Akamai

THE STATE OF MEDIA SECURITY

HOW MEDIA COMPANIES ARE SECURING THEIR ONLINE PROPERTIES

TABLE OF CONTENTS

INTRODUCTION

For media companies, the over-the-top (OTT) content opportunity is larger than ever and is projected to continue its rapid growth in the coming years as more viewers are "cutting the cord" and consuming their TV over the Internet. These organizations have the opportunity to not only replace traditional TV, but to provide a better-than-TV experience through personalization and other online-based innovations. In order to take advantage of this tremendous opportunity, broadcasters and OTT providers need to deliver flawless, uninterrupted viewing experiences to each and every one of their viewers. A key part of delivering that viewer experience will be securing it; not only the content itself, but perhaps more importantly, your applications, sites, and data, as the amount of cyber-attacks continues to grow.

A survey of almost 200 media technology influencers and decision-makers by BizTechInsights on behalf of Akamai Technologies reveals the most common types of attacks organizations are facing, the measures they are taking to protect against them, their biggest security concerns, and more.

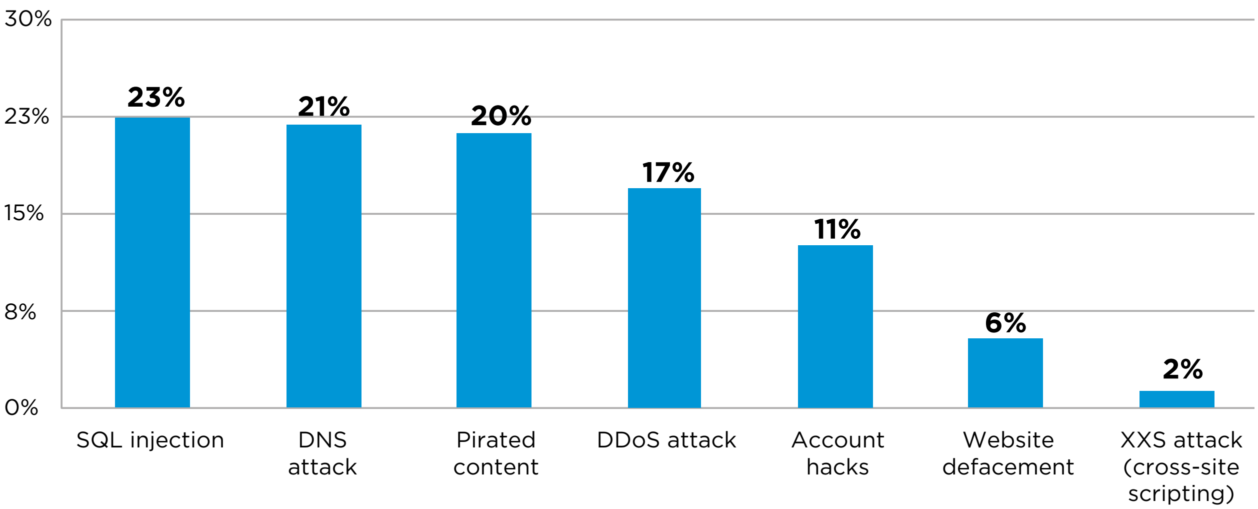
SURVEY FINDINGS

Recent Breaches Span a Broad Spectrum

Security breaches that go beyond stealing premium content are a real and present danger for media organizations. Attacks are widespread and of different types. The four most frequent breaches in the survey were SQL injections (23%), DNS attacks (21%), content pirating (20%), and DDoS (17%). These findings show that organizations must be prepared for a large variety of attacks.

> Breaches that go beyond stealing premium content are a real and present danger.

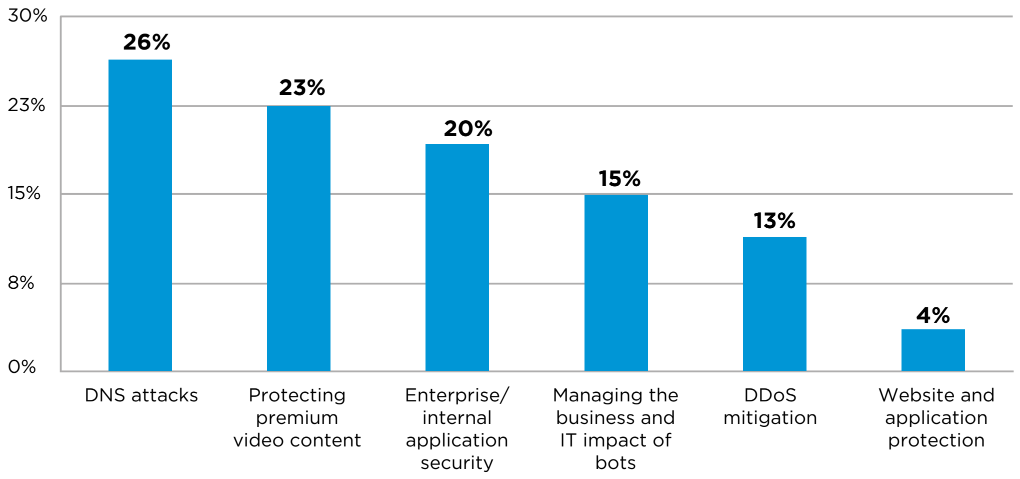
Figure 1: Which security breach has your organization recently experienced?



Site Downtime and Enterprise Application Security Are the Greatest Concerns

It's no secret to media leaders that threats are multiplying across all vectors and growing in size. Reflecting the prevalence of security breaches in the preceding chart, 26% of respondents indicated that slow site performance or downtime due to DNS attacks are their number one concern, while another 17% chose DDoS mitigation and site/application protection. These findings are not surprising as viewers cannot consume your content if it is not available. The second highest area of concern was protecting premium video content (23%). Interestingly, enterprise applications was the third most common concern. Next in the survey was managing the business impact of bots (15%).

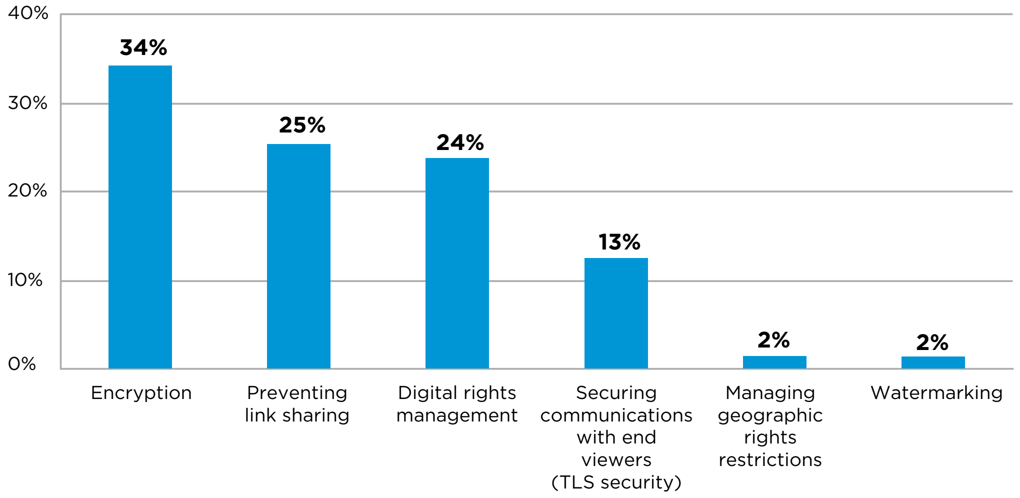
Figure 2: What are your biggest concerns when it comes to securing your online video business?



Premium Content is Key to a Successful Video Strategy, But it Must be Protected

For businesses to profitably provide premium video content, they should employ an ongoing process to protect it against unauthorized usage and distribution. In this endeavor, organizations face challenges in implementing technologies to assert control over access and usage. Encryption (34%) ranked as the top challenge, while preventing link sharing (25%) and digital rights management (24%) were second and third, respectively.

Figure 3: When it comes to protecting your premium content, what are your organization's biggest challenges?

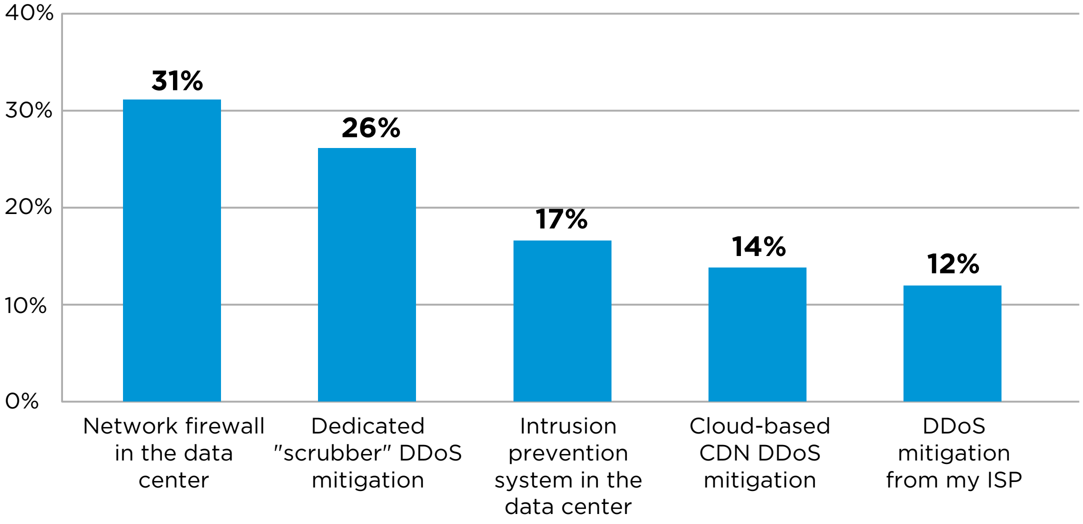


Media Companies Lag Behind Other Industries in Using Cloud Solutions to Defend Against DDoS Attacks

Organizations are pursuing several technology strategies in order to protect against DDoS attacks -- a high priority as previously noted. The defensive measure most frequently cited was the use of a network firewall in the data center (31%). The use of a dedicated "scrubber" DDoS mitigation solution (26%) was a close second while utilizing an intrusion prevention system in the data center (17%) was the third most popular measure. Surprisingly, only 14% of respondents indicated they are using cloud-based CDN DDoS mitigation, a method that has been more widely adopted in other industries.

Only 14% are using cloud-based CDN DDoS mitigation, which has been more widely adopted in other industries.

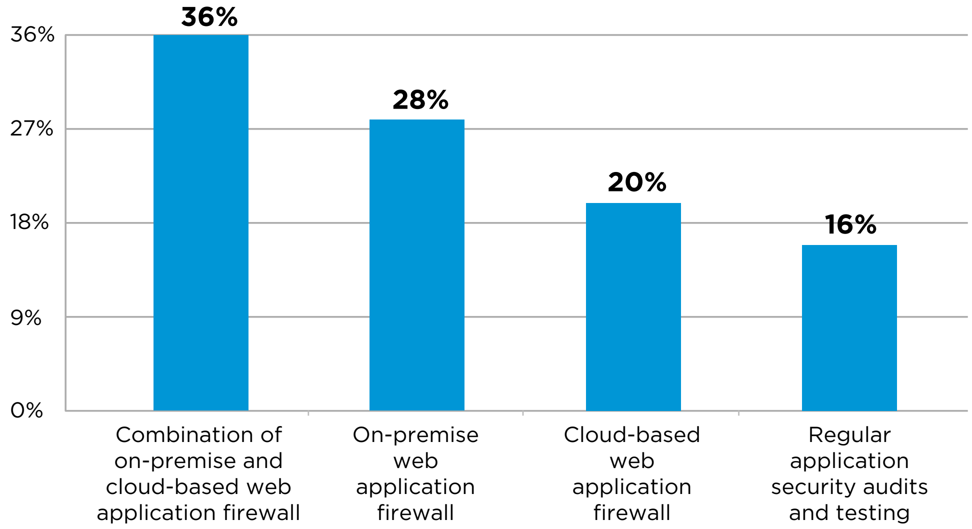
Figure 4: Describe your organization's strategy around protecting your online video business from DDoS attacks.



Defending Against Web Application Attacks with Cloud and On-Premise Firewalls

The majority of survey respondents indicated they are using a cloud-based web application firewall and 36% of respondents indicated they use on-premise measures in addition to cloud-based protections. 28% of respondents indicated that they only rely on an on-premise web application firewall while 20% said that they only use cloud-based web application firewalls.

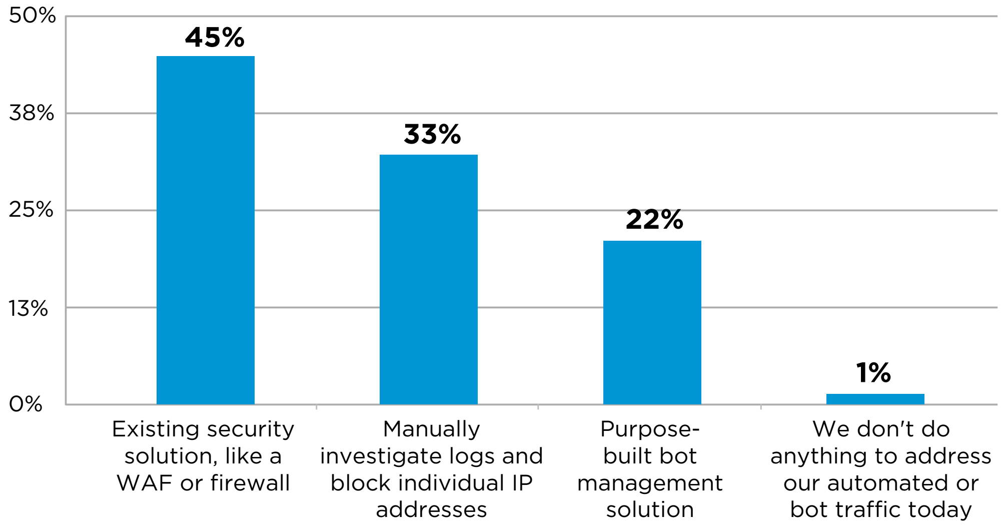
Figure 5: Describe how your online video business protects against web application attacks.



Dealing With Automated or Bot Traffic

Non-human agents, or bots, make up a large percentage of today's Internet traffic. Some of these bots are beneficial to your business while others can cause serious damage. Some bots can exploit stolen credentials to circumvent subscriptions while others could scrape your sites to steal content and sensitive data. Because of this, organizations need to manage bots, not completely block them. Of survey respondents, 22% are using a purpose-built bot management solution while 33% are manually investigating logs to manage bots.

Figure 6: How do you address automated or bot traffic today?

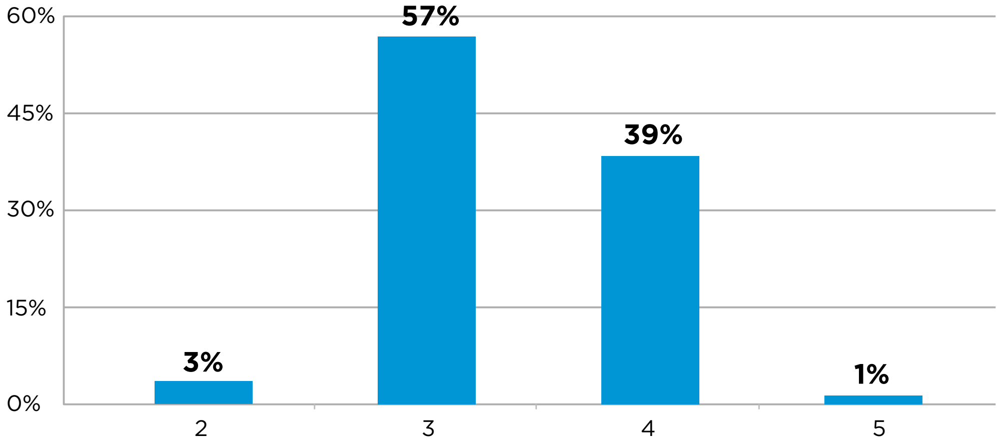


Media Organizations are Not Completely Confident in Their Current Security Measures

Only 1% of survey respondents indicated they are "very confident" in their current security measures and over half seem to be on the fence about whether or not they are fully prepared to protect against today's threats. Another 3% indicated they are not very confident in their current security measures. A healthy dose of skepticism and always striving to improve security measures are necessary as cyber-attacks become larger and more publicized. It seems that every month an attack makes global news, causing severe damage both to brands and consumers.

Only 1% are "very confident" in their current security measures.

Figure 7: How confident are you that your organization's current security measures provide sufficient protection against today's web threats [Rate on a scale of 1-5; 1=not confident, 5=very confident]?



CONCLUSION

As the number and variety of cyber-attacks increase, media organizations need to take measures to protect their entire online business, not just their video streams. Survey respondents recently have suffered seven different types of security breaches, with SQL injections, DNS attacks, content pirating and DDoS attacks leading the way.

Media companies appear to be aware of these threats and are taking steps to mitigate the risks they face. However, they are not yet confident the solutions they have put in place are sufficient to address the risks to their businesses -- only 1% of survey respondents indicated they were “very confident” in their current security measures. Such a gap indicates media companies will remain vulnerable to attackers until they employ strong security measures across their entire online ecosystem.

For media companies, solving the security challenge means establishing processes, communications and programs, not merely deploying a single-point-in-time solution. Other industries have addressed security by establishing industry forums, education seminars and close links to governmental security agencies. Such measures enable industry players to be well informed about the latest security challenges and solutions, giving them confidence in the particular security solution they have chosen to deploy. A similar industry community and communication system is developing among media companies and likewise will help bring awareness and confidence. ■

About Akamai

As the world's largest and most trusted cloud delivery platform, Akamai makes it easier for its customers to provide the best and most secure digital experiences on any device, anytime, anywhere. Akamai's massively distributed platform is unparalleled in scale with over 200,000 servers across 130 countries, giving customers superior performance and threat protection. Akamai's portfolio of web and mobile performance, cloud security, enterprise access, and video delivery solutions are supported by exceptional customer service and 24/7 monitoring. To learn why the top financial institutions, e-commerce leaders, media & entertainment providers, and government organizations trust Akamai, please visit www.akamai.com, blogs.akamai.com, or @Akamai on Twitter.