

Network Security Market By Solution (Firewall/Next Generation Firewall, Secure Web Gateways, Unified Threat Management, Network Detection & Response, Network Access Control), Network Environment (Branch, Campus, Data Center)- Global Forecast to 2030

Market Report | 2025-12-05 | 465 pages | MarketsandMarkets

AVAILABLE LICENSES:

- Single User \$4950.00
- Multi User \$6650.00
- Corporate License \$8150.00
- Enterprise Site License \$10000.00

Report description:

The network security market is projected to grow from USD 84.50 billion in 2025 to USD 119.70 billion by 2030 at a Compound Annual Growth Rate (CAGR) of 7.2% during the forecast period. The market is driven by the increasing frequency and sophistication of cyberattacks targeting hybrid networks, cloud workloads, and encrypted traffic, prompting organizations to strengthen both perimeter and internal defenses. At the same time, the growing BYOD trend is expanding enterprise attack surfaces as personal devices connect to corporate environments, necessitating the implementation of strict access controls, continuous monitoring, and advanced threat prevention. Together, these factors accelerate the adoption of next-generation network security solutions across industries.

<https://mnimg.marketsandmarkets.com/Images/network-security-market-img-overview.webp>

"By network environment, the data center network security segment is expected to hold the largest market size during the forecast period."

Data center network security is expected to be the largest segment in the network environment because data centers house the bulk of sensitive workloads, large volumes of structured/unstructured data, virtualized environments, and mission-critical applications. As enterprises consolidate operations, virtualize servers, and adopt hybrid cloud strategies, data centers become high-value targets for attackers, including advanced persistent threats, insider threats, and lateral movement attacks, as well as data exfiltration, DDoS, and application-layer breaches. To safeguard these assets, organizations deploy robust security

measures, including segmentation, micro-segmentation, intrusion detection/prevention, next-generation firewalls, secure access controls, and continuous monitoring. The importance of uptime, regulatory compliance, data confidentiality, and performance optimization ensures that data-center security remains central. Given the concentration of risk and value, data center network security continues to command the largest share of network security investments.

"By vertical, the cloud segment is projected to register the highest CAGR during the forecast period."

The healthcare and life sciences vertical is the fastest-growing sector due to rising digitization, regulatory pressure such as data privacy laws, the adoption of telemedicine, cloud-based patient data management, and the increasing interconnectedness of medical devices (IoMT - Internet of Medical Things). Hospitals, laboratories, and research institutions handle sensitive patient data, intellectual property, and mission-critical systems. The growing frequency of ransomware attacks, data breaches, and disruption risks necessitates the implementation of advanced security measures, including encryption, zero-trust access, secure network segmentation, cloud security, and continuous monitoring. As healthcare organizations modernize, move to cloud-based record systems, and collaborate globally, they require scalable, reliable, and compliant network security, prompting a surging demand and positioning the healthcare & life sciences sector as the fastest-growing vertical in the network security market.

By deployment mode, the on-premises segment is expected to lead in terms of market share during the forecast period.

On-premises deployment remains the dominant deployment mode in network security because many organizations, especially large enterprises, government institutions, and regulated industries, prefer full control over their security infrastructure, data residency, performance, and latency. On-premises setups allow organizations to integrate security tools tightly with legacy systems, internal networks, and existing infrastructure. They can customize configurations, enforce strict access policies, and apply segmentation in ways that suit internal governance rules. For compliance-driven sectors such as banking, finance, and government, data sovereignty and regulatory mandates often require sensitive data to remain on-site. Additionally, on-premises deployments eliminate potential cloud-related latency, visibility, or vendor dependency issues. Because of these factors, many enterprises continue to rely on on-premises security infrastructure, sustaining its position as the largest deployment mode segment.

Breakdown of Primaries

The study draws insights from a range of industry experts, including component suppliers, Tier 1 companies, and OEMs. The break-up of the primaries is as follows:

- By Company Type: Tier 1 - 40%, Tier 2 - 35%, and Tier 3 - 25%
- By Designation: Directors - 45%, Managers - 35%, Others - 20%
- By Region: North America - 35%, Europe - 30%, Asia Pacific - 25%, Middle East & Africa - 5%, Latin America - 5%

Major vendors in the network security market include Cisco (US), Palo Alto Networks (US), Fortinet (US), Check Point (US), Trend Micro (Japan), Verizon (US), IBM (US), Broadcom (US), Juniper Networks (US), Akamai (US), Netskope (US), Microsoft (US), CrowdStrike (US), Zscaler (US), Cloudflare (US), AWS (US), OpenText (Canada), Hillstone Networks (US), Barracuda Networks (US), Huawei (China), Trellix (US), SonicWall (US), Forcepoint (US), Sophos (UK), Ivanti (US), Extreme Networks (US), Zyxel Networks (Taiwan), Cato Networks (Israel), NordLayer (US), Versa Networks (US), Wijungle (India), Cynet (US), SECNAP Network Security (US), Nomios (Netherlands), easi (Belgium), GajShield (India), Stellar Cyber (US), NETSCOUT (US), and Fidelis Security (US).

The study includes an in-depth competitive analysis of the key players in the network security market, their company profiles, recent developments, and key market strategies.

Research Coverage

The report segments the network security market and forecasts its size based on solution (firewall/next-generation firewall, virtual private network, network access control, data loss prevention, intrusion detection/intrusion prevention systems, secure web gateways, distributed denial-of-service mitigation, unified threat management, network detection & response, and other solutions such as URL/content filtering, web/DNS filtering, and vulnerability scanning), service (professional services-including design, consulting & implementation, risk & threat assessment, training & education, support & maintenance-and managed services), network environment (branch, campus, and data center network security), deployment mode (cloud, on-premises, and hybrid), organization size (large enterprises and small & medium-sized enterprises), and vertical (BFSI, government, healthcare & life sciences, manufacturing, IT & ITeS, retail & e-commerce, energy & utilities, telecommunications, transportation & logistics, media & entertainment, aerospace & defense, and other verticals such as education, construction, real estate, and travel & hospitality).

The study also includes an in-depth competitive analysis of the market's key players, their company profiles, key observations related to product and business offerings, recent developments, and key market strategies.

Key Benefits of Buying the Report

The report will help market leaders/new entrants with information on the closest approximations of revenue numbers for the overall network security market and its subsegments. This report will help stakeholders understand the competitive landscape and gain valuable insights to better position their businesses and plan suitable go-to-market strategies. The report also helps stakeholders understand the market pulse and provides information on key market drivers, restraints, challenges, and opportunities.

The report provides insights into the following pointers:

- Analysis of key drivers (Increasing frequency and sophistication of cyberattacks, Growing BYOD trend necessitating network security measures, Rising cloud adoption and remote work trend), restraints (High implementation costs, Shortage of skilled cybersecurity professionals), opportunities (Simplified management and enhanced protection achieved using secure access service edge framework, Implementation of zero-trust approach in network security), and challenges (Lack of awareness and training concerning network security technologies, Integration complexities)
- Product Development/Innovation: Detailed insights on upcoming technologies, research & development activities, and new product & service launches in the network security market
- Market Development: Comprehensive information about lucrative markets - the report analyses the network security market across varied regions
- Market Diversification: Exhaustive information about new products & services, untapped geographies, recent developments, and investments in the network security market
- Competitive Assessment: In-depth assessment of market shares, growth strategies, and service offerings of leading players in the network security market, including Palo Alto Networks (US), Cisco (US), CrowdStrike (US), Check Point (Israel), and Trend Micro (Japan)

Table of Contents:

1	INTRODUCTION	40
1.1	STUDY OBJECTIVES	40
1.2	MARKET DEFINITION	40
1.3	STUDY SCOPE AND SEGMENTATION	41
1.3.1	MARKETS COVERED AND REGIONAL SCOPE	41
1.3.2	INCLUSIONS AND EXCLUSIONS	42
1.3.3	YEARS CONSIDERED	43
1.3.4	CURRENCY CONSIDERED	43
1.3.5	STAKEHOLDERS	44
1.3.6	SUMMARY OF CHANGES	44
2	RESEARCH METHODOLOGY	45
2.1	RESEARCH DATA	45
2.1.1	SECONDARY DATA	46
2.1.2	PRIMARY DATA	47
2.1.2.1	Breakup of primaries	47
2.1.2.2	Key industry insights	48
2.2	MARKET SIZE ESTIMATION	48
2.2.1	TOP-DOWN APPROACH	49
2.2.2	BOTTOM-UP APPROACH	51
2.3	MARKET DATA TRIANGULATION	52
2.4	FACTOR ANALYSIS	53
2.5	RESEARCH ASSUMPTIONS	54

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

2.6	RESEARCH LIMITATIONS	55
3	EXECUTIVE SUMMARY	56
3.1	KEY INSIGHTS AND MARKET HIGHLIGHTS	56
3.2	KEY MARKET PARTICIPANTS: SHARE INSIGHTS & STRATEGIC DEVELOPMENTS	58
3.3	DISRUPTIVE TRENDS SHAPING MARKET	59
3.4	HIGH-GROWTH SEGMENTS & EMERGING FRONTIERS	60
3.5	SNAPSHOT: GLOBAL MARKET SIZE, GROWTH RATE, AND FORECAST	61
4	PREMIUM INSIGHTS	62
4.1	ATTRACTIVE OPPORTUNITIES FOR PLAYERS IN NETWORK SECURITY MARKET	62
4.2	NETWORK SECURITY MARKET, BY SOLUTION	62
4.3	NETWORK SECURITY MARKET, BY SERVICE	63
4.4	NETWORK SECURITY MARKET, BY NETWORK ENVIRONMENT	63
4.5	NETWORK SECURITY MARKET, BY ORGANIZATION SIZE	64
4.6	NETWORK SECURITY MARKET, BY DEPLOYMENT MODE	64
4.7	NETWORK SECURITY MARKET, BY VERTICAL	65
4.8	NETWORK SECURITY MARKET, BY REGION	65
5	MARKET OVERVIEW	66
5.1	INTRODUCTION	66
5.2	MARKET DYNAMICS	66
5.2.1	DRIVERS	67
5.2.1.1	Increasing frequency and sophistication of cyberattacks	67
5.2.1.2	Growing BYOD trend necessitating network security measures	67
5.2.1.3	Increased cloud adoption and remote work trend	68
5.2.2	RESTRAINTS	68
5.2.2.1	High implementation costs	68
5.2.2.2	Shortage of skilled cybersecurity professionals	68
5.2.3	OPPORTUNITIES	69
5.2.3.1	Simplified management and enhanced protection using SASE framework	69
5.2.3.2	Implementation of zero-trust approach in network security	69
5.2.4	CHALLENGES	70
5.2.4.1	Lack of awareness and training on network security technologies	70
5.2.4.2	Integration complexities	70
5.3	UNMET NEEDS AND WHITE SPACES	70
5.4	INTERCONNECTED MARKETS AND CROSS-SECTOR OPPORTUNITIES	72
5.4.1	BFSI	72
5.4.2	HEALTHCARE & LIFE SCIENCES	72
5.4.3	GOVERNMENT	72
5.4.4	IT & ITES	73
5.4.5	TELECOMMUNICATIONS	73
5.5	STRATEGIC MOVES BY TIER 1/2/3 PLAYERS	73
5.5.1	STRATEGIC TRENDS	74
5.5.1.1	Rise of secure access service edge (SASE)	75
5.5.1.2	Adoption of zero trust network principles	75
5.5.1.3	AI-driven network analytics and automated threat response	75
5.5.1.4	Convergence of networking and security platforms	75
5.5.1.5	Privacy-preserving network inspection and encrypted traffic visibility	76
6	INDUSTRY TRENDS	77

6.1 PORTER'S FIVE FORCES ANALYSIS	77
6.1.1 THREAT OF NEW ENTRANTS	78
6.1.2 THREAT OF SUBSTITUTES	78
6.1.3 BARGAINING POWER OF SUPPLIERS	78
6.1.4 BARGAINING POWER OF BUYERS	78
6.1.5 INTENSITY OF COMPETITIVE RIVALRY	78
6.2 MACROECONOMIC INDICATORS	79
6.2.1 INTRODUCTION	79
6.2.2 GDP TRENDS AND FORECAST	79
6.2.3 TRENDS IN GLOBAL ICT INDUSTRY	81
6.2.4 TRENDS IN GLOBAL CYBERSECURITY INDUSTRY	81
6.3 VALUE CHAIN ANALYSIS	82
6.3.1 PLANNING AND DESIGNING	82
6.3.2 NETWORK SECURITY SOLUTION AND SERVICE PROVIDERS	83
6.3.3 SYSTEM INTEGRATION	83
6.3.4 DISTRIBUTION/RESELLERS/VALUE-ADDED RESELLERS	83
6.3.5 END USERS	83
6.4 ECOSYSTEM ANALYSIS	83
6.5 PRICING ANALYSIS	85
6.5.1 AVERAGE SELLING PRICE, BY SOLUTION, 2025	86
6.5.2 INDICATIVE PRICING ANALYSIS OF PRODUCTS, BY VENDOR, 2025	87
6.6 TRADE ANALYSIS	88
6.6.1 IMPORT SCENARIO (HS CODE 8517)	88
6.6.2 EXPORT SCENARIO (HS CODE 8517)	90
6.7 KEY CONFERENCES & EVENTS, 2025-2026	91
6.8 TRENDS/DISRUPTIONS IMPACTING CUSTOMERS' BUSINESSES	92
6.9 INVESTMENT AND FUNDING SCENARIO	93
6.10 CASE STUDY ANALYSIS	94
6.10.1 JUNIPER NETWORKS HELPED BEELINE ENHANCE EFFICIENCY AND CYBERSECURITY	94
6.10.2 AMANA BANK BUILT A ROBUST AND EASILY MANAGEABLE CYBERSECURITY INFRASTRUCTURE USING SOPHOS' TECHNOLOGIES	94
6.10.3 FORCEPOINT HELPED BURGER KING SECURE SCALABLE NETWORK TRANSITION	95
6.11 IMPACT OF 2025 US TARIFFS-NETWORK SECURITY MARKET	96
6.11.1 INTRODUCTION	96
6.11.2 KEY TARIFF RATES	97
6.11.3 PRICE IMPACT ANALYSIS	98
6.11.4 IMPACT ON COUNTRIES/REGIONS	99
6.11.4.1 North America	99
6.11.4.2 Europe	100
6.11.4.3 Asia Pacific	101
6.11.5 IMPACT ON END-USE INDUSTRIES	102
?	
7 STRATEGIC DISRUPTION THROUGH TECHNOLOGY, PATENTS, DIGITAL, AND AI ADOPTION	104
7.1 KEY EMERGING TECHNOLOGIES	104
7.1.1 FIREWALLS/NEXT-GENERATION FIREWALLS	104
7.1.2 INTRUSION DETECTION SYSTEMS/INTRUSION PREVENTION SYSTEMS	104

7.1.3 VIRTUAL PRIVATE NETWORKS	104
7.1.4 AI/ML	105
7.2 COMPLEMENTARY TECHNOLOGIES	105
7.2.1 SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)	105
7.2.2 NETWORK SEGMENTATION	105
7.2.3 THREAT INTELLIGENCE	106
7.2.4 SECURE ACCESS SERVICE EDGE	106
7.2.5 ZERO TRUST NETWORK ACCESS	106
7.3 TECHNOLOGY/PRODUCT ROADMAP	106
7.3.1 SHORT-TERM (2025-2027) FOUNDATION & EARLY COMMERCIALIZATION	106
7.3.2 MID-TERM (2027-2030) EXPANSION & STANDARDIZATION	107
7.3.3 LONG-TERM (2030-2035+) GLOBAL CONSOLIDATION & INTELLIGENT SECURITY ECOSYSTEMS	108
7.4 PATENT ANALYSIS	109
7.5 FUTURE APPLICATIONS	114
7.5.1 ZERO-TRUST ARCHITECTURES: BEYOND-PERIMETER NETWORK SECURITY	114
7.5.2 AI-POWERED THREAT DETECTION & AUTONOMOUS RESPONSE	115
7.5.3 SECURE ACCESS SERVICE EDGE (SASE) & SECURITY SERVICE EDGE (SSE)	115
7.5.4 OT & ICS CYBERSECURITY FOR CRITICAL INFRASTRUCTURE	116
7.5.5 5G/6G SECURITY & ULTRA-CONNECTED NETWORK DEFENSE	116
7.6 IMPACT OF AI/GEN AI ON NETWORK SECURITY MARKET	116
7.6.1 BEST PRACTICES IN NETWORK SECURITY MARKET	118
7.6.2 CASE STUDIES OF AI IMPLEMENTATION IN THE NETWORK SECURITY MARKET	118
7.6.3 INTERCONNECTED ADJACENT ECOSYSTEM AND IMPACT ON MARKET PLAYERS	119
7.6.4 CLIENTS' READINESS TO ADOPT GENERATIVE AI IN NETWORK SECURITY MARKET	119
8 REGULATORY LANDSCAPE	120
8.1 REGIONAL REGULATIONS AND COMPLIANCE	120
8.1.1 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS	120
8.1.2 INDUSTRY STANDARDS	125
?	
9 CONSUMER LANDSCAPE & BUYER BEHAVIOR	126
9.1 DECISION-MAKING PROCESS	126
9.2 BUYER STAKEHOLDERS AND BUYING EVALUATION CRITERIA	127
9.2.1 KEY STAKEHOLDERS IN BUYING PROCESS	127
9.2.2 BUYING CRITERIA	128
9.3 ADOPTION BARRIERS & INTERNAL CHALLENGES	128
9.4 UNMET NEEDS FROM VARIOUS END-USE INDUSTRIES	130
10 NETWORK SECURITY MARKET, BY SOLUTION	131
10.1 INTRODUCTION	132
10.1.1 SOLUTIONS: NETWORK SECURITY MARKET DRIVERS	134
10.2 FIREWALL/NEXT-GENERATION FIREWALL	135
10.2.1 NEED FOR SIMPLIFICATION AND AUTOMATION OF ENTERPRISE-GRADE SECURITY WITH CENTRALIZED MANAGEMENT ACROSS DISTRIBUTED NETWORKS TO DRIVE MARKET	135
10.3 VIRTUAL PRIVATE NETWORK	136
10.3.1 INCREASING DEMAND FOR MAINTAINING DATA SECURITY, PRIVACY, AND NETWORK INTEGRITY TO DRIVE MARKET	136
10.4 NETWORK ACCESS CONTROL	137
10.4.1 INCREASING NEED FOR STREAMLINING AUTHENTICATION PROCESS, REDUCING TIME AND COSTS TO FUEL MARKET GROWTH	137

10.5 DATA LOSS PREVENTION	139
10.5.1 DATA LOSS PREVENTION SOLUTIONS TO ENHANCE INTERNAL SECURITY AND MAINTAIN REGULATORY COMPLIANCE	139
10.6 INTRUSION DETECTION SYSTEM/INTRUSION PREVENTION SYSTEM	140
10.6.1 INCREASING DEMAND FOR ROBUST NETWORK SECURITY TO BOOST MARKET	140
10.7 SECURE WEB GATEWAY	141
10.7.1 SURGING DEMAND FOR SAFE INTERNET ACCESS TO DRIVE MARKET	141
10.8 DISTRIBUTED DENIAL-OF-SERVICE MITIGATION	142
10.8.1 RISING NEED TO PROTECT CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF RESOURCES TO FUEL MARKET GROWTH	142
10.9 UNIFIED THREAT MANAGEMENT	143
10.9.1 RISING POPULARITY OF UNIFIED THREAT MANAGEMENT SOLUTIONS TO DRIVE MARKET	143
10.10 NETWORK DETECTION AND RESPONSE	144
10.10.1 DELIVERS THREAT DETECTION, INCIDENT RESPONSE, AND FORENSICS FROM A UNIFIED NETWORK-CENTRIC PERSPECTIVE	144
11 NETWORK SECURITY MARKET, BY SERVICE	146
11.1 INTRODUCTION	147
11.1.1 SERVICES: NETWORK SECURITY MARKET DRIVERS	148
11.2 PROFESSIONAL SERVICES	148
11.2.1 NEED FOR RAPID RESPONSE TO BREACHES AND EXTERNAL SUPPORT TO DRIVE ADOPTION	148
11.2.2 DESIGN, CONSULTING, AND IMPLEMENTATION	150
11.2.3 RISK & THREAT ASSESSMENT	151
11.2.4 TRAINING & EDUCATION	152
11.2.5 SUPPORT & MAINTENANCE	153
11.3 MANAGED SERVICES	154
11.3.1 INCREASING DEMAND FOR SPECIALIZED SECURITY SERVICES TO BOOST MARKET GROWTH	154
12 NETWORK SECURITY MARKET, BY NETWORK ENVIRONMENT	156
12.1 INTRODUCTION	157
12.1.1 NETWORK ENVIRONMENT: NETWORK SECURITY MARKET DRIVERS	158
12.2 BRANCH NETWORK SECURITY	158
12.2.1 SURGING NEED FOR PROTECTION OF SENSITIVE INFORMATION AND ENFORCING OPERATIONAL CONTINUITY TO DRIVE MARKET	158
12.3 CAMPUS NETWORK SECURITY	159
12.3.1 STRENGTHENED VISIBILITY AND SAFE CONNECTIVITY ACROSS LARGE DISTRIBUTED FACILITIES TO DRIVE MARKET	159
12.4 DATA CENTER NETWORK SECURITY	160
12.4.1 INCREASING NEED FOR ENSURING CRITICAL ASSET AVAILABILITY, RELIABILITY, AND CONFIDENTIALITY TO ACCELERATE MARKET GROWTH	160
13 NETWORK SECURITY MARKET, BY DEPLOYMENT MODE	162
13.1 INTRODUCTION	163
13.1.1 DEPLOYMENT MODE: NETWORK SECURITY MARKET DRIVERS	164
13.2 ON-PREMISES	164
13.2.1 ON-PREMISES DEPLOYMENT TO HELP MAINTAIN COMPLIANCE, PROTECT DATA, AND CUSTOMIZE SECURITY CONFIGURATIONS	164
13.3 CLOUD	165
13.3.1 COST-EFFECTIVENESS AND EASE OF MAINTENANCE TO BOOST DEMAND FOR CLOUD-BASED SOLUTIONS	165
13.4 HYBRID	166
13.4.1 HYBRID APPROACH TO OFFER DATA SECURITY, FLEXIBILITY, COST-EFFICIENCY, AND THE RAPID DEPLOYMENT CAPABILITIES OF CLOUD SERVICES	166
14 NETWORK SECURITY MARKET, BY ORGANIZATION SIZE	168

14.1 INTRODUCTION 169

14.1.1 ORGANIZATION SIZE: NETWORK SECURITY MARKET DRIVERS 170

14.2 LARGE ENTERPRISES 170

14.2.1 INCREASING NEED FOR EFFECTIVE SECURITY MANAGEMENT TO BOOST MARKET 170

14.3 SMALL & MEDIUM-SIZED ENTERPRISES 171

14.3.1 INCREASING CYBER THREATS, REGULATORY COMPLIANCE REQUIREMENTS, AND NEED FOR PROTECTION OF SENSITIVE DATA TO DRIVE MARKET 171

?

15 NETWORK SECURITY MARKET, BY VERTICAL 173

15.1 INTRODUCTION 174

15.1.1 VERTICAL: NETWORK SECURITY MARKET DRIVERS 176

15.2 BANKING, FINANCIAL SERVICES, AND INSURANCE (BFSI) 177

15.2.1 INCREASING DEMAND FOR MAINTAINING COMPETITIVE EDGE, REDUCING COSTS, AND IMPROVING CUSTOMER EXPERIENCE WITH VALUE-ADDED SERVICES TO DRIVE MARKET 177

15.3 GOVERNMENT 178

15.3.1 NETWORK SECURITY SOLUTIONS TO HELP IMPROVE SECURITY OF CRITICAL INFORMATION AND REDUCE THREAT OF UNAUTHORIZED ACCESS 178

15.4 HEALTHCARE & LIFE SCIENCES 179

15.4.1 RISING USE OF NETWORK SECURITY SOLUTIONS AND INCREASING AWARENESS OF REGULATORY COMPLIANCE TO DRIVE MARKET 179

15.5 AEROSPACE & DEFENSE 180

15.5.1 SURGING DEMAND FOR OPERATIONAL EFFECTIVENESS AND NATIONAL SECURITY TO PROPEL MARKET 180

15.6 MANUFACTURING 181

15.6.1 INCREASING DEMAND FOR EFFICIENT REAL-TIME DATA ACCESS AND SECURE NETWORK CONNECTIVITY TO PROPEL MARKET 181

15.7 IT & ITES 182

15.7.1 INCREASING SHIFT TOWARD HYBRID AND REMOTE WORK MODELS TO HEIGHTEN DEMAND FOR SECURE REMOTE ACCESS SOLUTIONS 182

15.8 RETAIL & ECOMMERCE 183

15.8.1 RISING NETWORK-BASED CYBER-ATTACKS AND DATA THEFT ACTIVITIES TO BOOST ADOPTION OF NETWORK SECURITY SOLUTIONS 183

15.9 ENERGY & UTILITIES 184

15.9.1 NEED TO STRENGTHEN NETWORK SECURITY AND REDUCE COMPLEXITIES TO FUEL ADOPTION 184

15.10 TELECOMMUNICATIONS 185

15.10.1 NEED TO PROTECT VAST AND COMPLEX COMMUNICATION NETWORKS FROM CYBER THREATS TO PROPEL MARKET 185

15.11 TRANSPORTATION & LOGISTICS 186

15.11.1 STRENGTHENING TRANSPORTATION AND LOGISTICS OPERATIONS THROUGH ENHANCED NETWORK SECURITY TO PROPEL MARKET 186

15.12 MEDIA & ENTERTAINMENT 188

15.12.1 NETWORK SECURITY MEASURES TO SAFEGUARD AGAINST UNAUTHORIZED ACCESS, ENSURE THE INTEGRITY OF CONTENT, AND PROTECT CONSUMER PRIVACY 188

15.13 OTHER VERTICALS 189

?

16 NETWORK SECURITY MARKET, BY REGION 191

16.1 INTRODUCTION 192

16.2 NORTH AMERICA 193

16.2.1 NORTH AMERICA: NETWORK SECURITY MARKET DRIVERS 194

16.2.2 US 200

16.2.2.1 Increasing network attacks, cyber threats, and evolving regulatory norms to boost market 200

16.2.3 CANADA 205

16.2.3.1 Rapid digitalization and government initiatives to boost market 205

16.3 EUROPE 210

16.3.1 EUROPE: NETWORK SECURITY MARKET DRIVERS 211

16.3.2 UK 217

16.3.2.1 Surging demand for bolstering cybersecurity to drive market 217

16.3.3 GERMANY 222

16.3.3.1 Increasing cybercrimes and sophisticated cyberattacks to boost market 222

16.3.4 FRANCE 227

16.3.4.1 Compliance with stringent EU regulations to drive adoption of comprehensive security frameworks 227

16.3.5 ITALY 232

16.3.5.1 Adoption of modern network security solutions to protect digital infrastructure to drive market 232

16.3.6 REST OF EUROPE 237

16.4 ASIA PACIFIC 237

16.4.1 ASIA PACIFIC: NETWORK SECURITY MARKET DRIVERS 238

16.4.2 CHINA 244

16.4.2.1 Rapid digitalization and growing importance of safeguarding country's expansive digital economy to boost market 244

16.4.3 JAPAN 249

16.4.3.1 Intricate cyberattacks to drive adoption of network security solutions 249

16.4.4 INDIA 254

16.4.4.1 Increased internet penetration, improved telecom services, and government initiatives to drive market 254

16.4.5 SINGAPORE 259

16.4.5.1 Growing emphasis on cybersecurity measures and increasing investments in advanced network security measures to foster market growth 259

16.4.6 REST OF ASIA PACIFIC 264

16.5 MIDDLE EAST & AFRICA 264

16.5.1 MIDDLE EAST & AFRICA: NETWORK SECURITY MARKET DRIVERS 265

16.5.2 MIDDLE EAST 271

16.5.2.1 Rapid expansion of connected systems accelerating the demand for comprehensive network security solutions 271

16.5.2.2 GCC 277

16.5.2.3 UAE 283

16.5.2.3.1 Digital transformation and increasing cyber threats to drive adoption of modern network security solutions 283

16.5.2.4 KSA 288

16.5.2.4.1 Digital transformation and evolving threat landscape to boost market 288

16.5.2.5 Rest of GCC countries 293

16.5.3 REST OF MIDDLE EAST 293

16.5.4 AFRICA 294

16.5.4.1 Rising cyber risks and increasing digital adoption driving the growth of network security market 294

16.6 LATIN AMERICA 299

16.6.1 BRAZIL 305

16.6.1.1 Rising DDoS attacks in Brazil to propel market growth 305

16.6.2 MEXICO 310

16.6.2.1 Increasing demand for protection of sensitive information to bolster market growth 310

16.6.3 REST OF LATIN AMERICA 315

17 COMPETITIVE LANDSCAPE 316

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

17.1 KEY PLAYER STRATEGIES/RIGHT TO WIN	316
17.2 REVENUE ANALYSIS	318
17.3 MARKET SHARE ANALYSIS	319
17.4 BRAND/PRODUCT COMPARISON	322
17.5 COMPANY VALUATION AND FINANCIAL METRICS	323
17.5.1 COMPANY VALUATION, 2025	323
17.5.2 FINANCIAL METRICS USING EV/EBITDA, 2025	324
17.6 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2024	324
17.6.1 STARS	325
17.6.2 EMERGING LEADERS	325
17.6.3 PERVERSIVE PLAYERS	325
17.6.4 PARTICIPANTS	325
17.6.5 COMPANY FOOTPRINT: KEY PLAYERS, 2024	327
17.6.5.1 Company footprint	327
17.6.5.2 Region footprint	328
17.6.5.3 Solution footprint	329
17.6.5.4 Service footprint	330
17.6.5.5 Vertical footprint	331
17.7 COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2024	332
17.7.1 PROGRESSIVE COMPANIES	333
17.7.2 RESPONSIVE COMPANIES	333
17.7.3 DYNAMIC COMPANIES	333
17.7.4 STARTING BLOCKS	333
17.7.5 COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2024	335
17.7.5.1 Detailed list of key startups/SMEs	335
17.7.5.2 Competitive benchmarking of key startups/SMEs	336
17.8 COMPETITIVE SCENARIO	338
17.8.1 PRODUCT LAUNCHES AND ENHANCEMENTS	338
17.8.2 DEALS	339
18 COMPANY PROFILES	341
18.1 MAJOR PLAYERS	341
18.1.1 PALO ALTO NETWORKS	341
18.1.1.1 Business overview	341
18.1.1.2 Products/Solutions/Services offered	343
18.1.1.3 Recent developments	345
18.1.1.3.1 Product launches and enhancements	345
18.1.1.3.2 Deals	347
18.1.1.4 MnM view	348
18.1.1.4.1 Key strengths	348
18.1.1.4.2 Strategic choices made	348
18.1.1.4.3 Weaknesses and competitive threats	348
18.1.2 CISCO	349
18.1.2.1 Business overview	349
18.1.2.2 Products/Solutions/Services offered	350
18.1.2.3 Recent developments	355
18.1.2.3.1 Product launches and enhancements	355
18.1.2.3.2 Deals	356

18.1.2.4 MnM view 356
18.1.2.4.1 Key strengths 356
18.1.2.4.2 Strategic choices made 357
18.1.2.4.3 Weaknesses and competitive threats 357
18.1.3 FORTINET 358
18.1.3.1 Business overview 358
18.1.3.2 Products/Solutions/Services offered 359
18.1.3.3 Recent developments 362
18.1.3.3.1 Product launches and enhancements 362
18.1.3.3.2 Deals 364
18.1.3.4 MnM view 364
18.1.3.4.1 Key strengths 364
18.1.3.4.2 Strategic choices made 364
18.1.3.4.3 Weaknesses and competitive threats 365
18.1.4 CHECK POINT 366
18.1.4.1 Business overview 366
18.1.4.2 Products/Solutions/Services offered 367
18.1.4.3 Recent developments 370
18.1.4.3.1 Product launches 370
18.1.4.3.2 Deals 371
18.1.4.4 MnM view 372
18.1.4.4.1 Key strengths 372
18.1.4.4.2 Strategic choices made 372
18.1.4.4.3 Weaknesses and competitive threats 372
18.1.5 TREND MICRO 373
18.1.5.1 Business overview 373
18.1.5.2 Products/Solutions/Services offered 374
18.1.5.3 Recent developments 375
18.1.5.3.1 Product launches 375
18.1.5.3.2 Deals 375
18.1.5.4 MnM view 375
18.1.5.4.1 Key strengths 375
18.1.5.4.2 Strategic choices made 376
18.1.5.4.3 Weaknesses and competitive threats 376
18.1.6 VERIZON 377
18.1.6.1 Business overview 377
18.1.6.2 Products/Solutions/Services offered 378
18.1.6.3 Recent developments 380
18.1.6.3.1 Product launches 380
18.1.6.3.2 Deals 380
18.1.7 IBM 381
18.1.7.1 Business overview 381
18.1.7.2 Products/Solutions/Services offered 382
18.1.7.3 Recent developments 384
18.1.7.3.1 Product enhancements 384
18.1.7.3.2 Deals 384
18.1.8 BROADCOM 385

18.1.8.1 Business overview 385
18.1.8.2 Products/Solutions/Services offered 386
18.1.8.3 Recent developments 389
18.1.8.3.1 Product launches and enhancements 389
18.1.8.3.2 Deals 389
18.1.9 JUNIPER NETWORKS 390
18.1.9.1 Business overview 390
18.1.9.2 Products/Solutions/Services offered 391
18.1.9.3 Recent developments 395
18.1.9.3.1 Product launches and enhancements 395
18.1.9.3.2 Deals 396
?
18.1.10 AKAMAI 397
18.1.10.1 Business overview 397
18.1.10.2 Products/Solutions/Services offered 399
18.1.10.3 Recent developments 401
18.1.10.3.1 Product launches 401
18.1.10.3.2 Deals 402
18.1.11 NETSKOPE 403
18.1.11.1 Business overview 403
18.1.11.2 Products/Solutions/Services offered 403
18.1.11.3 Recent developments 404
18.1.11.3.1 Product launches 404
18.1.11.3.2 Deals 405
18.1.12 MICROSOFT 406
18.1.12.1 Business overview 406
18.1.12.2 Products/Solutions/Services offered 407
18.1.12.3 Recent developments 410
18.1.12.3.1 Deals 410
18.1.13 CROWDSTRIKE 411
18.1.13.1 Business overview 411
18.1.13.2 Products/Solutions/Services offered 412
18.1.13.3 Recent developments 413
18.1.13.3.1 Deals 413
18.1.14 HUAWEI 414
18.1.14.1 Business overview 414
18.1.14.2 Products/Solutions/Services offered 415
18.1.14.3 Recent developments 418
18.1.14.3.1 Product launches 418
18.1.14.3.2 Deals 419
18.1.15 BARRACUDA NETWORKS 420
18.1.15.1 Business overview 420
18.1.15.2 Products/Solutions/Services offered 420
18.1.15.3 Recent developments 422
18.1.15.3.1 Product launches and enhancements 422
18.1.15.3.2 Deals 423
18.1.16 ZSCALER 424

18.1.16.1 Business overview	424
18.1.16.2 Products/Solutions/Services offered	425
18.1.16.3 Recent developments	427
18.1.16.3.1 Product launches	427
18.1.16.3.2 Deals	427
?	
18.1.17 TRELLIX	429
18.1.17.1 Business overview	429
18.1.17.2 Products/Solutions/Services offered	429
18.1.17.3 Recent developments	431
18.1.17.3.1 Product launches	431
18.1.17.3.2 Deals	431
18.1.18 CLOUDFLARE	432
18.1.18.1 Business overview	432
18.1.18.2 Products/Solutions/Services offered	434
18.1.18.3 Recent developments	435
18.1.18.3.1 Product launches and enhancements	435
18.1.18.3.2 Deals	436
18.2 OTHER PLAYERS	437
18.2.1 AMAZON WEB SERVICES	437
18.2.2 OPENTEXT	438
18.2.3 SONICWALL	439
18.2.4 FORCEPOINT	440
18.2.5 SOPHOS	441
18.2.6 ZYXEL NETWORKS	442
18.2.7 NORDLAYER	443
18.2.8 CATO NETWORKS	444
18.2.9 HILLSTONE NETWORKS	445
18.2.10 VERSA NETWORKS	446
18.2.11 WIJUNGLE	447
18.2.12 CYNET	448
18.2.13 SECNAP	449
18.2.14 NOMIOS	449
18.2.15 EASI	450
18.2.16 GAJSHIELD	450
18.2.17 STELLAR CYBER	451
18.2.18 STAMUS NETWORKS	452
18.2.19 CORELIGHT	453
18.2.20 NETSCOUT	454
18.2.21 FIDELIS SECURITY	455
19 APPENDIX	456
19.1 DISCUSSION GUIDE	456
19.2 KNOWLEDGESTORE: MARKETSANDMARKETS' SUBSCRIPTION PORTAL	461
19.3 CUSTOMIZATION OPTIONS	463
19.4 RELATED REPORTS	463
19.5 AUTHOR DETAILS	464

Network Security Market By Solution (Firewall/Next Generation Firewall, Secure Web Gateways, Unified Threat Management, Network Detection & Response, Network Access Control), Network Environment (Branch, Campus, Data Center)- Global Forecast to 2030

Market Report | 2025-12-05 | 465 pages | MarketsandMarkets

To place an Order with Scotts International:

- Print this form
- Complete the relevant blank fields and sign
- Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User	\$4950.00
	Multi User	\$6650.00
	Corporate License	\$8150.00
	Enterprise Site License	\$10000.00
		VAT
		Total

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*	<input type="text"/>	Phone*	<input type="text"/>
First Name*	<input type="text"/>	Last Name*	<input type="text"/>
Job title*	<input type="text"/>	EU Vat / Tax ID / NIP number*	
Company Name*	<input type="text"/>	<input type="text"/>	
Address*	<input type="text"/>	City*	<input type="text"/>

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com

Zip Code*

Country*

Date

Signature

Scotts International. EU Vat number: PL 6772247784

tel. 0048 603 394 346 e-mail: support@scotts-international.com

www.scotts-international.com