PARKS ASSOCIATES

Cybersecurity: Turning Necessity into Business Opportunity

A Parks Associates Whitepaper Developed for Alticast

alticast

Cybersecurity: Turning Necessity into Business Opportunity

Operators are transitioning their business models from narrow consumer cases of providing broadband, video, and voice to operating as comprehensive media and technology entities. In addition, **operators are expanding their definition of security from preventing content piracy to securing big data streams and protecting consumer privacy.**

As critical players in the future of the connected home, operators have the opportunity to be leaders in a data-driven economy, while setting an example to be good stewards of consumers' personal data.

The purpose of this whitepaper is to provide an overview of current content security systems and to understand the pain points in the transition from content security to big data security, with an emphasis on real-time threat detection using machine learning. The whitepaper also identifies emerging business opportunities for operators for which intelligent data security plays an integral role.

Almost
one-half of consumers
rank data security and privacy issues
as their greatest concern about
connecting devices to the Internet.
© Parks Associates

Today's Security for Broadband and TV Service Operators

For television and broadband service operators, security has generally referred to securing content provided by programmers and content partners, with emphasis on preventing piracy and unauthorized access.

While content security has its origins in legacy conditional access systems (CAS), which evolved in the digital world to incorporate digital rights management (DRM), securing video content encompassed two main tactics:

Managing access – Through use of CAS and DRM, TV operators tracked customer entitlements to access specific content and either allowed or disallowed the ability to watch the content.

Preventing leaks – Signal piracy has existed in some form since the beginning of broadcasting. Leak prevention generally relied on signal scrambling or encryption so that, even if a malicious party intercepts the signal, the video stream would be unintelligible without the appropriate key to descramble or decrypt the signal.

Digital video systems have made both approaches more feasible by allowing easily deployable software solutions to prevent compromise rather than relying on hardware solutions.

Digital video services also allow consumers to view content with picture and audio quality previously unattainable with legacy analog systems. Digital distribution allows operators the ability to collect and manage customer datasets. However, the digital world has also made it easier for hackers to intercept, compromise, and distribute content illegally. In response, content partners have made security requirements more arduous on video providers.

> Distributing content securely and collecting and protecting data from its customers create several pain points for operators.

Content Security Requirements

With CE device makers and content partners pushing advanced picture technology like 4K resolution and high dynamic range (HDR), content creators and programmers are becoming even more protective of their investments. After all, a poor-quality pirated version of content is damaging to the content provider, but it provides a poor user experience that fewer consumers will tolerate. On the other hand, the damage associated with a leak of the highest quality video from a content provider would be irreparable. In response, motion picture technology consortium MovieLabs released a set of content security requirements for 4K content.

Requirements include the following:

- **Encryption** – Among the requirements is the specification that DRM, devices, and platforms support AES 128-bit encryption or better.
- **Secure computation environment** – The processing environment must be isolated by hardware mechanisms.
- **Hardware root of trust** – The root of trust must be permanently factory burned, meaning content providers must work with OEMs to distribute and screen 4K content meeting MovieLabs' specifications.
- **End-to-end protections** – MovieLabs specifies forensic and playback watermarking as a control measure for breach detection. This requires operators to partner directly with content providers on securing content through its entire distribution structure from origination to delivery.[1]

The enhanced requirements mean operators will need to forge complex partnerships with content providers, industry consortia, CE device makers, and security vendors. With such a complex set of security rules in place, and the possibility that rapid innovation will require additional rule changes, operators will need flexible security systems to institute new specifications to prevent content theft. With rapid changes in entitlements and data permissions, dynamic and adaptable systems to manage ever-changing security requirements will be critical for operators.

[1] Motion Picture Laboratories, Inc. "MovieLabs Specification for Enhanced Content Protection – Version 1.1." February 2015.

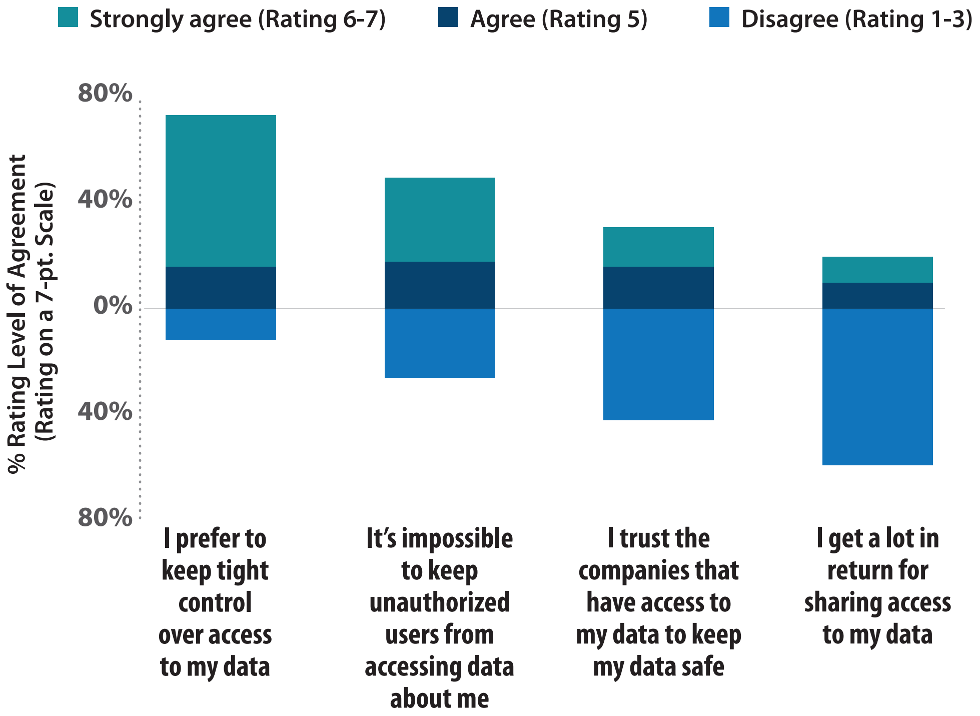
Big Data and Privacy

The rise of the software economy has given operators the ability to collect more information and data than ever before, including customer data, network quality and traffic data, and content asset-specific data. As a result, operators have taken a big data approach to data collection and security. Globally, service operator consolidation has led to a consolidation in cybersecurity systems as well, requiring previously regional and disaggregated cybersecurity groups to align their operations and security protocols. With the increase in data collection and consolidation of data and security functions, consumers have become savvier, and at the same time more wary, of their personal data being collected.

> Consumers are apprehensive towards giving up their personal data, and they are selective of the types of companies they trust.
>
> - 73% of U.S. broadband consumers express a desire to keep tight control over access to their personal data.
> - Only 23% of broadband consumers ranked a pay-TV provider as one of their three most trustworthy companies, and only 5% indicate a pay-TV provider as the most trustworthy company. When compared to consumers who rank a home property or home insurance provider (62%), a security monitoring provider (59%), and an electricity provider (58%), broadband and TV service operators have substantial ground to make up in trustworthiness to the consumer.
> - 24% of consumers agree that they receive a lot in return for sharing access to their data, while the majority do not believe they receive a lot in return. Overall, the digital economy has not done enough to communicate the value proposition for collecting personal data
>
> © Parks Associates

Concerns About Hacking of Smart Products

U.S. Broadband Households

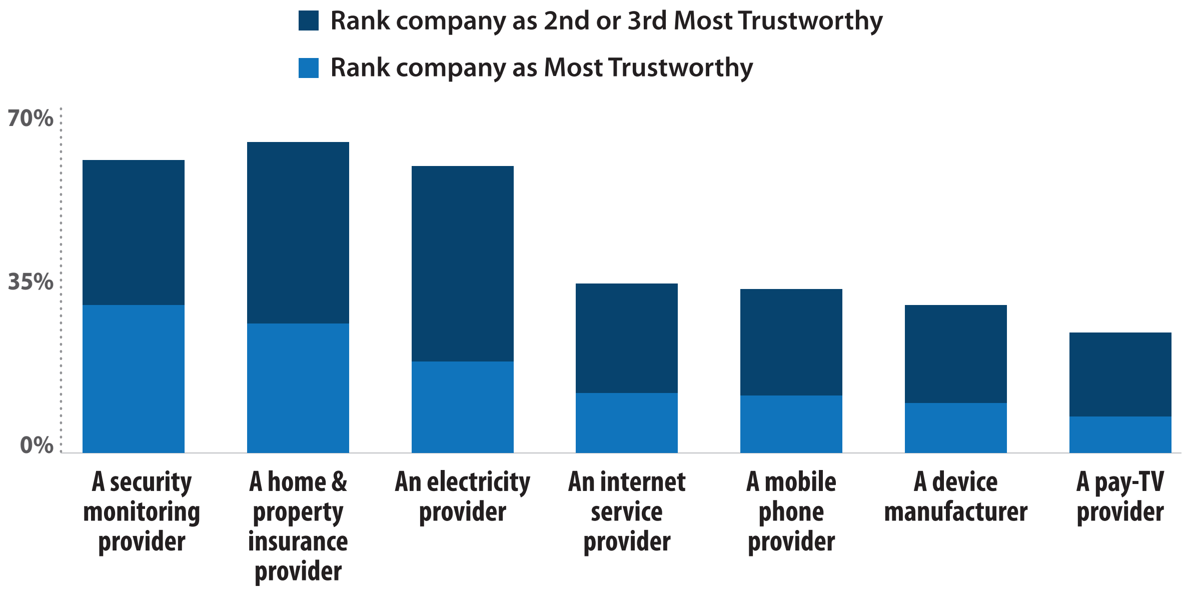


© Parks Associates

Operators may employ several methods to gain trust among consumers and promote the value of sharing personal data.

Trustworthiness of Company Types to Appropriately Access/Manage Personal Data

U.S. Broadband Households



© Parks Associates

From a consumer perspective, data security and data privacy are intertwined: consumers do not want their data stolen, nor do they want their data exploited by companies that have authority to access their data. The issue is control of the data; consumers want a say in who sees their data and how it is used, and operators must be good stewards of consumers' personal data.

Opportunities to Gain Consumer Trust

- **Security system upgrades** – Hackers are constantly changing their methods and exploiting new vulnerabilities in ever-changing systems, so operators must have up-to-date security systems and protocols to detect and mitigate threats. Machine learning and automated threat detection will play a key role in real time security systems in the short and long term.
- **Consumer education** – By and large, consumers are not knowledgeable of the security systems and protocols that protect their information. According to Parks Associates consumer research, consumers have indicated that they are less apprehensive towards giving up their personal data as long as it is protected in some fashion. Operators may gain a greater level of trust with their customers by demonstrating their commitment to data security with consumers and educating consumers on cybersecurity basics.
- **Monetary benefits** – Companies from ecommerce providers like Amazon to life insurance providers have offered discounts to customers willing to divulge personal data. Operators like Comcast have proposed similar measures, offering discounts on broadband access in exchange for personal data access.

By offering consumers a measureable value for their data, operators can more effectively translate the value proposition of their customers' personal data in a big data world.

Cybersecurity as a Cost Center

For operators, content security in particular has largely required intense spending with little tangible return on investment. While the costs of security solutions themselves are an expense, any potential security breach can lead to additional financial implications from legal penalties and fees.

A high-profile breach of consumer data from U.S. operator Cox in 2014 led to the cable company paying a $595,000 fine to the FCC, along with providing one year of free credit monitoring to affected customers.[2]

This was a relatively minor penalty, considering hackers did not gain access to financial or sensitive information. A breach of more sensitive information would result in a more severe financial penalty. The dynamic and ever-changing threats to data and content require autonomous security solutions that can detect, alert, and shut down breaches in real time. Content security has largely been a cost center for operators, deployed out of necessity to satisfy the requirements of content partners. However, in a digital world, the systems that accomplish content security can also accomplish more general cybersecurity applications to bolster operator services in the consumer space.

Machine learning systems will play a key role in automated threat detection by powering A.I. systems that are capable of real time threat alerting and mitigation.

Opportunities for Operators in Deploying Automated Cybersecurity Systems

- **Adaptable systems for reorganized cybersecurity operations** – Many operators are reorganizing their cybersecurity operations into a single consolidated Chief Security Officer group, according to Parks Associates briefings with broadband and pay-TV operators. As operators continue to consolidate their cybersecurity operations, they will need systems that can adapt to changing permissions and protocols.
- **Scalable security in a connected world** – Outsourcing security operations to cloud-based vendors gives operators the ability to scale their data collection operations without the need to invest in building comprehensive data warehouses and cybersecurity systems. At peak access times, operators can easily scale their security capacity on an on-demand basis.
- **Cost reduction** – By investing in automated cybersecurity systems, operators can reduce their OPEX by automating threat detection and mitigation, reducing workforce requirements. In addition, by anticipating and handling security threats, operators will reduce the inevitable support calls that occur with security breaches.

By deploying comprehensive cybersecurity systems with intelligent threat detection, operators can turn their security cost centers into revenue-generating operations through their big data applications.

While the security system and the data it protects transition from a cost to an asset, the real asset is the trust and faith that operators must build with its customers by demonstrating their commitment to protecting their customers' information.

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

Evolving Security Systems into Revenue Opportunities

Data has become a new form of currency both for operators and consumers. Data is necessary for smart devices and services to be smart, and any impact on the trust between consumers and service providers that collect their data will inevitably hinder growth in the smart services economy.

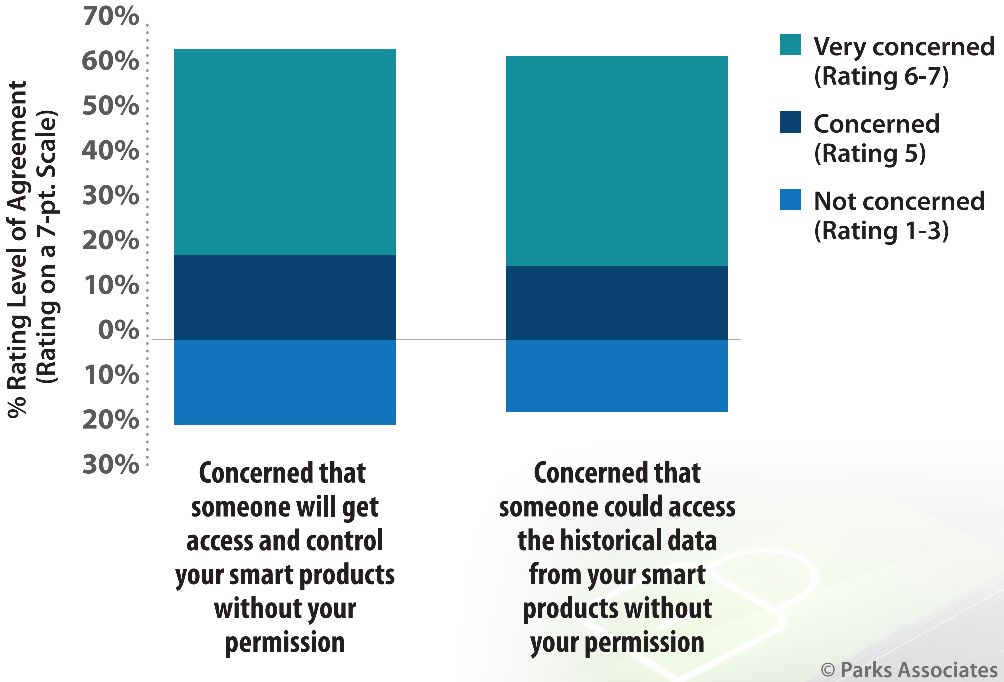
The advantage for broadband, mobile, and pay-TV service operators is that they are positioned to collect large quantities of data as the key gateway into the home and through mobile networks. A prominent challenge in translating this market status into value to consumers is providing peace of mind when it comes to connected living experiences. Most consumers express a level of concern with malicious parties accessing smart home devices and the data the devices provide without authorization.

Among
U.S. broadband consumers,
45%
are very concerned
about people accessing their devices or data without permission.

© Parks Associates

Concerns About Hacking of Smart Products

U.S. Broadband Households



© Parks Associates

Consumer concerns are palpable, and securing the data and devices around a connected home is new territory for many cable and telecom operators.

A security breach involving a content asset is a tangible loss for the content owner, and one for which an operator bears culpability if the breach occurred on its network. A security breach of a consumer's home control devices, however, may put the life of the consumer in danger.

Hacking and disabling connected devices like smart door locks or fire detection systems could lead to catastrophic consequences in a person's home.

Operators face a monumental task in not only translating the value-added services consumers can obtain through connected device and data exchange, but also in building a trust-based relationship with consumers.

With the expanded big data approach to cybersecurity, operators can transition their data security operations from a cost center to being managed as a strategic corporate asset. By incorporating intelligent security detection as an asset, the entire big data and cybersecurity operation becomes intrinsically valuable to the operator, the consumer, and the operator's partners to drive business opportunities in the connected home.

As operators become a greater part of the connected living experience, regulators in the United States aim to put service operators on a more level playing field with large technology companies like Google and Facebook for data collection and use. By incorporating intelligent threat detection and mitigation in their big data systems, operators can work to gain consumer trust of their data.

Supplemental Revenue Streams in Data Security

- **Data partnerships** – Consumer behavior and use of services become a monetizable asset for operators to leverage with product and service partners. Opportunities range from improving quality of experience to aligning relevant promotional and advertising media with consumers.
- **Service upgrades** – By understanding how consumers are engaging with different services on the operator's network, the operator can leverage consumer behavior into incremental revenue streams for upgraded services. This ensures a higher likelihood for consumers to engage in services, and provides relevant opportunities for consumers to expand their service experience with the operator.
- **Support assistance** – In the event there is an interruption in service or a disruption in the quality of service or experience, collected consumer data allows operators to more efficiently diagnose technical issues and cut time and labor on technical support operations.
- **Cloud services** – A secure big data system serves as a market differentiator for operators in marketing cloud services to data partners. This can include serving as a data center provider and white labelling data storage and security services to partners.

Once operators earn and maintain their customers' trust by protecting their devices and data, securing the connected home then becomes a jumping point to connected experiences outside the home.

Security beyond the Connected Home

The low-hanging fruit for leveraging data on mobile experiences is in smartphones, but as vehicles become more interconnected, the connected car presents a new opportunity for operators to have a guiding influence.

As connectivity is added to any and all devices, including vehicles and vehicle control systems, the unauthorized access to the device becomes a greater possibility.

Unauthorized access to location information in a vehicle may expose when consumers are away from their homes. Additionally, the possibility of unauthorized access to a vehicle's control system while in motion is particularly disconcerting.

As with securing the connected home, when a consumer is literally on-the-go, real-time fraud and breach detection and alerting are of utmost importance. A vehicle hack while traveling at highway speeds could result in a life-or-death situation. Extending intelligent security systems through mobility presents an additional growth opportunity for operators that implement comprehensive cybersecurity systems. Operators may also position themselves as innovators and experts in the mobility and connected car data security space.

As connected devices proliferate through connected homes and consumer lifestyles, operators and data gatekeepers must rely on dynamic intelligent threat detection systems to cut through the noise of data over their networks.

> The ability to recognize and handle threats immediately will be invaluable in showing consumers that the operator has their safety in mind.

Demonstrating these abilities provides operators the opportunity to build a trust-based relationship with their customers that is vital in the future of a data-driven economy.

In summation, the increased complexity of content security will force operators to expand cybersecurity capabilities. Security systems must be adaptable and react to threats in real time, which will require artificial intelligence and machine learning systems. Secondly, as big data becomes a vital part of operators' businesses, operators must prove to consumers that they can be trusted stewards of personal information. After investing in comprehensive cybersecurity solutions, operators will do well to educate consumers on the basics of cybersecurity, illustrate how they are protecting consumers, and begin to build a more trusting relationship with consumers. Finally, with comprehensive and effective cybersecurity systems in place, operators can open additional data-based revenue opportunities. Additional opportunities include providing or white labeling data management solutions, as well as pushing business outside the connected home with mobile-based data services and connected car services.

About Alticast

Alticast develops multi-screen solutions that enable service providers to quickly and reliably deliver innovative TV experiences to every customer. Alticast's STB software, CAS/DRM, Cyber Security, Smart UI/UX and Cloud Server solutions are based on non-proprietary software such as HTML5, RDK and GEM. The most deployed digital television provider, Alticast securely brings compelling personalized and interactive content to more than 52 million devices via broadcast, broadband and mobile platforms. The publicly traded company is headquartered in Seoul, South Korea with major offices in Amsterdam, Netherlands, Broomfield, Colorado and Hanoi, Vietnam. For more information, visit **www.alticast.com** and read Alticast's blog, TV Ready Forum, at **www.tvreadyforum.blogspot.com**.

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

Founded in 1986, Parks Associates creates research capital for companies ranging from Fortune 500 to small start-ups through market reports, primary studies, consumer research, custom research, workshops, executive conferences, and annual service subscriptions.

The company's expertise includes the Internet of Things (IoT), digital media and platforms, entertainment and gaming, home networks, Internet and television services, digital health, mobile applications and services, support services, consumer apps, advanced advertising, 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, *Senior 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.

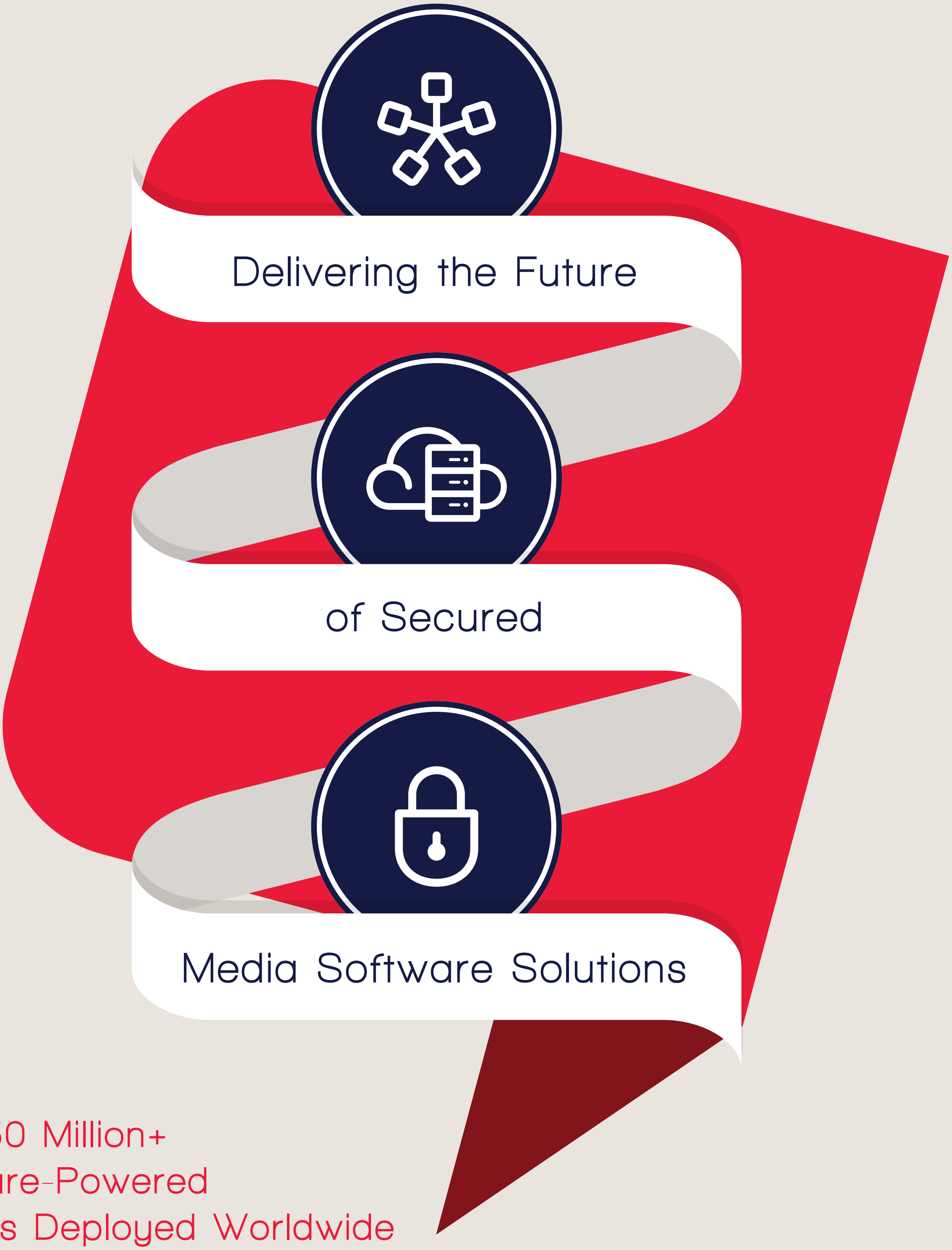
Industry Expertise: TV & Video Content Production, Content Licensing & Distribution, Television Services, Broadband Services, OTT Services, Digital Music

Twitter ID: @GlennatParks

DISCLAIMER—*Parks Associates has made every reasonable effort to ensure that all information in this report is correct. We assume no responsibility for any inadvertent errors.*

alticast

Monetize and Secure Your Business with Argus™



Delivering the Future

of Secured

Media Software Solutions

Over 50 Million+
Software-Powered
Devices Deployed Worldwide