

# Intrusion Prevention System Market - Forecast from 2026 to 2031

<https://marketpublishers.com/r/I6C6476FCE4EEN.html>

Date: January 2026

Pages: 149

Price: US\$ 3,950.00 (Single User License)

ID: I6C6476FCE4EEN

## Abstracts

Intrusion Prevention System Market is projected to increase at a 10.57% CAGR, reaching USD 13.777 billion in 2031 from USD 7.538 billion in 2025.

The Intrusion Prevention System (IPS) market is centered on the provision of network security solutions designed to actively monitor, detect, and preemptively block malicious activities and policy violations in real time. An IPS functions as a critical control point within the security architecture, analyzing network traffic to identify threats—including malware, exploit attempts, and unauthorized access—and taking automated action to prevent them from compromising network integrity and data confidentiality. This proactive stance distinguishes IPS from passive detection systems, positioning it as an essential component for enforcing security policy and mitigating risks before breaches occur.

### Primary Market Growth Drivers

Market expansion is propelled by a convergence of persistent threat dynamics and evolving organizational imperatives.

The foremost driver is the continuous escalation and evolution of cyber threats. Attackers are persistently developing more advanced techniques to breach network defenses, exploiting vulnerabilities with increasing speed and sophistication. This environment necessitates security controls that can respond in real time. The surge in attacks targeting cloud-based networks, in particular, underscores a shift in the threat landscape that demands adaptable, network-wide protection. Intrusion Prevention Systems are fundamental to this defense, providing the continuous monitoring and automated blocking required to counteract these advanced, persistent threats.

Parallel to the threat landscape is the stringent and expanding framework of global regulatory requirements. Organizations across sectors, especially in healthcare, finance, and critical infrastructure, are mandated to maintain rigorous administrative, technical, and physical safeguards for sensitive data. Regulations enforce standards for data integrity, confidentiality, and availability. IPS solutions directly support compliance efforts by providing documented, automated enforcement of security policies, preemptively blocking activities that could lead to a breach and demonstrating due diligence in protecting regulated information assets.

Furthermore, a marked increase in organizational security awareness is accelerating adoption. This awareness transcends the IT department, reaching executive leadership and board levels, where cybersecurity is now recognized as a core business risk. This shift is fueled by the proliferation of cybersecurity education, high-profile breach disclosures, and the understanding that reactive security is insufficient. Consequently, organizations are prioritizing investments in proactive defenses like IPS to enhance their overall security posture, protect critical assets, and build resilient defense-in-depth architectures.

### Key Market Challenges

A significant challenge to seamless market expansion is the inherent complexity of configuration and integration. Deploying an IPS effectively requires deep integration into often heterogeneous and complex network environments, which may include legacy systems, hybrid cloud architectures, and diverse endpoints. Configuring precise rules and policies that align with specific business processes without disrupting legitimate traffic demands specialized expertise. For large enterprises, the initial assessment of network infrastructure, data flows, and security policies prior to implementation can be a substantial undertaking. This complexity can act as a barrier to adoption, necessitating that vendors focus on improving usability, providing robust integration frameworks, and offering managed services to facilitate deployment.

### Geographic Market Outlook

North America is projected to maintain a dominant position in the IPS market. This leadership is attributed to several structural factors: the concentration of major cybersecurity vendors and innovators, significant and sustained investment in advanced security technologies, and a high degree of regulatory scrutiny and security maturity among enterprises. The region's advanced digital infrastructure and early adoption of

cloud services also present a expansive attack surface, driving a correspondingly high demand for sophisticated protective measures like intrusion prevention systems to safeguard critical operations and data.

## Competitive Landscape and Product Evolution

The competitive landscape features established cybersecurity leaders whose IPS offerings are evolving into more intelligent, integrated, and versatile platforms. Modern product developments emphasize several key capabilities:

**Advanced Threat Detection:** Leveraging comprehensive, continuously updated signature databases alongside proactive behavioral analysis and heuristics to identify both known and zero-day or potentially malicious activities.

**AI and Machine Learning Integration:** Incorporating AI/ML to enhance detection accuracy, reduce false positives, and provide near-real-time threat intelligence, enabling faster response to emerging attack patterns.

**Flexible Deployment Architectures:** Supporting versatile deployment modes—including inline, passive, and hybrid models—to accommodate diverse network topologies, from the perimeter and data center core to protecting specific assets and WAN connections.

**Preventive Security Functions:** Moving beyond detection to include active prevention capabilities such as virtual patching, which shields vulnerabilities from exploitation before official patches can be applied, and deep packet inspection for granular traffic analysis.

In conclusion, the Intrusion Prevention System market is driven by the non-negotiable need for proactive, automated network defense in the face of advanced threats and stringent compliance mandates. While integration complexity remains a hurdle, the evolution of IPS solutions towards greater intelligence, integration with broader security platforms, and flexible deployment is strengthening their value proposition. The market's trajectory points toward IPS becoming an even more adaptive and essential component of a holistic security fabric, crucial for organizations aiming to achieve resilient, real-time threat prevention.

## Key Benefits of this Report:

**Insightful Analysis:** Gain detailed market insights covering major as well as emerging geographical regions, focusing on customer segments, government policies and socio-economic factors, consumer preferences, industry verticals, and other sub-segments.

**Competitive Landscape:** Understand the strategic maneuvers employed by key players globally to understand possible market penetration with the correct strategy.

**Market Drivers & Future Trends:** Explore the dynamic factors and pivotal market trends and how they will shape future market developments.

**Actionable Recommendations:** Utilize the insights to exercise strategic decisions to uncover new business streams and revenues in a dynamic environment.

**Caters to a Wide Audience:** Beneficial and cost-effective for startups, research institutions, consultants, SMEs, and large enterprises.

What do businesses use our reports for?

Industry and Market Insights, Opportunity Assessment, Product Demand Forecasting, Market Entry Strategy, Geographical Expansion, Capital Investment Decisions, Regulatory Framework & Implications, New Product Development, Competitive Intelligence

Report Coverage:

Historical data from 2021 to 2025 & forecast data from 2026 to 2031

Growth Opportunities, Challenges, Supply Chain Outlook, Regulatory Framework, and Trend Analysis

Competitive Positioning, Strategies, and Market Share Analysis

Revenue Growth and Forecast Assessment of segments and regions including countries

Company Profiling (Strategies, Products, Financial Information, and Key

Developments among others.

## Intrusion Prevention System (IPS) Market Segmentation

### By Component

Hardware

Software

Services

### By Type

Network-Based Intrusion Prevention System (IPS)

Host-Based Intrusion Prevention System (IPS)

Others

### By Method

Signature-Based

Anomaly-Based

Policy-Based

### By Deployment

Cloud

On-Premise

### By Enterprise Size

Small

Medium

Large

By End-User

BFSI

Healthcare

IT & Telecommunication

Manufacturing

Retail

Others

By Geography

North America

United States

Canada

Mexico

South America

Brazil

Argentina

Others

Europe

United Kingdom

Germany

France

Spain

Others

Middle East and Africa

Saudi Arabia

UAE

Others

Asia Pacific

China

Japan

India

South Korea

Indonesia

Thailand

Others

## Contents

### **1. EXECUTIVE SUMMARY**

### **2. MARKET SNAPSHOT**

- 2.1. Market Overview
- 2.2. Market Definition
- 2.3. Scope of the Study
- 2.4. Market Segmentation

### **3. BUSINESS LANDSCAPE**

- 3.1. Market Drivers
- 3.2. Market Restraints
- 3.3. Market Opportunities
- 3.4. Porter's Five Forces Analysis
- 3.5. Industry Value Chain Analysis
- 3.6. Policies and Regulations
- 3.7. Strategic Recommendations

### **4. TECHNOLOGICAL OUTLOOK**

### **5. INTRUSION PREVENTION SYSTEM (IPS) MARKET BY COMPONENT**

- 5.1. Introduction
- 5.2. Hardware
- 5.3. Software
- 5.4. Services

### **6. INTRUSION PREVENTION SYSTEM (IPS) MARKET BY TYPE**

- 6.1. Introduction
- 6.2. Network-Based Intrusion Prevention System (IPS)
- 6.3. Host-Based Intrusion Prevention System (IPS)
- 6.4. Others

### **7. INTRUSION PREVENTION SYSTEM (IPS) MARKET BY METHOD**

- 7.1. Introduction
- 7.2. Signature-Based
- 7.3. Anomaly-Based
- 7.4. Policy-Based

## **8. INTRUSION PREVENTION SYSTEM (IPS) MARKET BY DEPLOYMENT**

- 8.1. Introduction
- 8.2. Cloud
- 8.3. On-Premise

## **9. INTRUSION PREVENTION SYSTEM (IPS) MARKET BY ENTERPRISE SIZE**

- 9.1. Introduction
- 9.2. Small
- 9.3. Medium
- 9.4. Large

## **10. INTRUSION PREVENTION SYSTEM (IPS) MARKET BY END-USER**

- 10.1. Introduction
- 10.2. BFSI
- 10.3. Healthcare
- 10.4. IT & Telecommunication
- 10.5. Manufacturing
- 10.6. Retail
- 10.7. Others

## **11. INTRUSION PREVENTION SYSTEM (IPS) MARKET BY GEOGRAPHY**

- 11.1. Introduction
- 11.2. North America
  - 11.2.1. USA
  - 11.2.2. Canada
  - 11.2.3. Mexico
- 11.3. South America
  - 11.3.1. Brazil
  - 11.3.2. Argentina
  - 11.3.3. Others

- 11.4. Europe
  - 11.4.1. Germany
  - 11.4.2. France
  - 11.4.3. United Kingdom
  - 11.4.4. Spain
  - 11.4.5. Others
- 11.5. Middle East and Africa
  - 11.5.1. Saudi Arabia
  - 11.5.2. UAE
  - 11.5.3. Others
- 11.6. Asia Pacific
  - 11.6.1. China
  - 11.6.2. India
  - 11.6.3. Japan
  - 11.6.4. South Korea
  - 11.6.5. Indonesia
  - 11.6.6. Thailand
  - 11.6.7. Others

## **12. COMPETITIVE ENVIRONMENT AND ANALYSIS**

- 12.1. Major Players and Strategy Analysis
- 12.2. Market Share Analysis
- 12.3. Mergers, Acquisitions, Agreements, and Collaborations
- 12.4. Competitive Dashboard

## **13. COMPANY PROFILES**

- 13.1. Fortinet Inc.
- 13.2. Broadcom Inc.
- 13.3. Check Point Software Technologies Ltd.
- 13.4. Cisco Systems, Inc.
- 13.5. Hewlett Packard Enterprise
- 13.6. Trellix
- 13.7. Palo Alto Networks
- 13.8. IBM
- 13.9. Sophos Limited
- 13.10. Hillstone Networks

## **14. APPENDIX**

- 14.1. Currency
- 14.2. Assumptions
- 14.3. Base and Forecast Years Timeline
- 14.4. Key Benefits for the Stakeholders
- 14.5. Research Methodology
- 14.6. Abbreviations

## I would like to order

Product name: Intrusion Prevention System Market - Forecast from 2026 to 2031

Product link: <https://marketpublishers.com/r/l6C6476FCE4EEN.html>

Price: US\$ 3,950.00 (Single User License / Electronic Delivery)

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

[info@marketpublishers.com](mailto:info@marketpublishers.com)

## Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/l6C6476FCE4EEN.html>