

Web Filtering Market – Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented By Component (Solution, Services), By Filtering Type (Domain Name System (DNS) Filtering, Uniform Resource Locator (URL) Filtering, Keyword Filtering, File Type Filtering, Others), By Deployment Mode (On-premises, Cloud), By Organization Size (Small and Medium-sized Enterprises (SMEs), Large Enterprises) and By Industry Vertical (Government Banking, Financial Services, and Insurance (BFSI), Manufacturing, IT and Telecom, Education, Healthcare, Retail, Others), By Region, By Competition Forecast & Opportunities, 2018-2028

<https://marketpublishers.com/r/WBCC2156A4F8EN.html>

Date: October 2023

Pages: 183

Price: US\$ 4,500.00 (Single User License)

ID: WBCC2156A4F8EN

Abstracts

The Global Web Filtering Market was valued at USD 5.24 Billion in 2022 and is growing at a CAGR of 14.81% during the forecast period. The ascendancy of Web Filtering technology has been a game-changer, triggering a profound revolution in various sectors and ushering in a new era of digital transformation in data security. These groundbreaking advancements serve as the bedrock for the establishment of comprehensive digital security ecosystems, signaling an epoch marked by fortified cybersecurity, threat mitigation, and predictive threat intelligence. The Global Web Filtering Market is poised for remarkable expansion, catalyzed by a convergence of pivotal factors. One of the driving forces behind the surging demand for Web Filtering is the relentless pursuit of robust data protection and heightened security across

organizations in an increasingly interconnected digital landscape. Industries spanning from finance to government agencies are actively seeking innovative solutions to fortify their cybersecurity posture, defend against evolving threats, and safeguard sensitive data. The arsenal of Web Filtering technology empowers organizations to bolster their digital defenses, furnishing them with holistic capabilities to monitor, filter, and proactively counteract online threats. The integration of Web Filtering technology is experiencing an unprecedented surge, largely propelled by the escalating volume of data traffic, the proliferation of connected devices, and the emergence of sophisticated cyber threats. This influx of data provides a wealth of critical insights into digital security threats, paving the way for data-driven threat mitigation strategies, proactive security planning, and the deployment of predictive threat analytics. Consequently, the adoption of Web Filtering is gaining momentum across diverse sectors, including finance, government, healthcare, and technology. Moreover, cybersecurity experts and IT professionals have wholeheartedly embraced the adoption of Web Filtering, further amplifying its market potential. Seasoned cybersecurity practitioners across various industries recognize the transformative potential of Web Filtering technology, viewing it as a linchpin to bolster digital security, safeguard critical assets, and ensure regulatory compliance. One notable attribute of Web Filtering technology is its adaptability to tailor bespoke security solutions for specific industries. For example, in the financial sector, Web Filtering facilitates comprehensive cybersecurity management, enabling real-time threat detection, incident response, and security analytics tailored to the unique needs of financial institutions. This tailored approach ultimately leads to fortified digital defenses, reduced security risks, and enhanced data protection. In summary, the Global Web Filtering Market stands at the forefront of remarkable expansion, driven by the unceasing pursuit of data security, cyber resilience, and the unwavering support of cybersecurity experts and industry leaders. As organizations continue their relentless journey towards digital security fortification, Web Filtering stands as a linchpin, meticulously shaping the contours of the future for cybersecurity and threat mitigation. The luminous potential of Web Filtering is indeed a guiding beacon for organizations worldwide, illuminating the path to an era of unparalleled digital security, threat resilience, and innovation.

Key Market Drivers

Rising Cybersecurity Threats and Data Privacy Concerns

The Global Web Filtering Market is experiencing a surge in demand, fueled by the escalating cybersecurity threats and growing data privacy concerns that have gripped the digital landscape. In recent years, the world has witnessed an alarming increase in

cyberattacks, with malicious actors employing increasingly sophisticated tactics to breach organizations' digital defenses. These cyber threats, ranging from malware and phishing attacks to ransomware and data breaches, have left no industry untouched. Consequently, organizations across the globe are on high alert, recognizing the imperative need to fortify their cybersecurity measures. One of the primary drivers propelling the demand for Web Filtering technology is the relentless onslaught of cyber threats that exploit vulnerabilities in an interconnected world. Malware, in various forms, has become a pervasive menace, infiltrating systems to steal sensitive data, disrupt operations, or hold organizations hostage for ransom. Phishing attacks, designed to deceive unsuspecting users into revealing confidential information, have become alarmingly sophisticated, making them even harder to detect. Ransomware attacks have surged in frequency and severity, causing substantial financial losses and tarnishing the reputations of targeted entities. In response, organizations are turning to Web Filtering solutions as a crucial line of defense. These solutions empower them to filter and block malicious web content, identify and neutralize threats in real-time, and enforce stringent access controls to minimize the attack surface. Furthermore, data privacy concerns are a pressing issue in today's digital landscape, driven by stricter regulatory frameworks and heightened awareness among individuals regarding the value of their personal information. Regulatory bodies such as the European Union's GDPR and the California Consumer Privacy Act (CCPA) have imposed stringent requirements on organizations regarding the collection, storage, and processing of personal data. Failure to comply with these regulations can result in severe fines and reputational damage. Consequently, organizations are increasingly turning to Web Filtering technology to ensure compliance with data privacy regulations. These solutions help organizations monitor and filter web traffic to prevent the inadvertent exposure of sensitive data, ensuring that personal and confidential information remains protected.

Moreover, the remote work revolution, accelerated by the COVID-19 pandemic, has expanded the attack surface for cybercriminals. The proliferation of remote devices and the blurring of the traditional network perimeter have exposed organizations to new security challenges. With employees accessing corporate networks from various locations and devices, the need for robust Web Filtering solutions has never been more pronounced. These solutions enable organizations to extend their security controls to remote environments, ensuring that employees are protected regardless of their location.

In conclusion, the Global Web Filtering Market is experiencing unprecedented growth due to the rising tide of cybersecurity threats and data privacy concerns. The ever-evolving threat landscape demands proactive measures, and Web Filtering technology

has emerged as a linchpin in safeguarding organizations' digital assets and ensuring compliance with data protection regulations. As cyber threats continue to evolve and data privacy regulations become more stringent, the demand for Web Filtering solutions is expected to persist and expand, shaping the future of cybersecurity in an increasingly digital world.

Increasing Internet Usage and the Need for Productivity Enhancement:

The Global Web Filtering Market is experiencing significant growth driven by the widespread increase in internet usage and the pressing need for productivity enhancement across various industries. In recent years, the internet has become an integral part of both personal and professional life, serving as a vast repository of information, communication, and collaboration. However, this increased internet access has also brought forth challenges related to distractions, security risks, and the efficient use of online resources.

The relentless surge in internet usage is a primary driver behind the growing demand for Web Filtering solutions. As internet accessibility becomes more ubiquitous, individuals and organizations are confronted with a deluge of digital content and online activities. While the internet offers a wealth of valuable information, it also presents distractions that can impede productivity. Social media, online entertainment, and non-work-related websites can easily divert individuals from their tasks, leading to reduced efficiency and productivity in the workplace. To address this issue, organizations are turning to Web Filtering technology as a means to manage and optimize internet usage. These solutions allow organizations to set policies and filters that restrict access to non-productive websites and content during work hours, ensuring that employees stay focused on their tasks and business objectives.

Additionally, the proliferation of remote work and mobile devices has further exacerbated the need for Web Filtering solutions. With employees working from various locations and using diverse devices, it has become increasingly challenging for organizations to enforce consistent internet usage policies and protect against security threats. Web Filtering solutions provide a centralized means of managing and securing internet access across a distributed workforce. They enable organizations to apply uniform web filtering policies, block malicious websites, and prevent employees from accessing potentially harmful content, regardless of their location or device. This not only enhances productivity but also strengthens the organization's overall cybersecurity posture.

Security concerns also play a pivotal role in driving the demand for Web Filtering technology. The internet is rife with cybersecurity threats, including malware, phishing attacks, and data breaches. These threats can have devastating consequences for organizations, leading to financial losses, data breaches, and reputational damage. Web Filtering solutions act as a critical line of defense against these threats by monitoring internet traffic in real-time, identifying malicious websites and content, and blocking access to them. This proactive approach helps organizations mitigate security risks and protect their sensitive data, ensuring a safer online environment for both employees and customers.

Moreover, the need for compliance with industry regulations and data protection laws further drives the adoption of Web Filtering technology. Many industries, such as healthcare and finance, are subject to stringent regulations that require them to maintain strict control over internet access to safeguard sensitive data. Web Filtering solutions enable these organizations to enforce compliance by monitoring and controlling internet usage, ensuring that confidential information remains protected and that regulatory requirements are met.

In conclusion, the Global Web Filtering Market is experiencing robust growth due to the increasing prevalence of internet usage and the imperative need for productivity enhancement and security across various sectors. As the digital landscape continues to evolve, organizations recognize the importance of effectively managing internet access to optimize productivity, protect against security threats, and maintain regulatory compliance. Web Filtering technology is poised to remain a cornerstone in achieving these goals, shaping the future of internet usage and cybersecurity in an increasingly interconnected world.

Cloud-Based Solutions and Remote Work Trends

The Global Web Filtering Market is witnessing substantial growth driven by the rapid adoption of cloud-based solutions and the prevailing trends in remote work. In recent years, the cloud has become a fundamental technology infrastructure for organizations, offering unparalleled flexibility, scalability, and accessibility. Simultaneously, the emergence and acceleration of remote work have transformed the way businesses operate, requiring enhanced digital security measures and productivity management tools. Web Filtering solutions have emerged as a critical component in addressing the evolving needs of modern organizations. The proliferation of cloud-based solutions is a primary driver behind the increased demand for Web Filtering technology. Organizations of all sizes and across various industries are migrating their applications

and data to the cloud to benefit from cost savings, agility, and improved collaboration. However, this shift to the cloud brings new challenges related to web security and content management. Cloud-hosted applications and services often rely on web-based interactions, making them susceptible to web-borne threats such as malware, phishing attacks, and data breaches. To mitigate these risks, organizations are turning to cloud-based Web Filtering solutions that can seamlessly integrate with their cloud infrastructure. These solutions provide real-time web content analysis and filtering, allowing organizations to enforce consistent web security policies across all devices and locations, whether employees are in the office or working remotely.

The remote work trend, accelerated by the COVID-19 pandemic, has further emphasized the need for Web Filtering technology. With a significant portion of the workforce now operating from home or other remote locations, organizations face new challenges in managing and securing internet access. Remote employees often use personal devices and unsecured networks, which can increase the risk of cyber threats and productivity disruptions. Web Filtering solutions are indispensable in this context, as they enable organizations to extend their web security policies to remote workers. By routing web traffic through the Web Filtering solution, organizations can block access to malicious websites, enforce content filtering, and monitor online activities in real-time, regardless of where employees are working. This not only helps protect sensitive data but also ensures that employees remain productive and compliant with company policies, even in remote settings.

Furthermore, the dynamic nature of the remote work trend calls for flexible and scalable Web Filtering solutions. Cloud-based Web Filtering offers the agility required to adapt to changing work environments and evolving security threats. Organizations can easily scale their web security resources up or down as needed, ensuring that they remain protected and productive in the face of shifting workforce dynamics.

In summary, the Global Web Filtering Market is experiencing robust growth driven by the widespread adoption of cloud-based solutions and the ongoing trend of remote work. As organizations increasingly rely on cloud services and accommodate remote workers, the need for effective web security and content management has never been greater. Web Filtering technology, particularly in its cloud-based form, is poised to play a central role in safeguarding organizations' digital environments, promoting productivity, and ensuring a secure and compliant remote work experience. The flexibility and scalability of cloud-based Web Filtering solutions make them an indispensable tool in the arsenal of modern organizations looking to thrive in the digital age.

Key Market Challenges

Evolving Threat Landscape and Zero-Day Attacks:

The Global Web Filtering Market faces considerable challenges posed by the evolving threat landscape and the persistent menace of zero-day attacks. In recent years, the threat landscape has undergone a significant transformation, with cyber adversaries becoming increasingly sophisticated and adaptable in their methods. These threat actors constantly seek new vulnerabilities and exploit them before security measures can catch up, giving rise to zero-day attacks – a formidable challenge for organizations and Web Filtering solutions. Zero-day attacks are particularly insidious because they target vulnerabilities in software or systems that are unknown to the software vendor or security community. This means that there are no pre-existing patches or fixes to protect against these attacks when they are first discovered. As a result, organizations are left exposed to potentially devastating security breaches, data theft, and system compromise. Web Filtering solutions are a critical component of an organization's cybersecurity strategy, responsible for monitoring and filtering web traffic to identify and block malicious content and threats. However, zero-day attacks pose a unique challenge to these solutions. Traditional signature-based Web Filtering systems rely on known patterns and signatures of threats to detect and block malicious content. In the case of zero-day attacks, there are no predefined signatures to identify them, making them highly elusive.

To address this challenge, Web Filtering solutions are evolving to incorporate advanced threat detection techniques such as behavior analysis, heuristics, and machine learning. These approaches enable Web Filtering systems to identify suspicious behavior and anomalies, even in the absence of known threat signatures. By analyzing patterns of web traffic and user behavior, these solutions can detect unusual activities that may indicate the presence of a zero-day attack. Additionally, threat intelligence sharing and collaboration within the cybersecurity community play a crucial role in combating zero-day attacks. Organizations and Web Filtering vendors often rely on threat intelligence feeds and information sharing platforms to stay updated on emerging threats and vulnerabilities. This collaborative approach allows for quicker detection and response to zero-day threats, helping organizations mitigate the risks associated with these attacks.

In conclusion, the evolving threat landscape and the persistent threat of zero-day attacks present significant challenges to the Global Web Filtering Market. As cyber adversaries become more adept at exploiting unknown vulnerabilities, Web Filtering

solutions must adapt by incorporating advanced threat detection techniques and leveraging threat intelligence sharing to provide robust protection against these elusive threats. The ability to effectively counter zero-day attacks is a critical factor in the continued evolution and effectiveness of Web Filtering solutions in safeguarding organizations' digital environments.

Complexity of Content Classification and False Positives

The Global Web Filtering Market faces a substantial challenge in the complexity of content classification and the persistent issue of false positives. As the internet continues to expand with diverse content types and evolving user-generated content, accurately categorizing and filtering this vast array of data has become an intricate task. Web Filtering solutions are tasked with ensuring that organizations can effectively control access to websites and content while minimizing the risk of over-blocking or incorrectly categorizing legitimate content. This complex content landscape and the occurrence of false positives present significant hurdles for the industry.

Content Classification Complexity: The internet is a dynamic and ever-evolving ecosystem, hosting a plethora of content, including text, images, videos, and interactive applications. Moreover, the rise of user-generated content on social media platforms and websites introduces a continuous influx of new and often unclassified content. Accurate content classification is crucial for Web Filtering solutions to function effectively. These solutions rely on categorization to determine what content should be allowed or blocked based on predefined policies.

However, the diversity and intricacy of content make classification challenging. Content can be context-dependent, meaning that it may be suitable in one context but not in another. For example, a news article discussing violence may be appropriate in a journalistic context but not in an educational setting. Web Filtering systems need to consider the context in which content is presented, which adds complexity to the classification process.

False positives occur when Web Filtering solutions incorrectly block or categorize legitimate content as malicious or inappropriate. These false alarms can have detrimental consequences, leading to restricted access to essential resources, decreased productivity, and user frustration. False positives are particularly problematic in educational institutions, where access to educational content is critical, and overly restrictive filtering can hinder learning opportunities. One common cause of false positives is overzealous content classification algorithms. In an effort to err on the side

of caution, Web Filtering solutions may inadvertently block content that is not actually in violation of filtering policies. This cautious approach is intended to enhance security and protect users from potentially harmful content but can result in over-blocking. To address the complexity of content classification and reduce false positives, Web Filtering solutions are increasingly incorporating advanced technologies and techniques. Machine learning and artificial intelligence (AI) play a vital role in improving content classification accuracy. These technologies can analyze content in real-time, taking into account context, sentiment analysis, and user behavior to make more informed decisions about content categorization. Moreover, user feedback mechanisms are being integrated into Web Filtering solutions to allow users to report false positives and provide input on content classification accuracy. This feedback loop helps improve the algorithms over time, making the filtering process more precise. Additionally, organizations are customizing their Web Filtering policies to strike a balance between security and usability. By tailoring filtering rules to their specific needs and regularly reviewing and updating these policies, organizations can reduce the risk of over-blocking and false positives. In conclusion, the Global Web Filtering Market faces a considerable challenge in dealing with the complexity of content classification and the persistent issue of false positives. As the internet continues to evolve and diversify, Web Filtering solutions must adapt by leveraging advanced technologies, considering context, and incorporating user feedback mechanisms. Striking the right balance between security and usability is essential to ensure that Web Filtering solutions effectively protect users while minimizing disruptions caused by false positives.

Key Market Trends

AI and Machine Learning-Powered Filtering:

The Global Web Filtering Market is witnessing a significant trend towards the integration of AI (Artificial Intelligence) and machine learning-powered filtering solutions. This trend is driven by the need for more intelligent, adaptive, and accurate web content filtering capabilities in the face of a rapidly evolving digital landscape. AI and machine learning-powered filtering solutions are revolutionizing web filtering by enhancing the accuracy and efficiency of content classification and threat detection. These technologies enable Web Filtering systems to continuously learn and adapt to emerging threats and changing content patterns, making them more effective at identifying and addressing evolving online risks. One key advantage of AI and machine learning in web filtering is their ability to analyze vast amounts of data in real-time. This enables the system to detect subtle patterns, anomalies, and behavioral indicators associated with malicious websites, phishing attempts, or inappropriate content. As a result, the accuracy of

identifying and blocking threats and unwanted content improves significantly, reducing the risk of false positives and false negatives. Furthermore, AI and machine learning-powered filtering solutions can adapt to shifting user behavior and content trends. They can dynamically adjust filtering policies and priorities based on user preferences, evolving content types, and emerging threats. This adaptability is particularly valuable in a world where the internet's content landscape is constantly changing. Another benefit is the ability to perform content analysis beyond traditional keyword matching. AI-powered filters can consider context, sentiment analysis, and user behavior, allowing for a more nuanced understanding of web content. This enables the differentiation between harmless content and potentially harmful or inappropriate material, enhancing both security and usability. Overall, the incorporation of AI and machine learning into web filtering solutions represents a significant advancement in the field. It empowers organizations to stay ahead of the curve in addressing complex content classification and security challenges, making web filtering more effective, adaptive, and responsive to the demands of the ever-evolving digital environment. This trend is poised to continue shaping the Global Web Filtering Market as organizations seek more intelligent and dynamic solutions to protect their networks, users, and sensitive data from an array of online threats and content risks.

Segmental Insights

Type Insights

The DNS filtering segment is dominating the global web filtering market. It is estimated to hold the largest market share in 2022. DNS filtering is a type of web filtering that blocks access to websites by filtering the Domain Name System (DNS) requests. When a user tries to access a website, their computer sends a DNS request to a DNS server. The DNS server then returns the IP address of the website. DNS filtering works by blocking the DNS requests for websites that are blacklisted. There are several reasons why DNS filtering is the dominant filtering type in the global web filtering market. First, it is a very effective way to block access to websites. DNS filtering can block all traffic to a website, regardless of the content of the website. This makes it a very effective way to block malicious websites, such as phishing websites and malware websites. DNS filtering is very scalable. It can be easily deployed to large networks. This makes it a good choice for organizations with a large number of users. DNS filtering is relatively easy to manage. It can be easily configured to block specific websites or categories of websites. DNS filtering is a cost-effective solution. It is a relatively inexpensive way to block access to websites. The other filtering types, such as URL filtering, keyword filtering, and file type filtering, are not as widely used as DNS filtering. URL filtering

blocks access to websites based on their URLs. Keyword filtering blocks access to websites that contain certain keywords. File type filtering blocks access to files of certain types. These filtering types are not as effective as DNS filtering because they can be bypassed by using different URLs, keywords, or file types. In conclusion, the DNS filtering segment is dominating the global web filtering market because it is a very effective, scalable, easy-to-manage, and cost-effective way to block access to websites..

Regional Insights

North America accounted for the largest share of revenue in 2022. Advanced Technological Infrastructure: North America, particularly the United States, boasts a highly advanced technological infrastructure. This includes robust internet connectivity, data centers, and cloud computing capabilities. Such infrastructure is fundamental for the efficient deployment and management of web filtering solutions, which rely on fast and reliable internet connections and data processing capabilities. North America is home to a vast and diverse business landscape, including small and medium-sized enterprises (SMEs) as well as large multinational corporations. These organizations have diverse web filtering needs, from safeguarding against cyber threats to enforcing content policies and ensuring regulatory compliance. The presence of a wide range of industries, including finance, healthcare, education, and government, drives the demand for web filtering solutions. The United States and Canada have some of the world's most stringent data privacy and security regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS). These regulations mandate strict controls over data access and security, driving the adoption of web filtering solutions to ensure compliance and protect sensitive information.

High Cybersecurity Awareness: North American organizations have a high level of awareness regarding cybersecurity threats and the importance of web filtering in mitigating these threats. High-profile data breaches and cyberattacks have underscored the need for robust cybersecurity measures, including web filtering, to protect against malicious activities. The region is known for its innovation and investment in research and development, including cybersecurity technologies. Many leading web filtering solution providers are headquartered or have a significant presence in North America. This fosters innovation and the development of cutting-edge web filtering solutions, attracting both domestic and international customers. **Global Headquarters of Tech Giants:** North America is home to some of the world's largest technology companies, including Google, Microsoft, Cisco, and Symantec (now NortonLifeLock). These tech

giants often offer web filtering solutions as part of their cybersecurity product portfolios, contributing to the region's dominance in the market. Early Adoption of Cloud-Based Solutions: North American businesses have been early adopters of cloud-based web filtering solutions. The scalability, flexibility, and accessibility of cloud-based solutions have resonated well with organizations in the region, particularly in the context of remote work and the need for centralized management of web filtering policies. Government agencies and educational institutions in North America have also been significant adopters of web filtering solutions to protect networks, students, and sensitive government data. These institutions play a substantial role in driving demand for web filtering services. While North America has historically been dominant in the global web filtering market, it's important to note that other regions, such as Europe and Asia-Pacific, are also witnessing substantial growth in web filtering adoption. The global market is dynamic, and the regional landscape can evolve as organizations worldwide recognize the importance of web filtering in addressing cybersecurity threats and ensuring safe and compliant internet usage.

Key Market Players

Cisco Systems Inc.

SYMANTEC CORPORATION

McAfee Inc.

Palo Alto Networks Inc.

Fortinet

TREND MICRO INC.

Forcepoint

Sophos Group plc

BARRACUDA NETWORKS INC.

Zscaler

Report Scope:

In this report, the Global Web Filtering Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Global Web Filtering Market, By Component:

Solution

Services

Global Web Filtering Market, By Filtering Type:

Domain Name System (DNS) Filtering

Uniform Resource Locator (URL) Filtering

Keyword Filtering

File Type Filtering

Others

Global Web Filtering Market, By Deployment Mode:

On-premises

Cloud

Global Web Filtering Market, By Organization Size:

Small and Medium-sized Enterprises (SMEs)

Large Enterprises

Global Web Filtering Market, By Industry Vertical:

Government

Banking

Financial Services and Insurance (BFSI)

Manufacturing

IT and Telecom

Education

Healthcare

Retail

Others

Global Web Filtering Market, By Region:

North America

United States

Canada

Mexico

Europe

France

United Kingdom

Italy

Germany

Spain

Asia-Pacific

China

India

Japan

Australia

South Korea

South America

Brazil

Argentina

Colombia

Middle East & Africa

South Africa

Saudi Arabia

UAE

Competitive Landscape

Company Profiles: Detailed analysis of the major companies present in the Global Web Filtering Market.

Contents

1. PRODUCT OVERVIEW

- 1.1. Market Definition
- 1.2. Scope of the Market
 - 1.2.1. Markets Covered
 - 1.2.2. Years Considered for Study
 - 1.2.3. Key Market Segmentations

2. RESEARCH METHODOLOGY

- 2.1. Objective of the Study
- 2.2. Baseline Methodology
- 2.3. Key Industry Partners
- 2.4. Major Association and Secondary Sources
- 2.5. Forecasting Methodology
- 2.6. Data Triangulation & Validation
- 2.7. Assumptions and Limitations

3. EXECUTIVE SUMMARY

4. VOICE OF CUSTOMERS

5. GLOBAL WEB FILTERING MARKET OUTLOOK

- 5.1. Market Size & Forecast
 - 5.1.1. By Value
- 5.2. Market Share & Forecast
 - 5.2.1. By Component (Solution, Services)
 - 5.2.2. By Filtering Type (Domain Name System (DNS) Filtering, Uniform Resource Locator (URL) Filtering, Keyword Filtering, File Type Filtering, Others)
 - 5.2.3. By Deployment Mode (On-premises, Cloud)
 - 5.2.4. By Organization Size (Small and Medium-sized Enterprises (SMEs), Large Enterprises)
 - 5.2.5. By Industry Vertical (Government Banking, Financial Services, and Insurance (BFSI), Manufacturing, IT and Telecom, Education, Healthcare, Retail, Others))
 - 5.2.6. By Region
- 5.3. By Company (2022)

5.4. Market Map

6. NORTH AMERICA WEB FILTERING MARKET OUTLOOK

6.1. Market Size & Forecast

6.1.1. By Value

6.2. Market Share & Forecast

6.2.1. By Component

6.2.2. By Filtering Type

6.2.3. By Deployment Mode

6.2.4. By Organization Size

6.2.5. By Industry Vertical

6.2.6. By Country

6.3. North America: Country Analysis

6.3.1. United States Web Filtering Market Outlook

6.3.1.1. Market Size & Forecast

6.3.1.1.1. By Value

6.3.1.2. Market Share & Forecast

6.3.1.2.1. By Component

6.3.1.2.2. By Filtering Type

6.3.1.2.3. By Deployment Mode

6.3.1.2.4. By Organization Size

6.3.1.2.5. By Industry Vertical

6.3.2. Canada Web Filtering Market Outlook

6.3.2.1. Market Size & Forecast

6.3.2.1.1. By Value

6.3.2.2. Market Share & Forecast

6.3.2.2.1. By Component

6.3.2.2.2. By Filtering Type

6.3.2.2.3. By Deployment Mode

6.3.2.2.4. By Organization Size

6.3.2.2.5. By Industry Vertical

6.3.3. Mexico Web Filtering Market Outlook

6.3.3.1. Market Size & Forecast

6.3.3.1.1. By Value

6.3.3.2. Market Share & Forecast

6.3.3.2.1. By Component

6.3.3.2.2. By Filtering Type

6.3.3.2.3. By Deployment Mode

6.3.3.2.4. By Organization Size

6.3.3.2.5. By Industry Vertical

7. ASIA-PACIFIC WEB FILTERING MARKET OUTLOOK

7.1. Market Size & Forecast

7.1.1. By Value

7.2. Market Share & Forecast

7.2.1. By Component

7.2.2. By Filtering Type

7.2.3. By Deployment Mode

7.2.4. By Organization Size

7.2.5. By Industry Vertical

7.2.6. By Country

7.3. Asia-Pacific: Country Analysis

7.3.1. China Web Filtering Market Outlook

7.3.1.1. Market Size & Forecast

7.3.1.1.1. By Value

7.3.1.2. Market Share & Forecast

7.3.1.2.1. By Component

7.3.1.2.2. By Filtering Type

7.3.1.2.3. By Deployment Mode

7.3.1.2.4. By Organization Size

7.3.1.2.5. By Industry Vertical

7.3.2. India Web Filtering Market Outlook

7.3.2.1. Market Size & Forecast

7.3.2.1.1. By Value

7.3.2.2. Market Share & Forecast

7.3.2.2.1. By Component

7.3.2.2.2. By Filtering Type

7.3.2.2.3. By Deployment Mode

7.3.2.2.4. By Organization Size

7.3.2.2.5. By Industry Vertical

7.3.3. Japan Web Filtering Market Outlook

7.3.3.1. Market Size & Forecast

7.3.3.1.1. By Value

7.3.3.2. Market Share & Forecast

7.3.3.2.1. By Component

7.3.3.2.2. By Filtering Type

- 7.3.3.2.3. By Deployment Mode
- 7.3.3.2.4. By Organization Size
- 7.3.3.2.5. By Industry Vertical
- 7.3.4. South Korea Web Filtering Market Outlook
 - 7.3.4.1. Market Size & Forecast
 - 7.3.4.1.1. By Value
 - 7.3.4.2. Market Share & Forecast
 - 7.3.4.2.1. By Component
 - 7.3.4.2.2. By Filtering Type
 - 7.3.4.2.3. By Deployment Mode
 - 7.3.4.2.4. By Organization Size
 - 7.3.4.2.5. By Industry Vertical
- 7.3.5. Australia Web Filtering Market Outlook
 - 7.3.5.1. Market Size & Forecast
 - 7.3.5.1.1. By Value
 - 7.3.5.2. Market Share & Forecast
 - 7.3.5.2.1. By Component
 - 7.3.5.2.2. By Filtering Type
 - 7.3.5.2.3. By Deployment Mode
 - 7.3.5.2.4. By Organization Size
 - 7.3.5.2.5. By Industry Vertical

8. EUROPE WEB FILTERING MARKET OUTLOOK

- 8.1. Market Size & Forecast
 - 8.1.1. By Value
- 8.2. Market Share & Forecast
 - 8.2.1. By Component
 - 8.2.2. By Filtering Type
 - 8.2.3. By Deployment Mode
 - 8.2.4. By Organization Size
 - 8.2.5. By Industry Vertical
 - 8.2.6. By Country
- 8.3. Europe: Country Analysis
 - 8.3.1. Germany Web Filtering Market Outlook
 - 8.3.1.1. Market Size & Forecast
 - 8.3.1.1.1. By Value
 - 8.3.1.2. Market Share & Forecast
 - 8.3.1.2.1. By Component

- 8.3.1.2.2. By Filtering Type
- 8.3.1.2.3. By Deployment Mode
- 8.3.1.2.4. By Organization Size
- 8.3.1.2.5. By Industry Vertical
- 8.3.2. United Kingdom Web Filtering Market Outlook
 - 8.3.2.1. Market Size & Forecast
 - 8.3.2.1.1. By Value
 - 8.3.2.2. Market Share & Forecast
 - 8.3.2.2.1. By Component
 - 8.3.2.2.2. By Filtering Type
 - 8.3.2.2.3. By Deployment Mode
 - 8.3.2.2.4. By Organization Size
 - 8.3.2.2.5. By Industry Vertical
- 8.3.3. France Web Filtering Market Outlook
 - 8.3.3.1. Market Size & Forecast
 - 8.3.3.1.1. By Value
 - 8.3.3.2. Market Share & Forecast
 - 8.3.3.2.1. By Component
 - 8.3.3.2.2. By Filtering Type
 - 8.3.3.2.3. By Deployment Mode
 - 8.3.3.2.4. By Organization Size
 - 8.3.3.2.5. By Industry Vertical
- 8.3.4. Italy Web Filtering Market Outlook
 - 8.3.4.1. Market Size & Forecast
 - 8.3.4.1.1. By Value
 - 8.3.4.2. Market Share & Forecast
 - 8.3.4.2.1. By Component
 - 8.3.4.2.2. By Filtering Type
 - 8.3.4.2.3. By Deployment Mode
 - 8.3.4.2.4. By Organization Size
 - 8.3.4.2.5. By Industry Vertical
- 8.3.5. Spain Web Filtering Market Outlook
 - 8.3.5.1. Market Size & Forecast
 - 8.3.5.1.1. By Value
 - 8.3.5.2. Market Share & Forecast
 - 8.3.5.2.1. By Component
 - 8.3.5.2.2. By Filtering Type
 - 8.3.5.2.3. By Deployment Mode
 - 8.3.5.2.4. By Organization Size

8.3.5.2.5. By Industry Vertical

9. SOUTH AMERICA WEB FILTERING MARKET OUTLOOK

9.1. Market Size & Forecast

9.1.1. By Value

9.2. Market Share & Forecast

9.2.1. By Component

9.2.2. By Filtering Type

9.2.3. By Deployment Mode

9.2.4. By Organization Size

9.2.5. By Industry Vertical

9.2.6. By Country

9.3. South America: Country Analysis

9.3.1. Brazil Web Filtering Market Outlook

9.3.1.1. Market Size & Forecast

9.3.1.1.1. By Value

9.3.1.2. Market Share & Forecast

9.3.1.2.1. By Component

9.3.1.2.2. By Filtering Type

9.3.1.2.3. By Deployment Mode

9.3.1.2.4. By Organization Size

9.3.1.2.5. By Industry Vertical

9.3.2. Argentina Web Filtering Market Outlook

9.3.2.1. Market Size & Forecast

9.3.2.1.1. By Value

9.3.2.2. Market Share & Forecast

9.3.2.2.1. By Component

9.3.2.2.2. By Filtering Type

9.3.2.2.3. By Deployment Mode

9.3.2.2.4. By Organization Size

9.3.2.2.5. By Industry Vertical

9.3.3. Colombia Web Filtering Market Outlook

9.3.3.1. Market Size & Forecast

9.3.3.1.1. By Value

9.3.3.2. Market Share & Forecast

9.3.3.2.1. By Component

9.3.3.2.2. By Filtering Type

9.3.3.2.3. By Deployment Mode

9.3.3.2.4. By Organization Size

9.3.3.2.5. By Industry Vertical

10. MIDDLE EAST & AFRICA WEB FILTERING MARKET OUTLOOK

10.1. Market Size & Forecast

10.1.1. By Value

10.2. Market Share & Forecast

10.2.1. By Component

10.2.2. By Filtering Type

10.2.3. By Deployment Mode

10.2.4. By Organization Size

10.2.5. By Industry Vertical

10.2.6. By Country

10.3. Middle East & Africa: Country Analysis

10.3.1. Saudi Arabia Web Filtering Market Outlook

10.3.1.1. Market Size & Forecast

10.3.1.1.1. By Value

10.3.1.2. Market Share & Forecast

10.3.1.2.1. By Component

10.3.1.2.2. By Filtering Type

10.3.1.2.3. By Deployment Mode

10.3.1.2.4. By Organization Size

10.3.1.2.5. By Industry Vertical

10.3.2. South Africa Web Filtering Market Outlook

10.3.2.1. Market Size & Forecast

10.3.2.1.1. By Value

10.3.2.2. Market Share & Forecast

10.3.2.2.1. By Component

10.3.2.2.2. By Filtering Type

10.3.2.2.3. By Deployment Mode

10.3.2.2.4. By Organization Size

10.3.2.2.5. By Industry Vertical

10.3.3. UAE Web Filtering Market Outlook

10.3.3.1. Market Size & Forecast

10.3.3.1.1. By Value

10.3.3.2. Market Share & Forecast

10.3.3.2.1. By Component

10.3.3.2.2. By Filtering Type

- 10.3.3.2.3. By Deployment Mode
- 10.3.3.2.4. By Organization Size
- 10.3.3.2.5. By Industry Vertical

11. MARKET DYNAMICS

- 11.1. Drivers
- 11.2. Challenge

12. MARKET TRENDS & DEVELOPMENTS

13. COMPANY PROFILES

- 13.1. Cisco Systems Inc.
 - 13.1.1. Business Overview
 - 13.1.2. Key Revenue and Financials
 - 13.1.3. Recent Developments
 - 13.1.4. Key Personnel
 - 13.1.5. Key Product/Services
- 13.2. SYMANTEC CORPORATION
 - 13.2.1. Business Overview
 - 13.2.2. Key Revenue and Financials
 - 13.2.3. Recent Developments
 - 13.2.4. Key Personnel
 - 13.2.5. Key Product/Services
- 13.3. Zscaler; McAfee Inc.
 - 13.3.1. Business Overview
 - 13.3.2. Key Revenue and Financials
 - 13.3.3. Recent Developments
 - 13.3.4. Key Personnel
 - 13.3.5. Key Product/Services
- 13.4. Palo Alto Networks Inc.
 - 13.4.1. Business Overview
 - 13.4.2. Key Revenue and Financials
 - 13.4.3. Recent Developments
 - 13.4.4. Key Personnel
 - 13.4.5. Key Product/Services
- 13.5. Fortinet
 - 13.5.1. Business Overview

- 13.5.2. Key Revenue and Financials
- 13.5.3. Recent Developments
- 13.5.4. Key Personnel
- 13.5.5. Key Product/Services
- 13.6. TREND MICRO INC.
 - 13.6.1. Business Overview
 - 13.6.2. Key Revenue and Financials
 - 13.6.3. Recent Developments
 - 13.6.4. Key Personnel
 - 13.6.5. Key Product/Services
- 13.7. Forcepoint
 - 13.7.1. Business Overview
 - 13.7.2. Key Revenue and Financials
 - 13.7.3. Recent Developments
 - 13.7.4. Key Personnel
 - 13.7.5. Key Product/Services
- 13.8. Sophos Group plc
 - 13.8.1. Business Overview
 - 13.8.2. Key Revenue and Financials
 - 13.8.3. Recent Developments
 - 13.8.4. Key Personnel
 - 13.8.5. Key Product/Services
- 13.9. BARRACUDA NETWORKS INC.
 - 13.9.1. Business Overview
 - 13.9.2. Key Revenue and Financials
 - 13.9.3. Recent Developments
 - 13.9.4. Key Personnel
 - 13.9.5. Key Product/Services
- 13.10. Zscaler
 - 13.10.1. Business Overview
 - 13.10.2. Key Revenue and Financials
 - 13.10.3. Recent Developments
 - 13.10.4. Key Personnel
 - 13.10.5. Key Product/Services

14. STRATEGIC RECOMMENDATIONS

About Us & Disclaimer

I would like to order

Product name: Web Filtering Market – Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented By Component (Solution, Services), By Filtering Type (Domain Name System (DNS) Filtering, Uniform Resource Locator (URL) Filtering, Keyword Filtering, File Type Filtering, Others), By Deployment Mode (On-premises, Cloud), By Organization Size (Small and Medium-sized Enterprises (SMEs), Large Enterprises) and By Industry Vertical (Government Banking, Financial Services, and Insurance (BFSI), Manufacturing, IT and Telecom, Education, Healthcare, Retail, Others), By Region, By Competition Forecast & Opportunities, 2018-2028

Product link: <https://marketpublishers.com/r/WBCC2156A4F8EN.html>

Price: US\$ 4,500.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/WBCC2156A4F8EN.html>