WHITE PAPER

Protecting the Media and Entertainment Industry With the Fortinet Security Fabric

Executive Summary

Media and entertainment (M&E) firms are increasingly vulnerable to cybercrime. Breaches and hacks against firms can result in compromised emails, early release of films or transcripts, and diminished employee productivity due to system downtime. Protecting content and intellectual property (IP) is at the forefront of the M&E industry. Yet, the risk does not stop there. When content is compromised as a result of a cyberattack, the companies face myriad implications.

Operational disruptions and downtime can cause delays in filming and post-production, impact back-office administrative and financial productivity, and even inhibit customer experiences—all of which can result in impacted revenue. Further, the risk of tarnished brand reputation as the result of stolen customer and employee data remains a threat.

The Fortinet Security Fabric addresses the protection of assets and information with a broad, integrated, and automated approach that is tailored to the needs of this rapidly evolving industry. With cybersecurity solutions that span corporate infrastructure, branch locations, customer experience, and content protection, M&E firms can secure both systems and data from bad actors, and in doing so, their bottom lines.

Though many attacks go unreported, cyber threats against entertainment and media companies are growing.

The average cost of a typical data breach is $4.24 million.

Key Media and Entertainment Cybersecurity Challenges

While the M&E industry faces a unique set of challenges when it comes to protecting content—files, scripts, music, films—the sector must also grapple with the same cybersecurity issues as any other consumer-facing organization. These firms must have secure networks that protect their intellectual property as well as critical employee and consumer data. At the same time, these networks must meet the high-performance demands of customers and employees, while enabling connectivity across distributed locations.

In addition, digital innovations that enhance customer experience such as cloud-based services, Internet-of-Things (IoT) devices, and mobile networks must be readily available and secure—protected against both known and unknown threats. Any network downtime can hinder customer experience and negatively impact revenue and brand reputation. All the while, firms must ensure customer data is protected and demonstrate compliance to regulations such as the EU's General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS), and the Payment Card Industry Software Security Framework (PCI SSF).

Further, many M&E organizations operate in fragmented silos, creating operational inefficiencies across the entire network that hinder cybersecurity and other business functions. Firms often lack the integrated visibility of all of their devices and services across their expanded attack surface, which creates new vulnerabilities.

It can be difficult for M&E firms to find qualified cybersecurity personnel who are equipped to deliver the unified, high-performance, secure networking capabilities that this industry requires. While serious cyberattacks targeting entertainment IP are on the rise,[1] and the average cost of a data breach reached an all-time high of $4.24 million last year,[2] it is clear that the M&E industry needs a new approach to protecting business-critical data and intellectual property. An integrated, automated approach to security can help prevent advanced threats, break down silos, and bridge the growing cybersecurity skills gap.[3]

Cybersecurity Use Cases

The above challenges break across various use cases for the industry:

Corporate infrastrature

Sophisticated technology increases the entertainment industry's online footprint and thus makes it more susceptible to remote compromise.[4] Corporate infrastructure for M&E companies consists of IT services that support data for finance, HR, sales, and marketing—housing valuable IP. In addition, these networks must support employee and third-party supplier mobile and IoT devices, as well as deliver web and mobile applications for external customer experiences. Protecting corporate systems and assets is critical to the success of each firm, but new, complex, distributed networks in the face of advanced threats make achieving end-to-end security increasingly difficult.

Media and technology firms need to protect their corporate infrastructure by breaking down silos via a simplified, integrated security architecture. The Fortinet Security Fabric enables companies to protect their entire infrastructure through centralized visibility and control, unlocking automated security processes to protect sensitive data wherever it resides—from endpoint and IoT devices to multi-cloud environments, and from the main office to branch locations. In addition, it protects the necessary systems that support day-to-day operations, and provides secure networking capabilities to deliver business-critical applications without hindering networking performance.

Sophisticated technology increases the entertainment industry's online footprint and thus makes it more susceptible to remote compromise.

The Fortinet Security Fabric is comprised of a complete set of integrated network security technologies that works together, supported by industry-leading threat intelligence.

The Fortinet Security Fabric is comprised of a complete set of integrated network security technologies. It delivers:

- **Broad** visibility of the entire digital attack surface to better manage risk
- An **integrated** solution that reduces the complexity of supporting multiple point products
- **Automated** workflows to increase the speed of operations and response

At the foundation of the Security Fabric are industry-leading FortiGate Next-Generation Firewalls (NGFWs) and artificial intelligence (AI)-powered threat intelligence from FortiGuard Labs. Security teams also gain a proactive response to sophisticated threats with integrated security analytics and security orchestration, automation, and response (SOAR) tools. They can easily protect and monitor known and unknown endpoint and IoT devices across the network with Fortinet endpoint protection and response tools and FortiNAC network access control (NAC). Teams can also integrate network-based video security and voice communications for complete protection.

Additionally, they can leverage existing third-party Fabric-Ready Partner solutions and seamlessly integrate them into the Security Fabric with application programming interface (API) tools.

Secure branch locations

Many M&E firms span multiple locations that can consist of retail stores, movie theaters, venues, and theme parks. In order to enhance user experience and streamline operations, these branch locations require secure, reliable, and high-performance connectivity. With the increasing use of cloud-based applications for customer experiences and business services, these locations need to evolve their infrastructures to support agile connectivity that does not impact operations.

Fortinet secure branch infrastructure solutions enable secure, high-performance networking to all branches without adding significant cost or complexity. FortiGate NGFWs include built-in software-defined wide-area network (SD-WAN) technology, allowing firms to achieve secure and direct internet access. Firms can save time and simplify complex networks with the unified Fortinet Secure SD-WAN solution that comes with zero-touch deployment and does not require additional point products.

Fortinet SD-Branch extends this secure SD-WAN connectivity and protection to branch locations. Branches gain secure networking and end-to-end protection of the entire infrastructure no matter the branch size. Further, SD-Branch improves network performance for distributed branches and protects against breaches at the branch level.

On-site customer experience

Media and entertainment firms know that customer experience is often paramount to reputation and profit at on-site locations and events. Public Wi-Fi not only needs to meet guest expectations, but it also needs to protect devices and ensure guests do not have access to private corporate assets. Slow, limited, or unsecure wireless access can compromise a performance or experience and negatively impact brand or revenue.

The best approach, in many cases, is to deploy public Wi-Fi as an integrated part of their overall security architecture, versus as an independent solution that creates silos, manual processes, and complexity. With the Fortinet Security Fabric, firms can take an integrated approach by deploying public Wi-Fi with the rest of the security architecture.

FortiAP wireless access points and FortiSwitch Ethernet LAN switches provide secure Wi-Fi access. Meanwhile, FortiPresence and positioning analytics allow firms to track and understand user behavior to enhance customer experiences. All of these products can be seamlessly integrated with powerful FortiGate NGFWs. In addition, FortiGate NGFWs deliver intent-based segmentation, partitioning public Wi-Fi and ensuring guest devices cannot access corporate assets. Finally, since the Fortinet on-site customer experience solution is integrated with the greater Security Fabric, security teams also gain complete visibility and control of their Wi-Fi solutions.

According to FortiGuard Labs, ransomware attacks increased by 10x last year.

Cloud computing security skills is one of the biggest skills gaps in cybersecurity staff.

Content Protection

IP is a core driver for the success of many M&E firms. Breaches that compromise critical intellectual property can harm a firm's brand valuation and profits. Organizations must move beyond reliance of traditional security such as usernames and passwords to safeguard data by building a multilayered defense with intent-based segmentation at the core to limit network access.

The Fortinet Security Fabric protects content stored across the network by providing granular levels of access to only approved users. It also uses a zero-trust approach that analyzes each device as it attempts access to the network. FortiGate NGFWs, the core of the Security Fabric, enable intent-based segmentation, while FortiNAC works to protect the network from unauthorized devices attempting to access it.

To further secure intellectual property and ensure only specific users can access it, identity and access management tools FortiToken and FortiAuthenticator provide two-factor authentication to verify users. Meanwhile, FortiInsight user and entity behavior analytics (UEBA) detects behavioral anomalies across the network that may indicate insider threats. FortiDeceptor deception technology delivers automated detection and response to malicious and unintentional insider threats, and FortiSandbox provides AI-powered analysis to combat unknown threats. These solutions are all tightly integrated via FortiGate NGFWs to deliver comprehensive content protection across the entire network.

Advanced threat protection

Media and entertainment firms are known for being both high profile and high revenue, making them alluring targets for cybercriminals. On a global scale, the entertainment market generates more than $100 billion in annual revenues.[5] Advanced threats, such as botnets and ransomware, targeting high-value targets have both been on the rise. Last year, FortiGuard Labs research showed that ransomware attacks in particular increased tenfold.[6] With no shortage of threats targeting the M&E industry, advanced threat protection is a necessity.

The Security Fabric integrates various sources of threat intelligence to protect against advanced threats. By delivering real-time threat intelligence with AI and machine learning (ML), organizations gain a fast, automated response to threats.

FortiGuard Labs collects this threat intelligence from a global network of NGFWs that analyze the threat landscape in real time. This team has also developed an AI-powered self-evolving detection system (SEDS). SEDS has leveraged ML to intelligently adapt its algorithms, resulting in precise, immediate identification of unknown threats.

These AI and ML capabilities are integrated within Fortinet products to deliver smarter, faster threat detection and prevention. The FortiWeb web application firewall (WAF) leverages ML to detect unknown malicious threats in the cloud and protect business-critical applications. FortiInsight uses ML-based analytics to quickly detect risky user activity, and FortiSandbox AI-powered analysis and browser isolation tools provide additional security. The Fortinet Advanced Malware Protection service also provides wide-scale protection from malware threats.

Multi-cloud security

The vast majority of large enterprises indicated having already adopted multiple clouds as part of their infrastructure.[7] The built-in security provided by each cloud provider varies per vendor, resulting in a fragmented security architecture across each cloud that lacks visibility and connectivity. Not only does this hinder operational efficiency but it also lacks the necessary security to protect digital assets.

Organizations need a more robust security framework for their cloud deployments, one that is truly integrated and extends from the data center to multi-cloud environments. Part of the Security Fabric, Fortinet Cloud Security solutions break down silos between clouds and provide security teams with unified policy management and centralized visibility.

FortiCASB cloud access security broker (CASB) provides complete visibility and control, while FortiCWP cloud workload protection (CWP) helps teams keep track of their entire multi-cloud security posture, analyzing traffic across multiple clouds. FortiWeb web application firewall (WAF) deploys powerful ML capabilities to define benign and malicious cloud traffic, and then blocks malicious traffic.

With Fortinet Cloud Security solutions, security teams can confidently deploy any application in any cloud at any time. Integration in the Security Fabric and consistent policies increase efficiencies and reduce risk.

Date protection and compliance

Protecting customer devices, personally identifiable information (PII), as well as employee and contractor data by demonstrating compliance is a crucial responsibility of M&E firms. Failure to meet regulations and compliance standards can result in unsavory consequences, including penalties and fines from regulators, and worse, a tarnished brand reputation.

The Security Fabric solves these challenges with integrated, centralized control and reporting that ensures consistent end-to-end policy management—eliminating tedious manual audit reporting. Integrated SOAR and security analytics tools with FortiManager and FortiAnalyzer provide customizable automated reporting. As the threat landscape continues to expand, it becomes increasingly difficult to protect the entire attack surface. The Fortinet Security Rating Service provides tools that help security teams improve security posture over time with actionable, measurable suggestions. In addition, it helps teams meet compliance and regulations by ranking a firm's security posture compared with regulations, standards, and peer organizations; offers best practices to improve; and generates reports to measure progress.[8]

Conclusion

The Fortinet Security Fabric delivers comprehensive solutions that address the cybersecurity challenges facing the media and entertainment industry. With an architecture specifically built to meet the unique and evolving needs of the trade, lean security teams can save time, reduce resources, and lower costs all while implementing high-performance networking capabilities and industry-leading security from headquarters to branch locations. Firms gain the peace of mind that their most critical assets are protected wherever they reside—from endpoint to robust multi-cloud environments—while also delivering a high-class customer experience and ensuring operational availability. Fortinet is the dedicated media and entertainment industry partner for complete end-to-end protection.

[1] "Entertainment & Media – The Next Big Cyber Attack Target?" Security Boulevard, April 13 2022.

[2] "2021 Cost of a Data Breach Report," Ponemon Institute and IBM Security, July 28, 2021.

[3] "Addressing the Need for a New Security Platform," Fortinet, October 22, 2021

[4] "Why Cyber Attacks Against Film And Media Industries Are Escalating," Forbes, June 11 2021.

[5] Ibid.

[6] "FortiGuard Labs Threat Landscape Report Highlights Tenfold Increase in Ransomware" Forinet, August 23, 2021.

[7] "Multi cloud adoption worldwide in 2021 and 2023, by organization size," Statista, February 21, 2022.

[8] "FortiGuard Security Services," Fortinet, February 26, 2022.

May 10, 2022 3:16 PM
1580475-0-0-EN