

Secure Web Gateway Market Forecasts to 2032 – Global Analysis By Component (Solutions and Services), Deployment Mode, Organization Size, Function, Delivery Method, End User and By Geography

<https://marketpublishers.com/r/S78437EE06F2EN.html>

Date: April 2025

Pages: 200

Price: US\$ 4,150.00 (Single User License)

ID: S78437EE06F2EN

Abstracts

According to Statistics MRC, the Global Secure Web Gateway Market is accounted for \$17.7 billion in 2025 and is expected to reach \$65.7 billion by 2032 growing at a CAGR of 20.6% during the forecast period. Secure Web Gateway (SWG) is a cybersecurity solution that monitors and filters internet traffic to prevent unauthorized access, data breaches, and malware threats. It enforces enterprise security policies by inspecting web requests, blocking malicious content, and ensuring compliance with regulatory standards. SWGs typically integrate URL filtering, antivirus scanning, data loss prevention, and SSL inspection to safeguard users and devices. Positioned between users and the internet, they provide secure, policy-driven access to web resources while minimizing exposure to external threats.

Market Dynamics:

Driver:

Increasing frequency and sophistication of phishing, ransomware, and zero-day

Enterprises are increasingly adopting SWG solutions to safeguard sensitive data and ensure secure internet access across distributed workforces. As threat actors leverage AI-driven tactics and polymorphic malware, SWG platforms are evolving to offer real-time threat detection, sandboxing, and behavioral analytics. The shift toward hybrid work environments and cloud-based applications further amplifies the need for robust

gateway-level security, positioning SWG as a critical component of enterprise cybersecurity architecture.

Restraint:

Integrating SWG with outdated IT infrastructure

Many organizations operate on legacy networks that lack the agility to support modern security protocols, leading to implementation delays and increased costs. Integrating SWG with older systems may require extensive reconfiguration, specialized middleware, or phased rollouts, which can strain IT resources. Additionally, concerns around system downtime and data migration risks discourage some enterprises from upgrading, thereby limiting market penetration in traditional sectors.

Opportunity:

Expansion in BFSI, healthcare, and government sectors

The SWG market is witnessing significant growth opportunities in highly regulated industries such as banking, financial services, insurance (BFSI), healthcare, and government. These sectors handle vast volumes of confidential data and are subject to stringent compliance mandates, making secure web access a top priority. The rise of digital banking, telehealth platforms, and e-governance initiatives is accelerating adoption, with organizations seeking scalable and policy-driven security frameworks to protect against data breaches and insider threats.

Threat:

Intense competition and overlapping functionalities

Many endpoint protection platforms, cloud access security brokers (CASBs), and next-generation firewalls now incorporate web filtering and threat prevention features, blurring the lines between categories. This convergence challenges SWG providers to innovate beyond basic URL filtering and malware blocking, emphasizing advanced threat intelligence, user behavior analytics, and integration with broader security ecosystems. Moreover price wars and commoditization further pressure margins, especially among mid-tier vendors.

Covid-19 Impact:

The COVID-19 pandemic catalyzed a surge in SWG adoption as organizations rapidly transitioned to remote work. SWG solutions enabled centralized policy enforcement, encrypted traffic inspection, and protection against web-based threats across distributed endpoints. While initial disruptions in supply chains and IT budgets posed challenges, the long-term impact has been positive, with enterprises prioritizing cloud-native and scalable SWG deployments to support hybrid work models and digital transformation initiatives.

The solutions segment is expected to be the largest during the forecast period

The solutions segment is expected to account for the largest market share during the forecast period as enterprises are investing in comprehensive SWG platforms that offer integrated threat detection, URL filtering, SSL inspection, and data protection capabilities. These solutions are increasingly cloud-delivered, enabling seamless scalability and centralized management across global operations. The demand for customizable policy enforcement and real-time analytics is driving innovation, with vendors offering modular architectures to cater to diverse enterprise needs.

The data loss prevention (DLP) segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the data loss prevention (DLP) segment is predicted to witness the highest growth rate driven by rising concerns around data exfiltration and insider threats. As organizations embrace cloud collaboration tools and remote work, the risk of unauthorized data sharing has intensified. SWG platforms with embedded DLP capabilities enable granular control over sensitive information, preventing leakage through web channels, email, and file transfers. Advanced DLP features such as contextual analysis, fingerprinting, and machine learning are gaining traction, particularly in sectors handling regulated data.

Region with largest share:

During the forecast period, the Asia Pacific region is expected to hold the largest market share attributed to rapid digitalization, expanding internet penetration, and growing cybersecurity awareness. Countries like China, India, Japan, and South Korea are investing heavily in secure IT infrastructure to combat rising cyber threats. Government-led initiatives promoting data protection and cloud adoption are further fueling demand for SWG solutions. The region's vibrant SME sector and increasing reliance on mobile

and web-based services contribute to robust market expansion.

Region with highest CAGR:

Over the forecast period, the North America region is anticipated to exhibit the highest CAGR driven by advanced threat landscapes and proactive cybersecurity investments. The region hosts a mature IT ecosystem with high adoption of cloud services, making SWG a strategic priority for enterprises. Regulatory frameworks such as CCPA and HIPAA are compelling organizations to implement stringent web security measures. Additionally, the presence of leading SWG vendors and continuous innovation in AI-powered threat detection are accelerating market growth across the U.S. and Canada.

Key players in the market

Some of the key players in Secure Web Gateway Market include Broadcom, Cisco Systems, Zscaler, Forcepoint, McAfee, iboss, Sophos, Trend Micro, Barracuda Networks, Netskope, Fortinet, Palo Alto Networks, Check Point Software Technologies, Menlo Security, Sangfor Technologies, Cato Networks, Kaspersky Lab, and Proofpoint Inc.

Key Developments:

In October 2025, Broadcom announced new high-performance networking chips and deepened its AI infrastructure focus through a strategic collaboration to deliver custom AI accelerators. The chip and systems news highlights Broadcom's push into data-center networking for large-scale AI and signals expanded competition with other AI-infrastructure vendors.

In October 2025, Cisco partnered with the City of Los Angeles and local nonprofits to launch a citywide community Wi-Fi initiative, expanding public broadband access. The program combines Cisco technology, local partners and municipal support to deliver free or low-cost connectivity and digital inclusion services across LA neighborhoods.

In October 2025, Forcepoint expanded its Self-Aware Data Security platform with AI-native DSPM to cover enterprise databases and data lakes. The announcement positions Forcepoint as providing unified Data Security Posture Management (DSPM) + adaptive DLP across structured and unstructured data.

Components Covered:

Solutions

Services

Deployment Modes Covered:

Cloud-Based

On-Premise

Hybrid

Organization Sizes Covered:

Small & Medium Enterprises (SMEs)

Large Enterprises

Functions Covered:

URL Filtering

Data Loss Prevention (DLP)

Malware Protection

Application Control

SSL Inspection

Threat Intelligence Integration

Other Functions

Delivery Methods Covered:

Inline Gateway

Proxy-Based Gateway

API-Based Gateway

End Users Covered:

BFSI (Banking, Financial Services & Insurance)

IT & Telecom

Healthcare & Life Sciences

Government & Defense

Retail & eCommerce

Manufacturing

Education

Energy & Utilities

Other End Users

Regions Covered:

North America

US

Canada

Mexico

Europe

Germany

UK

Italy

France

Spain

Rest of Europe

Asia Pacific

Japan

China

India

Australia

New Zealand

South Korea

Rest of Asia Pacific

South America

Argentina

Brazil

Chile

Rest of South America

Middle East & Africa

Saudi Arabia

UAE

Qatar

South Africa

Rest of Middle East & Africa

What our report offers:

- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2024, 2025, 2026, 2028, and 2032
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market estimations
- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as

per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliances

Contents

1 EXECUTIVE SUMMARY

2 PREFACE

- 2.1 Abstract
- 2.2 Stake Holders
- 2.3 Research Scope
- 2.4 Research Methodology
 - 2.4.1 Data Mining
 - 2.4.2 Data Analysis
 - 2.4.3 Data Validation
 - 2.4.4 Research Approach
- 2.5 Research Sources
 - 2.5.1 Primary Research Sources
 - 2.5.2 Secondary Research Sources
 - 2.5.3 Assumptions

3 MARKET TREND ANALYSIS

- 3.1 Introduction
- 3.2 Drivers
- 3.3 Restraints
- 3.4 Opportunities
- 3.5 Threats
- 3.6 End User Analysis
- 3.7 Emerging Markets
- 3.8 Impact of Covid-19

4 PORTERS FIVE FORCE ANALYSIS

- 4.1 Bargaining power of suppliers
- 4.2 Bargaining power of buyers
- 4.3 Threat of substitutes
- 4.4 Threat of new entrants
- 4.5 Competitive rivalry

5 GLOBAL SECURE WEB GATEWAY MARKET, BY COMPONENT

- 5.1 Introduction
- 5.2 Solutions
- 5.3 Services
 - 5.3.1 Professional Services
 - 5.3.2 Managed Services
 - 5.3.3 Support & Maintenance
 - 5.3.4 Consulting & Integration Services

6 GLOBAL SECURE WEB GATEWAY MARKET, BY DEPLOYMENT MODE

- 6.1 Introduction
- 6.2 Cloud-Based
- 6.3 On-Premise
- 6.4 Hybrid

7 GLOBAL SECURE WEB GATEWAY MARKET, BY ORGANIZATION SIZE

- 7.1 Introduction
- 7.2 Small & Medium Enterprises (SMEs)
- 7.3 Large Enterprises

8 GLOBAL SECURE WEB GATEWAY MARKET, BY FUNCTION

- 8.1 Introduction
- 8.2 URL Filtering
- 8.3 Data Loss Prevention (DLP)
- 8.4 Malware Protection
- 8.5 Application Control
- 8.6 SSL Inspection
- 8.7 Threat Intelligence Integration
- 8.8 Other Functions

9 GLOBAL SECURE WEB GATEWAY MARKET, BY DELIVERY METHOD

- 9.1 Introduction
- 9.2 Inline Gateway
- 9.3 Proxy-Based Gateway
- 9.4 API-Based Gateway

10 GLOBAL SECURE WEB GATEWAY MARKET, BY END USER

- 10.1 Introduction
- 10.2 BFSI (Banking, Financial Services & Insurance)
- 10.3 IT & Telecom
- 10.4 Healthcare & Life Sciences
- 10.5 Government & Defense
- 10.6 Retail & eCommerce
- 10.7 Manufacturing
- 10.8 Education
- 10.9 Energy & Utilities
- 10.10 Other End Users

11 GLOBAL SECURE WEB GATEWAY MARKET, BY GEOGRAPHY

- 11.1 Introduction
- 11.2 North America
 - 11.2.1 US
 - 11.2.2 Canada
 - 11.2.3 Mexico
- 11.3 Europe
 - 11.3.1 Germany
 - 11.3.2 UK
 - 11.3.3 Italy
 - 11.3.4 France
 - 11.3.5 Spain
 - 11.3.6 Rest of Europe
- 11.4 Asia Pacific
 - 11.4.1 Japan
 - 11.4.2 China
 - 11.4.3 India
 - 11.4.4 Australia
 - 11.4.5 New Zealand
 - 11.4.6 South Korea
 - 11.4.7 Rest of Asia Pacific
- 11.5 South America
 - 11.5.1 Argentina
 - 11.5.2 Brazil

- 11.5.3 Chile
- 11.5.4 Rest of South America
- 11.6 Middle East & Africa
 - 11.6.1 Saudi Arabia
 - 11.6.2 UAE
 - 11.6.3 Qatar
 - 11.6.4 South Africa
 - 11.6.5 Rest of Middle East & Africa

12 KEY DEVELOPMENTS

- 12.1 Agreements, Partnerships, Collaborations and Joint Ventures
- 12.2 Acquisitions & Mergers
- 12.3 New Product Launch
- 12.4 Expansions
- 12.5 Other Key Strategies

13 COMPANY PROFILING

- 13.1 Broadcom
- 13.2 Cisco Systems
- 13.3 Zscaler
- 13.4 Forcepoint
- 13.5 McAfee
- 13.6 iboss
- 13.7 Sophos
- 13.8 Trend Micro
- 13.9 Barracuda Networks
- 13.10 Netskope
- 13.11 Fortinet
- 13.12 Palo Alto Networks
- 13.13 Check Point Software Technologies
- 13.14 Menlo Security
- 13.15 Sangfor Technologies
- 13.16 Cato Networks
- 13.17 Kaspersky Lab
- 13.18 Proofpoint Inc.

List Of Tables

LIST OF TABLES

Table 1 Global Secure Web Gateway Market Outlook, By Region (2024-2032) (\$MN)

Table 2 Global Secure Web Gateway Market Outlook, By Component (2024-2032) (\$MN)

Table 3 Global Secure Web Gateway Market Outlook, By Solutions (2024-2032) (\$MN)

Table 4 Global Secure Web Gateway Market Outlook, By Services (2024-2032) (\$MN)

Table 5 Global Secure Web Gateway Market Outlook, By Professional Services (2024-2032) (\$MN)

Table 6 Global Secure Web Gateway Market Outlook, By Managed Services (2024-2032) (\$MN)

Table 7 Global Secure Web Gateway Market Outlook, By Support & Maintenance (2024-2032) (\$MN)

Table 8 Global Secure Web Gateway Market Outlook, By Consulting & Integration Services (2024-2032) (\$MN)

Table 9 Global Secure Web Gateway Market Outlook, By Deployment Mode (2024-2032) (\$MN)

Table 10 Global Secure Web Gateway Market Outlook, By Cloud-Based (2024-2032) (\$MN)

Table 11 Global Secure Web Gateway Market Outlook, By On-Premise (2024-2032) (\$MN)

Table 12 Global Secure Web Gateway Market Outlook, By Hybrid (2024-2032) (\$MN)

Table 13 Global Secure Web Gateway Market Outlook, By Organization Size (2024-2032) (\$MN)

Table 14 Global Secure Web Gateway Market Outlook, By Small & Medium Enterprises (SMEs) (2024-2032) (\$MN)

Table 15 Global Secure Web Gateway Market Outlook, By Large Enterprises (2024-2032) (\$MN)

Table 16 Global Secure Web Gateway Market Outlook, By Function (2024-2032) (\$MN)

Table 17 Global Secure Web Gateway Market Outlook, By URL Filtering (2024-2032) (\$MN)

Table 18 Global Secure Web Gateway Market Outlook, By Data Loss Prevention (DLP) (2024-2032) (\$MN)

Table 19 Global Secure Web Gateway Market Outlook, By Malware Protection (2024-2032) (\$MN)

Table 20 Global Secure Web Gateway Market Outlook, By Application Control (2024-2032) (\$MN)

Table 21 Global Secure Web Gateway Market Outlook, By SSL Inspection (2024-2032) (\$MN)

Table 22 Global Secure Web Gateway Market Outlook, By Threat Intelligence Integration (2024-2032) (\$MN)

Table 23 Global Secure Web Gateway Market Outlook, By Other Functions (2024-2032) (\$MN)

Table 24 Global Secure Web Gateway Market Outlook, By Delivery Method (2024-2032) (\$MN)

Table 25 Global Secure Web Gateway Market Outlook, By Inline Gateway (2024-2032) (\$MN)

Table 26 Global Secure Web Gateway Market Outlook, By Proxy-Based Gateway (2024-2032) (\$MN)

Table 27 Global Secure Web Gateway Market Outlook, By API-Based Gateway (2024-2032) (\$MN)

Table 28 Global Secure Web Gateway Market Outlook, By End User (2024-2032) (\$MN)

Table 29 Global Secure Web Gateway Market Outlook, By BFSI (Banking, Financial Services & Insurance) (2024-2032) (\$MN)

Table 30 Global Secure Web Gateway Market Outlook, By IT & Telecom (2024-2032) (\$MN)

Table 31 Global Secure Web Gateway Market Outlook, By Healthcare & Life Sciences (2024-2032) (\$MN)

Table 32 Global Secure Web Gateway Market Outlook, By Government & Defense (2024-2032) (\$MN)

Table 33 Global Secure Web Gateway Market Outlook, By Retail & eCommerce (2024-2032) (\$MN)

Table 34 Global Secure Web Gateway Market Outlook, By Manufacturing (2024-2032) (\$MN)

Table 35 Global Secure Web Gateway Market Outlook, By Education (2024-2032) (\$MN)

Table 36 Global Secure Web Gateway Market Outlook, By Energy & Utilities (2024-2032) (\$MN)

Table 37 Global Secure Web Gateway Market Outlook, By Other End Users (2024-2032) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

I would like to order

Product name: Secure Web Gateway Market Forecasts to 2032 – Global Analysis By Component (Solutions and Services), Deployment Mode, Organization Size, Function, Delivery Method, End User and By Geography

Product link: <https://marketpublishers.com/r/S78437EE06F2EN.html>

Price: US\$ 4,150.00 (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/S78437EE06F2EN.html>