection/analytics.

Its unmatched partner ecosystem and close relationship with major studios, broadcasters and standards organizations enables Verimatrix to provide a unique advantage to video business issues beyond content security as operators introduce new services to leverage the proliferation of connected devices. Verimatrix is an ISO 9001:2008 certified company. For more information, please visit www.verimatrix.com, our Pay TV Views blog and follow us @verimatrixinc, Facebook and LinkedIn to join the conversation.

Parks Associates is an internationally recognized market research and consulting company specializing in emerging consumer technology products and services.

The company's expertise includes new media, digital entertainment and gaming, home networks, Internet and television services, digital health, mobile applications and services, consumer electronics, energy management, and home control systems and security. For more information, visit **parksassociates.com** or contact us at **972.490.1113** / **info@parksassociates.com**

About The Author

Glenn Hower, *Research Analyst,* Parks Associates

Glenn Hower currently studies entertainment content and delivery services. Glenn is experienced in entertainment content production and distribution systems with a particular emphasis on radio, television, and film content.

Glenn earned his BA in music with a focus on the music business and industry from the University of Texas at Austin. He earned his MS and MBA from Texas Woman's University in Denton, Texas.

Industry Expertise: TV & Video Content Production, Content Licensing & Distribution, Television Services, Broadband Services, OTT Services, Digital Music

Twitter ID: @GlennatParks

PARKS ASSOCIATES

INTERNATIONAL RESEARCH FIRM

Research & Analysis

for Digital Living Technologies

- Access and Entertainment Services
- Advertising
- Connected CE and Platforms
- Connected Home Systems and Services
- Digital Gaming
- Digital Health
- Digital Home Support Services
- Digital Living Overview
- Digital Media
- Home Energy Management
- Internet of Things
- Mobile and Portable
- App Ecosystem
- Smart Home
- SMB Market
- European and Worldwide Consumer Research

Back your venture *with accurate consumer data and strategic analysis.*

Discover Parks Associates Today.

www.ParksAssociates.com