FROST & SULLIVAN

Multi-Faceted Security: Imperative for IP-Powered Video Businesses

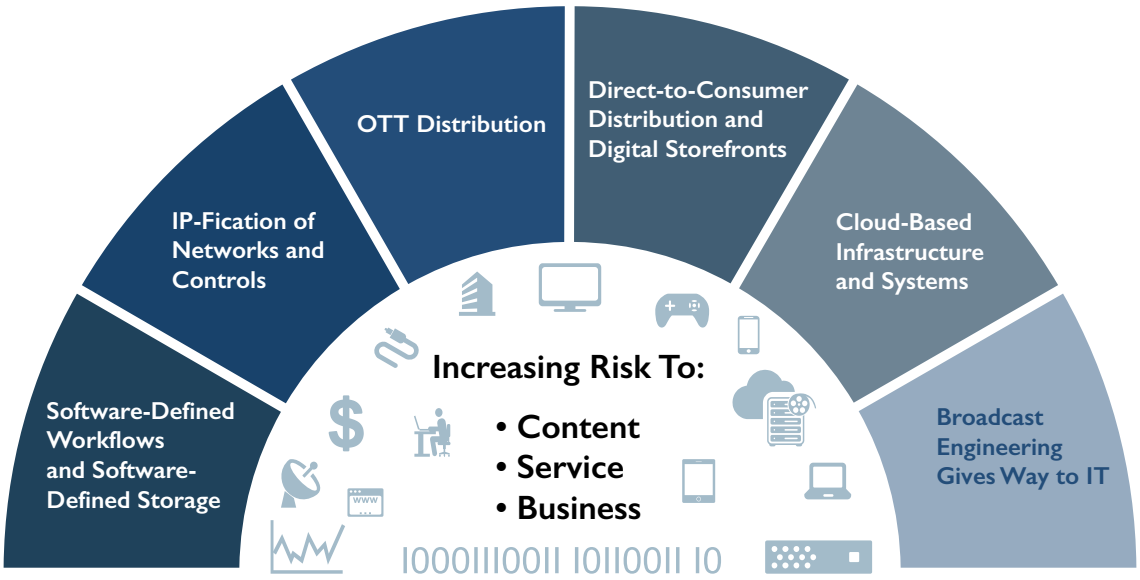
Extend and Integrate Protection beyond the Content to cover Services and the Business

A Frost & Sullivan White Paper

Avni Rambhia, Industry Principal, Digital Transformation

INTRODUCTION

The video content industry is in an exciting phase, characterized simultaneously by both disruption and growth. IP, virtualization and the Internet are transforming media companies such as service providers, video service operators, studios, MVPDs, programmers, and online video providers. This transformation is occurring at both the operational and service levels. At the operational level, networks, storage and workflows are increasingly IP connected and software based. At a service level, TV by appointment and channel bouquets are on the way to on-demand, OTT viewing with corresponding shifts in business models. These changes promise to deliver solid returns in terms of increased agility, higher capacity, higher revenues and improved customer experience. The flip side of the coin is, however, a new set of threats to media companies, the services they provide, and the content they deliver.



Historically, security concerns for media companies have been dominated by piracy of content and hacking of secured players or set-top boxes. Consequently, video security is often equated with protection against service theft or loss of subscription and pay-per-view revenue. Technologies solving the piracy challenge include conditional access and digital rights management technologies, standards for digital cinema encryption, and secure media playback standards such as AACS and SCSA. The bar for CAS and DRM technologies continues to rise. Over and above this, however, the threat landscape is becoming more complex, as IP-enabled and virtualized networks deliver rich hunting grounds to hackers. Less integration of security across components and processes results in decreased effectiveness of any security tools that may be deployed; this results in increased vulnerability. The growing number of successful attacks witnessed by media companies, occurring at rapidly increasing frequency, is as testament to an urgent need for a broader set of tightly integrated cybersecurity tools in order to achieve comprehensive protection.

AN INDUSTRY IS BEING TRANSFORMED

As with all IT-powered businesses, media companies and service providers are susceptible to covert and overt compromises of their internal communication systems, data stores, and external web pages and apps. Accordingly, assets in need of protection now extend beyond finished content ready for external distribution. Target assets for hackers now include internal content such as mezzanine files, dailies, and animation models. Target assets also go beyond any type of video to include internal communication such as emails, databases with transaction and customer information, and more.

The following underlying transformations to video services and workflow implementations are introducing new security challenges for media companies. While each area of transformation delivers clear benefits, it also brings with it an added dimension of risk or vulnerability.

- **Workflows are transitioning to IP:** Media companies making the shift from traditional hardware-based equipment to software-defined workflows and software-defined storage gain flexibility of resource allocation, freedom of vendor choice, and simplified extensibility of networking capacity. With this flexibility and openness, however, comes vulnerability to threats such as ransomware, data theft and denial of service.

- **Processing and delivery is moving into the cloud:** The benefits of cloud-based operations are well understood: lowered CAPEX, predictable OPEX, instant-on-instant-off scalability, deployment in minutes, global collaboration, and freedom from capacity constraints of in-house physical facilities. However, alongside these benefits come risks of network interruption, service outage, data theft, and channel hijacking. While cloud infrastructure providers invest heavily in security of their data centers, there remains significant burden on the content companies themselves to protect ingest and egress sections of the workflow, and to be able to control the spread of any compromise from within the company's firewall into the cloud infrastructure as well.

- **Pay TV services are evolving:** For service providers who are adding skinny bundles, app-based delivery and live streaming, these innovations offer exciting new revenue options but also open new avenues of revenue loss, such as embedding legitimate streams in illegitimate pages to steal ad revenue. Traditional areas such as conditional access are newly challenged by the cost and complexity of building and maintaining adequately secure playback applications for high-resolution, early-window content across a wide, ever-changing range of video-enabled devices and platforms.

- **New direct-to-consumer business models are emerging:** Direct-to-consumer sales of subscription services and pay-per-view content by broadcasters, programmers and even enterprises help counter the effect of falling subscription and advertising. With this promise of new revenue, particularly from the coveted cord-shaving, millennial demographic, comes added responsibilities to safeguard privacy and financial data, and ensure compliance with regulations such as PCI and SOX. For many content companies, this is an unfamiliar and challenging terrain to traverse.

- **The enterprise perimeter is fading:** The transition from SDI to IP dilutes the traditional enterprise perimeter. More open networks and more open APIs make video systems more easily extensible and more virtualization-friendly, but also expand the threat surface of the service provider's infrastructure. This lack of a concrete perimeter results in many more potential attack points on both the content and the systems, whether at the head or at the edge. Everyday tools such as e-mail have become popular vectors for spearfishing attacks; web and network attacks are also plentiful and dangerous. Accordingly, the need to ensure equivalent levels of protection and monitoring of sensitive video data from end to end becomes more critical.

We find that most media companies are still grappling with the complexities of transitioning to IP workflows, cloud-based delivery and multi-screen distribution. Video engineering teams are not fully aware of the many risks that are inevitably incurred while urgently undertaking business-critical infrastructure and service transformations. Too often, business imperatives dominate priorities during design and implementation, while security is often applied as an afterthought. Figuring out how best to stitch together a wide and appropriate range of security tools to cover all these threats is a difficult endeavor, covering uncharted territory. For example, even experienced IT teams find it

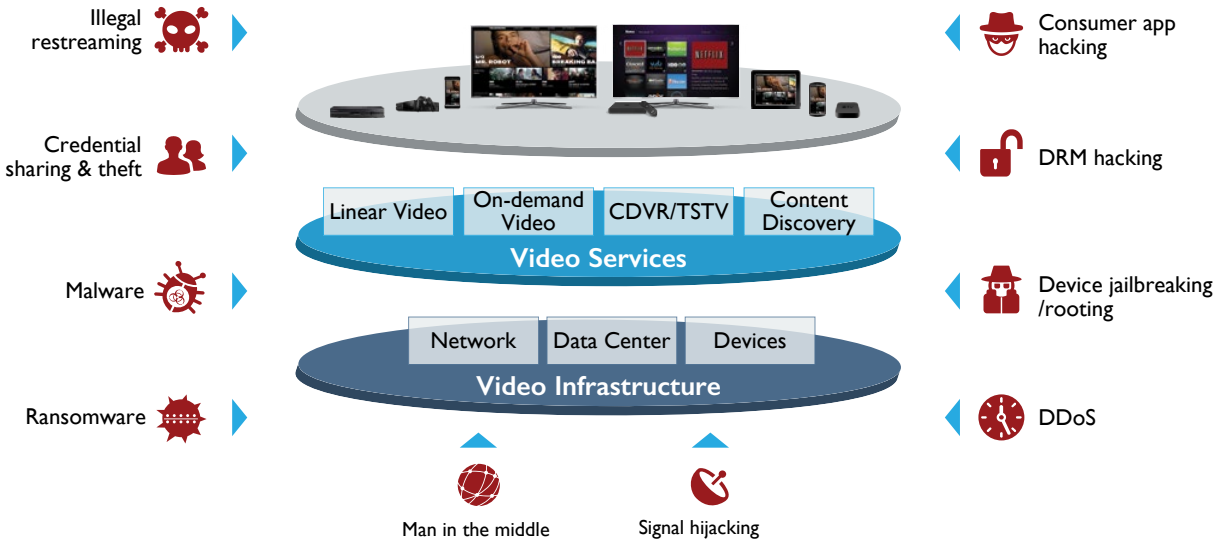
challenging to adapt security tools such as data encryption and data leakage prevention to high-bandwidth, low-latency content workflows while simultaneously preparing for potential distributed denial of services (DDoS) attacks, malware, or emerging threats. To bridge this knowledge gap, we provide a comprehensive discussion of the threat landscape across modern media companies. We further offer an integrated security paradigm, which enables media companies, including service providers, to build out robust and durable protection for all their assets and business processes.

SECURITY CONSIDERATIONS FOR IP-ENABLED MEDIA BUSINESSES

A NEW NORMAL: THE EXPANDING DEFINITION OF SECURITY

As discussed earlier, the primary goal for content protection in the past has been mostly limited to the prevention of unauthorized distribution and uncontrolled use after the content was distributed to viewers. Moving forward, an expanded definition of security for video is needed. This is due to the need to account for new risks affecting the underlying video infrastructure as well as the services, applications and content.

Hackers Will Attack the Weakest Link



Security goals are expanded into three distinct categories:

- **Preventing loss of content:** This includes theft of content during and after distribution, but also the theft of content—and assets related to the content—during production and before distribution. It also goes beyond theft to include corruption or deletion of content and associated data such as metadata tags and closed captioning, whether intentionally by hackers or accidentally by an employee or partner.

- **Preventing disruption of services:** This includes interruption of live and/or on-demand video delivery, as a result of external network-based attacks such as DDoS, botnets, or malware; malicious insider attacks for data theft; or internal attacks including malware installation and data theft after network infiltration. Examples of compromise span accidental overlay of one program's captions on another program's videos, to intentional replacement of broadcast programming by a hacker's video stream. This also includes familiar IT threats against websites such as denial of service, vandalism or defacing, and replacement or insertion of content.

- **Preventing loss of data:** This covers the traditional IT threat of loss of emails, internal documents, customer personally identifiable data and sensitive financial information to overt or covert attackers who may attack for bragging rights, blackmail, or professional cyber theft. In the context of service provider businesses, data also includes information related to the content or to the consumption of the service, such as subscriber viewing history. This data may be directly abused (such as for identity theft) or indirectly abused (for example it may be sold to competitors or other companies to enable targeted advertising).

SECURITY CONSIDERATIONS ACROSS THE WORKFLOW

Any digital video workflow can be divided into three large sections: Creation & Processing, Distribution, and Consumption. We detail the breadth of risks applicable today across these segments as video transforms into an open IP ecosystem. We also discuss security tools typically used to address each risk and the difficulties of applying them naively to video applications.

Video Creation and Processing

Workflows are transforming from relatively protected appliance-based architectures to more open software-based implementations. They may be deployed in private data centers or, increasingly, in the public cloud. As this transformation continues, the attack surface for loss of data and disruption of workflows is growing.

Insider attacks, where data is directly moved to unsecured portable media or Internet ports are opened to ease external access to data, are worrisome. Traditional attacks such as malware exploits, phishing, and password guessing can also be used by external hackers to gain access to networks and covertly siphon off data for extended durations of time. Attacks can be executed through ransomware, by disgruntled insiders, or through inadvertent personnel error. Where companies outsource production tasks or when workflows involve multiple distributed teams collaborating in the cloud, the severity of these vulnerabilities is determined by the least secure link in the chain.

Traditionally, data encryption and access control lists (ACLs) are widely employed to protect sensitive data within networks. Authentication securely establishes identity, and access control determines the proper rights for a given identity to a given set of content and data. While the use of encryption to enforce access control policies can work well for text documents and images, it imposes unreasonable overhead on an uncompressed HD stream and can easily interfere with latency and throughput of demanding scenarios such as contribution. Similarly, data leakage prevention solutions would be hard-pressed to differentiate sensitive from routine traffic across gigabits-per-second volumes of compressed video.

Network segmentation is an additional layer of protection, where silos are created across unrelated functions to contain damage from exploits such as escalation of privileges. For example, the U.S.-based retail chain Target was exploited this way. For many media companies that have transitioned to modern IP infrastructures, or are in the process of doing so, the focus tends to be more on functionality and uptime rather than security. Consequently, there are often oversights such as lack of proper network segmentation. This tendency attracts hackers, since one successful incident of network invasion or elevation of privilege can be quickly leveraged across the entire business to compromise many connected systems and reach many content repositories. This escalation is particularly problematic for traditional media businesses where security hygiene and sophistication tends to trail the maturity found in other types of businesses that are much further ahead in the digital transformation lifecycle.

For example, poor password hygiene (such as use of common passwords or failure to change default passwords) dramatically increases the likelihood of a successful and catastrophic exploit. Inexperienced users with administrator privileges are also more vulnerable to generic phishing and targeted password discovery (i.e., spearfishing/spear phishing) attacks. For hackers in unsegmented networks, even a single foothold within the network is enough to

hone in on specific targets such as high-value content titles or coveted email accounts. Once a hacker is inside the network, a company's ability to contain damage and limit theft becomes extremely limited. Hackers are adept at quickly fingerprinting networks and probing infrastructure to find rewarding targets such as content on video playback servers, credit card information on billing servers and personal customer data on OSS/BSS/CRM systems. In a recent attack on Sony's networks, for example, attackers went straight for the premium content—it was clear that they knew exactly what they were looking for and were able to find it and pull the data relatively easily. The adverse impact from the exploit included millions of dollars in lost content revenue as well as significant adverse publicity and loss of consumer trust.

Context-aware protection solutions, which are aware of typical data patterns resulting from workflows, can be far more effective at catching potential compromises early and flagging them with a higher degree of accuracy. Network topologies, which inherently restrict the ability of unrelated workflow components from talking to each other, can also help quarantine the impact of a succession invasion. Professional security services can also assist with least-privilege best practices to ensure that even when networks are invaded, damage and access are as closely contained as possible. Correlation between client-side security measures, such as forensics or usage analytics, and server-side metrics, such as stream authorization, can help discover and flag emerging forms of content loss such as password sharing, stream capture, and more. Traditional Conditional Access System (CAS) solutions can be leveraged, with some modification, to augment network security tools for protecting content in digital networks during primary and secondary backhaul, and in storage.

Video Distribution

Video distribution encompasses many scenarios—primary distribution of programming feeds to cable plants, live-linear distribution of Pay TV content to set-top boxes, OTT live streams, on-demand content streaming, pay-per-view content download and ad-supported streaming being just a few examples. As distribution increasingly occurs through the cloud to a community of apps and browsers on consumer-owned devices, the number of attack vectors for loss of content and disruption of services and workflows is that much larger and evolves that much more quickly.

Denial of service (DoS) and distributed denial of service (DDoS) are the most pertinent threats in this area. Certainly, these can be inadvertently caused when there is inadequate server capacity to meet a sudden surge in demand, and there is inadequate provision to roll the overflow demand over to a cloud-based alternative. However, malicious denial of service is also a real threat. Video signal hijacking is an emerging threat as live streams are delivered by a growing number of broadcasters and sports programmers over the open Internet. For example, TV5 Monde saw a multi-pronged coordinated attack across its website, social media page and 12 live channels. The attack took several hours to resolve. During this time, hackers were able to stream their own content over all 12 of TV5 Monde's online channels. This attack not only resulted in millions of dollars of lost revenue, but presented a worrisome breach of the company's critical infrastructure.

Storage servers are an attractive, payload-rich target for hackers. Conventional storage structures such as Oracle or SQL databases are familiar targets for hackers. Software-defined storage, which is increasingly popular for data-intensive video applications, provides additional threat vectors for hackers while introducing even more complexity for content companies.

Many state-of-the-art tools are available for network and server protection. An important characteristic needed for OTT service protection is rapid detection, root-cause analysis (forensics), and remediation. Future-proofing is also crucial as unknown attacks will emerge over time, and new vulnerabilities will be discovered and exploited. Therefore, a multi-layered approach to security is necessary to limit the likelihood of success when a new attack surfaces—which will inevitably happen.

Video Consumption

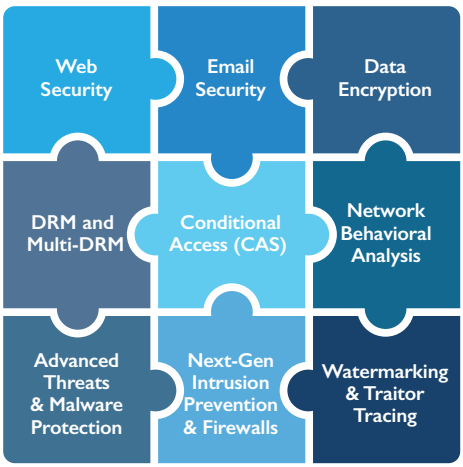
Security during video consumption is familiar terrain for media companies. Even here, however, disruptive changes are afoot. In traditional content protection scenarios, the security bar is being raised by the advent of UltraHD and High Dynamic Range (HDR) content. Techniques such as watermarking and hardware-secured playback paths will be increasingly required. Staying aware of upcoming changes and ongoing hacks is an onerous task, and one that is often best achieved in partnership with a security expert. New challenges for securing media during playback on CE devices include rooted and jailbroken phones, virtualized apps, and other hazards that do not arise in managed set-top box playback situations. Proliferation of broadband also lends new potency to well-known exploits such as frame-grabbing of Pay TV streams from set-top boxes, followed by global, uncontrolled Internet-based redistribution.

Loss of revenue can happen in more varied ways today than simply via theft of content. For example, ad-supported services suffer from the vulnerability that a legitimate stream can be embedded in a pirate's website. While the content company pays for content licensing, processing and delivery, it is the pirates who pocket the corresponding advertising revenue. Thus, secure players now need to make more diverse checks such as ensuring that advertising streams and media manifests have not been manipulated, and that the display page is legitimate.

That said, we emphasize again that security is only as strong as the weakest link in the chain, and the weakest link in content companies is increasingly likely to rest within the previous two categories rather than in the playback segment. For example, in the case of piracy and uncontrolled distribution of a set of 4K content from Netflix, the original content was stolen from within the company's network. Hackers did not even have to tap into the distributed content streams. The impact of successful attacks occurring further and further upstream is that the accuracy of attacks increases, one single attack can compromise a rich haul of targets, and the quality of content captured is typically much higher than what is available from more downstream attacks.

Tying it all Together

A modern media company's security strategy must encompass many building blocks. The solution has to go beyond familiar content protection technologies such as CAS and digital rights management (DRM), to further include familiar IT security technologies such as next-generation firewalls, data leakage prevention systems, next-generation intrusion detection/prevention systems, and advanced breach detection and sandbox technologies. These two disparate security disciplines (content versus IT) must be stitched together to provide effective protection that is compliant with the high throughput and content volume demands of video applications while delivering the level of security required for valuable content business assets, which include, but are not limited to, video assets. Each security product must be compatible with fixed as well as virtualized (or software-defined) deployment scenarios.



Traditionally, there are tens of vendors—each specializing in a particular security product—that each sell their individual product or point solutions. The company's IT team would then be responsible for integrating the individual products into the workflows and infrastructure, in partnership with the broadcast engineering team. In practice, integration is rarely perfect and thus exploitable gaps and cracks remain. As proof, a recent survey published by CommunicAsia showed that within the global cable industry, nearly all vendors had firewalls and traditional end point security in place. At the same time, nearly two-thirds of respondents indicated they had been victims of some type of compromise. This exemplifies how comprehensive security remains a significant unsolved problem for content companies.

Media companies also have to go one step further in their security mindset. Just as companies need to step away from thinking about point products for video processing and moving toward holistic workflow solutions, the same applies to security. Service providers need to move away from a tool-based security mindset, which entails a laundry list of individual products such as DRM for devices, watermarking for traitor tracing, encryption for data security and firewalls for perimeter protection. Rather, companies must think of security as a holistic solution that infiltrates and envelops the whole video delivery architecture from the infrastructure all the way to the video services, apps and content. This transformation of mindset is the first step toward embracing a holistic security paradigm.

The onus for delivering these types of solutions rests with the vendors of security solutions and video technology solutions. With cyberattacks becoming stealthier, more sophisticated and more targeted every day, comprehensive security will become an increasingly hard problem to solve. Vendors who embrace this unified architectural view, with a tightly integrated and multi-layered architectural approach, are leading the charge to establish this new security-centric mindset and therefore help media companies and service providers brace themselves for the ongoing security challenge.

NEED OF THE HOUR: A UNIFIED, CONTENT-AWARE SECURITY APPROACH

Media and service provider companies cannot overcome today's and tomorrow's video security challenges by naively stringing different point product solutions together. Traditional network security tools cannot be directly applied to the video ecosystem; imagine, for example, the futility of securing a real-time 4K contribution stream via a HTTPS connection. Maintaining productivity while ensuring security is always hard, but it's particularly troublesome for the data-intensive video processing industry. Fulfilling the terms of service-level agreements (SLAs) for millions of users with a wide range of devices and platforms is similarly a non-trivial complication that layers itself over fundamental app security and tamper protection requirements.

Consequently, media companies find that they need to integrate each security component deliberately, in a **video-aware manner.** The key to success is to deeply integrate components, in a context-aware manner, with each other and with the workflows and services as a whole. In order to close all the gaps, constrict the impact of attacks and effectively remediate potential exploits, these characteristics are ideal:

- A unified view and tightly integrated implementation of multiple security layers, including the ability to properly configure and maintain all controls through a consolidated user interface.
- Global context, global visibility, internal separation of roles and privileges, and the ability to signal potential local flags globally.
- Individual security technologies pre-adapted to video workflow scenarios and pre-integrated with each other to work in a unified, consistent manner with no gaps, right out of the box. Proper integration, correct configuration and correct maintenance are all crucial to ongoing security hygiene, as an improperly implemented tool cannot provide effective protection.
- Cybersecurity and video piracy intelligence to complement technology and tools for enhanced protection, and to serve as key input to continually enhance such tools to address the latest threats.

Given the plethora of threats and tools, the present approach of selecting best-of-breed products from individual vendors and cobbling them all together is not effective. Selecting individual technologies and vendors, and stitching all those components together to try and get complete coverage, is an inherently complex and unproductive endeavor. Moreover, companies frequently underestimate the ongoing challenge of keeping all these individual tools updated and in sync with each other.

Media companies must ensure they have a unified solution provider who can deliver each of these individual components, but in a way that they are pre-designed to fit in with each other and provide production-grade security for these highly demanding applications.

There is a critical unmet need in the industry for vendors who blend IT security expertise with expertise in broadcast engineering and video service operator use cases. Having an appreciation for both aspects of the challenge, and holding the expertise to solve difficult security challenges without jeopardizing demanding performance constraints, is the need of the hour. Media companies are already overwhelmed with the complexities of transitioning to IP networks and monetizing OTT content; attempting all this aggregation and integration on their own is unadvisable and theoretically unnecessary. Media companies are experts at content; they should focus on their distinctive competency while strategically relying on partners who provide robust, outcome-based security solutions as their distinctive competency. Risks to the DIY approach include unmitigated vulnerabilities and difficulty in maintaining and enhancing the architecture over time. As with most security situations, we find it far more advisable to partner with a proactive vendor who offers a comprehensive and integrated portfolio of security solutions that deliver outcomes (not products) and are optimized for modern content companies.

THE VISION OF CISCO

Cisco Systems is in the unique position of having decades of experience in video infrastructure, IP infrastructure, and security in both realms. The company is a leading provider of traditional broadcast engineering, modern multi-screen and cloud-based workflows, and a leading provider of Internet and IP infrastructure. Cloud computing and virtualization are an integral part of Cisco's DNA. As such, the company is well positioned to deliver best-in-class security solutions as characterized above.

Cisco maintains a holistic perspective on security, and it already operates a full portfolio of products and services on both the security and video fronts. The company is continually enhancing its security portfolio by building and buying relevant technologies.

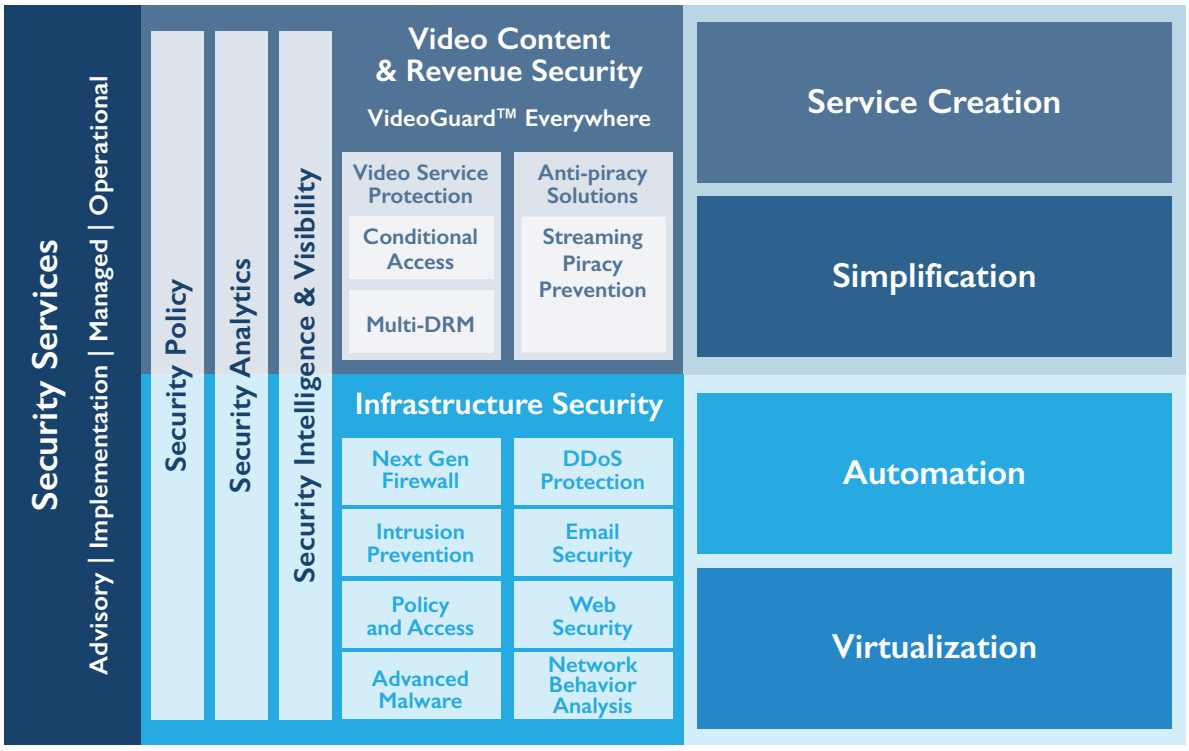
Cisco is proactively committed to adapting and integrating products together for video-specific implementations, while working continuously to discover new security holes and build solutions to fill those holes. As a result, clients are freed from struggling individually, while also achieving more robust protection across the entire workflow.

As an example of how Cisco is applying and integrating IT security products for video systems, the company offers the ability to segment a video backend environment through TrustSec into different functions, such as transcoding, encryption, storage, and so forth, and thus prevent access to one silo by enabling access to the others. As a technology example, NetFlow monitors network traffic on a device-by-device basis and enables intelligent models of "normal" network behavior to be established. On top of this, another component called Stealthwatch digests this firehose of information to provide a powerful, context-rich tool for identifying and diagnosing network problems. Because Stealthwatch relies on data flow analysis rather than packet inspection, it is inherently suited for video applications. These automated monitoring layers watch flows of data between components and flag anomalies of traffic as potential attacks. As an example of multi-faceted DDoS protection, Cisco partners with Arbor Networks to protect against high bandwidth or volumetric attacks at the network edge, while partnering with Radware to block against App- or Service-related DDoS attacks between apps and headend networks to secure backend infrastructure. These

are compelling examples of how architects from security and video sides of the company are proactively coming together to ensure that individual components are optimized or adjusted to work well together. Cisco's high-throughput network security services are compatible with video ingest and collaboration applications; for example, the Firepower 9300 appliance offers Tbps-level firewall as well as high-performance, next-generation firewall, VPN, next-generation IPS, and advanced malware services to lock down the network perimeter with granular access control over as well as enhanced visibility and control across the video broadcast and media infrastructure to stop known and potential threats before they can cause damage.

On the more familiar video security side, Cisco is also taking a comprehensive and innovative approach to addressing new forms of piracy. For example, in order to help curb the growing problem of illegal redistribution of live events such as sports, Cisco has developed VideoGuard Everywhere Streaming Piracy Prevention, a solution built on multiple services and technologies that work together to locate pirate sites and networks, identify source devices responsible for the leaks and enact a blocking of the source devices, all in real time.

This represents an early stage in the latest evolution of Cisco's industry-leading video security efforts, and it is already breaking the status quo for media company and service provider security. Over time, we expect that deeper integration of security intelligence and analytics will be achieved. This will, in turn, allow components to work even more effectively in tandem to protect video content, services and businesses. As shown in the figure below, Cisco positions itself as a partner rather than a vendor through a combination of point products, professional solutions and expert thought leadership. This is welcome news for media companies struggling to cope with expanding security challenges.



CONCLUSION

As content companies embrace the potential of IP and the promise of OTT, they tap into significant new opportunities for savings and growth. On the flip side, however, new security challenges arise and the range of threat vectors and attack surfaces open up tremendously. While content companies do and should continue to rely on familiar CAS and DRM technologies for content protection, these are no longer enough. Security challenges that are typically familiar to IT professionals are becoming relevant to the media and video service provider realm. The problem is that a point-product approach for individual security threats or requirements will not provide the comprehensive security coverage needed by the modern IP-based media company. Further, security tools cannot be naively applied to secure video workflows or protect content services. Compressed video data has no reliable semantics or signatures, and uncompressed video is massive in size. Real-time performance is crucial.

Media companies are typically not equipped to acquire and integrate individual components such as next-generation firewalls, VPNs, web security, email protection appliances, data leakage prevention systems, identity services, policy and access, network behavioral analysis, next-generation intrusion prevention systems, anti-malware protection, DDoS mitigation, multi-DRM, watermarking, password share detection, forensics, "malvertising" detection and data encryption. Simple patchworks of security are not effective at protecting against determined attackers. A unified security paradigm is critical to ensuring a composite, unified whole security solution that minimizes exploitable gaps. It also reduces operational cost and complexity, making the security program more sustainable over time. The market demands unified security solution providers that can optimize each component for demanding video applications and deeply integrate each component. Fortunately, vendors such as Cisco are bringing their dual security and video expertise to bear on the problem, boding extremely well for media companies, including video service operators, broadcasters and online video service providers.

NEXT STEPS

Schedule a meeting with our global team to experience our thought leadership and to integrate your ideas, opportunities and challenges into the discussion.

Interested in learning more about the topics covered in this white paper? Call us at 877.GoFrost and reference the paper you're interested in. We'll have an analyst get in touch with you.

Visit our **Digital Transformation** web page.

Attend one of our **Growth Innovation & Leadership (GIL)** events to unearth hidden growth opportunities.

SILICON VALLEY
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

SAN ANTONIO
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

LONDON
Floor 3 - Building 5,
Chiswick Business Park,
566 Chiswick High Road,
London W4 5YF
Tel +44 (0)20 8996 8500
Fax +44 (0)20 8994 1389

877.GoFrost
myfrost@frost.com
www.frost.com

Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding permission, write:
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041