Security and Vulnerability Management Market by Software (Vulnerability Scanner, Patch Management, SIEM, Risk assessment, Threat Intelligence), Type (Network Security, Application Security, Endpoint Security, and Cloud Security) - Global Forecast to 2030

Market Report | 2024-10-14 | 460 pages | MarketsandMarkets

AVAILABLE LICENSES:

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

Report description:

The global security and vulnerability management market size is projected to grow from USD 16.51 billion in 2024 to USD 24.04 billion by 2030 at a Compound Annual Growth Rate (CAGR) of 6.4% during the forecast period. An increase in security breaches drives the growth of the security and vulnerability management market because of the deployment of third-party applications in existing systems. Organizations are becoming aware of implementing robust security and vulnerability management solutions to avoid financial and critical data loss caused by third-party applications.

"By professional services, consulting and deployment services segment is expected to grow at the highest CAGR during the forecast period."

The consulting and deployment services segment is growing at the highest rate in the security and vulnerability management market due to the increasing complexity of cyber threats and the demand for expert guidance. Organizations facing sophisticated attacks require consulting services for developing customized security approaches according to the regulations and guidelines followed by each organization. High adoption of digital transformation and cloud increases demand for deployment services that can effectively embed the latest security solutions. Ongoing support for cloud environments and IoT devices highly fuels the demand, leaving this segment to grow significantly as businesses take proactive measures in risk management and continuous security improvement.

"By services, penetration testing services hold the largest market size during the forecast period."

Penetration testing services hold the largest market share in the security and vulnerability management market due to organizations' need to protect themselves from emerging cyberattacks. As businesses increasingly face cyber-attacks, the

demand for thorough and proactive penetration testing solutions has also increased. Regulatory compliance requires regular assessments to ensure data safety, creating growth in this segment. Advancements in AI and ML have further enhanced penetration testing services; hence, penetration testing becomes essential in strategy implementations for most organizations to bring about total protection against vulnerabilities.

By Region, Asia Pacific is expected to grow at the highest CAGR during the forecast period.

Growth in the Asia Pacific security and vulnerability management market is trending upward, influenced by increased digitalization in economies, economic expansion, and cyber threats. Increased usage of the internet, combined with digital transformation, is posing enhanced risks for businesses in the region. High-profile data breaches push organizations to be more aware and look for robust security and vulnerability management solutions. Government initiatives regarding new data protection laws and cybersecurity frameworks further boost the security demand. Besides this, awareness among the public, training programs, and competitive forces require these organizations to step up their security posture. This drives industries to adopt advanced security solutions like vulnerability management.

Breakdown of primaries

The study contains insights from various industry experts, from component suppliers to Tier 1 companies and OEMs. The break-up of the primaries is as follows:

-□By Company Type: Tier 1 - 35%, Tier 2 - 45%, and Tier 3 - 20%

-□By Designation: C-level Executives- 35%, Directors - 25%, Others - 40%

-□By Region: North America - 45%, Asia Pacific - 25%, Europe - 20%, Middle East and Africa - 5%, Latin America - 5%

Major vendors in the global Security and vulnerability management market include Microsoft (US), AT&T (US), CrowdStrike (US), IBM (US), Tenable (US), Cisco (US), DXC Technology (US), Check Point Software Technologies (Israel), Rapid7 (US), Qualys (US), ManageEngine (US), RSI Security (US), Fortra (US), Ivanti (US), Tanium (US), Invicti (US), Outpost24 (Sweden), Skybox Security (US), Vulcan Cyber (Israel), SecPod (India), Balbix (US), Intruder (UK), Brinqa (US), Holm Security (Sweden), Nucleus Security (US), and NopSec (US) in the Security and vulnerability management market.

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

Research Coverage

The report segments the security and vulnerability management market and forecasts its size by Component (Software and Services), by software (Vulnerability Scanner, Patch Management, SIAM, Risk Assessment, Threat intelligence and Other Software), by Services (Professional Services, Managed Services), by Type (Endpoint Security, Network Security, Application Security, Cloud Security), by Target (Content Management Vulnerabilities, IoT Vulnerabilities, Application, Programming Interface (API) Vulnerabilities, Other Target Vulnerabilities (Server Technology Vulnerabilities, Database Vulnerabilities), by Deployment Mode (on-premises, cloud), by organization size (small and medium-sized enterprises, large enterprises), by Vertical (Banking, Financial Services, and Insurance (BFSI), Healthcare, Government, Manufacturing, Energy & Utilities, IT & ITeS, Retail & eCommerce, Telecommunications, Travel And Hospitality, Others (Education, Transportation, And Media & Entertainment).

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 the market leaders/new entrants with information on the closest approximations of the revenue numbers for the overall security and vulnerability management market and the subsegments. This report will help stakeholders understand the competitive landscape and gain more insights to position their businesses better 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 on the following pointers:

-□Analysis of key drivers (Increase in vulnerabilities across the globe, growth in the deployment of third-party applications, high monetary losses and loss of critical data due to the absence of vulnerability management solutions, stringent regulatory standards and data privacy compliances), restraints (Difficulty in integrating with existing complex systems), opportunities (Widespread adoption of the industrial revolution, integration of advanced technologies with vulnerability management solutions for

vulnerability prioritization and remediation, integration of vulnerability management and patch management solutions), and challenges (High initial installation, maintenance, and deployment cost, lack of appropriate parameters to prioritize risks, regularizing organizations' vulnerability management program)
-Product Development/Innovation: Detailed insights on upcoming technologies, research & development activities, and new product & service launches in the security and vulnerability management market.
-Market Development: Comprehensive information about lucrative markets - the report analyses the security and vulnerability management market across varied regions.
-Market Diversification: Exhaustive information about new products & services, untapped geographies, recent developments, and investments in the security and vulnerability management market.
-Competitive Assessment: In-depth assessment of market shares, growth strategies, and service offerings of leading players in security and vulnerability management market strategies, including Microsoft (US), AT&T (US), CrowdStrike (US), IBM (US), and Tenable (US).

Table of Contents:

1INTRODUCTION46
1.1STUDY OBJECTIVES46
1.2MARKET DEFINITION46
1.2.1INCLUSIONS AND EXCLUSIONS47
1.3MARKET SCOPE48
1.3.1MARKET SEGMENTATION48
1.4YEARS CONSIDERED49
1.5CURRENCY CONSIDERED49
1.6STAKEHOLDERS50
1.7SUMMARY OF CHANGES50
2RESEARCH METHODOLOGY51
2.1RESEARCH DATA51
2.1.1SECONDARY DATA53
2.1.2PRIMARY DATA53
2.1.2.1Breakup of primary profiles54
2.1.2.2Key industry insights54
2.2DATA TRIANGULATION55
2.3MARKET SIZE ESTIMATION56
2.3.1REVENUE ESTIMATES57
2.4MARKET FORECAST60
2.5RESEARCH ASSUMPTIONS61
2.6RESEARCH LIMITATIONS62
3EXECUTIVE SUMMARY63
4PREMIUM INSIGHTS67
4.1ATTRACTIVE GROWTH OPPORTUNITIES FOR PLAYERS IN SECURITY AND VULNERABILITY MANAGEMENT MARKET67
4.2SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY COMPONENT, 202467
4.3SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY SOFTWARE, 202468
4.4SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY SERVICE, 202469
4.5SECURITY AND VULNERABILITY MANAGEMENT MARKET,
BY PROFESSIONAL SERVICE, 202469
4.6SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY TYPE, 202470
4.7SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY TARGET, 202470
4.8SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY ORGANIZATION SIZE, 202471

4.9 SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY DEPLOYMENT MODE, 2024 71
4.10 SECURITY AND VULNERABILITY MANAGEMENT MARKET,
BY VERTICAL AND REGION, 2024 72
4.11 MARKET INVESTMENT SCENARIO 72
5 MARKET OVERVIEW AND INDUSTRY TRENDS 73
5.1 INTRODUCTION 73
5.2 MARKET DYNAMICS 73
5.2.1 DRIVERS 74
5.2.1.1 Increase in vulnerabilities globally 74
5.2.1.2 Growth in third-party application deployments 75
5.2.1.3 High monetary and critical data losses due to absence of vulnerability management solutions 76
5.2.1.4 Stringent regulatory standards and data privacy compliances 76
5.2.1.5 Security breaches due to internal vulnerabilities 77
5.2.2 RESTRAINTS 77
5.2.2.1 Integration difficulty with existing complex systems 77
5.2.3 OPPORTUNITIES 78
5.2.3.1 Need for advanced security solutions due to increasing industrialization 78
5.2.3.2 Integration of advanced technologies with vulnerability management solutions for vulnerability prioritization and remediation 78
5.2.3.3 Integration of vulnerability management and patch management solutions 78
5.2.4 CHALLENGES 79
5.2.4.1 High initial installation, maintenance, and deployment costs 79
5.2.4.2 Lack of appropriate parameters to prioritize risks 79
5.2.4.3 Regularizing vulnerability management programs of organizations 79
5.3 ECOSYSTEM ANALYSIS 79
5.4 VALUE CHAIN ANALYSIS 81
5.4.1 COMPONENT PROVIDERS 82
5.4.2 TECHNOLOGY PROVIDERS 82
5.4.3 SECURITY SOLUTION AND SERVICE PROVIDERS 82
5.4.4 SYSTEM INTEGRATORS 82
5.4.5 SALES AND DISTRIBUTION 82
5.4.6 END USER GROUPS 82
5.5 PATENT ANALYSIS 82
5.6 PRICING ANALYSIS 86
5.6.1 AVERAGE PRICING ANALYSIS OF SOFTWARE, BY KEY PLAYERS, 2024 86
5.6.2 INDICATIVE PRICING ANALYSIS OF SOFTWARE, BY VENDOR, 2024 87
5.7 TECHNOLOGY ANALYSIS 87
5.7.1 KEY TECHNOLOGIES 87
5.7.1.1 AI/ML 87
5.7.2 COMPLEMENTARY TECHNOLOGIES 87
5.7.2.1 Cloud computing 87
5.7.2.2 Big data and analytics 88
5.7.3 ADJACENT TECHNOLOGIES 88
5.7.3.1 Internet of Things (IoT) 88
5.8 IMPACT OF GEN AI ON SECURITY AND VULNERABILITY MANAGEMENT MARKET 88
5.8.1 TOP USE CASES AND MARKET POTENTIAL 88
5.8.1.1 Key use cases 89

5.8.2 IMPACT OF GEN AI ON INTERCONNECTED AND ADJACENT ECOSYSTEMS 89
5.8.2.1 Big data and analytics 90
5.8.2.2 Endpoint detection and response (EDR) 90
5.8.2.3 Cloud computing 91
5.8.2.4 Internet of Things (IoT) 91
5.9 CASE STUDY ANALYSIS 91
5.9.1 CASE STUDY 1: INFOSYS RELIES ON QUALYS VMDR FOR BETTER VISIBILITY ACROSS RISKS 91
5.9.2 CASE STUDY 2: SAI GLOBAL USES RAPID7'S INSIGHTIDR TO PROTECT CLIENT'S HIGHLY SECURE AND REGULATED DATA 92
5.9.3 CASE STUDY 3: NETWORK INTELLIGENCE CHOSE TRIPWIRE INDUSTRIAL VISIBILITY TO SECURE ITS CRITICAL INFRASTRUCTURE SITES 92
5.9.4 CASE STUDY 4: QUANTIPHI RELIES ON TENABLE VULNERABILITY MANAGEMENT TO REDUCE CYBER RISK IN CLOUD 93
5.10 TRENDS/DISRUPTIONS IMPACTING CUSTOMER BUSINESS 93
5.11 PORTER'S FIVE FORCES ANALYSIS 94
5.11.1 THREAT OF NEW ENTRANTS 95
5.11.2 THREAT OF SUBSTITUTES 95
5.11.3 BARGAINING POWER OF SUPPLIERS 96
5.11.4 BARGAINING POWER OF BUYERS 96
5.11.5 INTENSITY OF COMPETITIVE RIVALRY 96
5.12 KEY STAKEHOLDERS AND BUYING CRITERIA 97
5.12.1 KEY STAKEHOLDERS IN BUYING PROCESS 97
5.12.2 BUYING CRITERIA 98
5.13 REGULATORY LANDSCAPE 98
5.13.1 GENERAL DATA PROTECTION REGULATION 99
5.13.2 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT 99
5.13.3 HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH 99
5.13.4 GOVERNANCE, RISK, AND COMPLIANCE 99
5.13.5 FEDERAL INFORMATION SECURITY MANAGEMENT ACT 99
5.13.6 SARBANES-OXLEY ACT 100
5.13.7 GRAMM-LEACH-BLILEY ACT 100
5.13.8 PAYMENT CARD INDUSTRY DATA SECURITY STANDARD 100
5.13.9 FEDERAL INFORMATION PROCESSING STANDARDS 100
5.13.10 INTERNATIONAL ORGANIZATION FOR STANDARDIZATION 27001 101
5.13.11 REGULATORY BODIES, GOVERNMENT AGENCIES, AND OTHER ORGANIZATIONS 101
5.14 KEY CONFERENCES AND EVENTS IN 2025 104
5.15 BUSINESS MODEL ANALYSIS 104
5.16 INVESTMENT AND FUNDING SCENARIO 105
6 SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY COMPONENT 106
6.1 INTRODUCTION 107
6.1.1 COMPONENT: SECURITY AND VULNERABILITY
MANAGEMENT MARKET DRIVERS 107
6.2 SOFTWARE 108
6.2.1 VULNERABILITY SCANNERS 110
6.2.1.1 Modern vulnerability scanners automate system monitoring, reducing manual inspections 110
6.2.2 PATCH MANAGEMENT 111
6.2.2.1 Rise of remote and hybrid work makes security patch management increasingly vital 111
6.2.3 SECURITY INCIDENT AND EVENT MANAGEMENT 112
6.2.3.1 SIEM systems employ AI to determine activities that qualify as security events 112

6.2.4 RISK ASSESSMENT 113
6.2.4.1 Risk assessment proves essential for making informed decisions 113
6.2.5 THREAT INTELLIGENCE 114
6.2.5.1 Threat intelligence provides information about potential attackers 114
6.2.6 OTHER SOFTWARE 115
6.3 SERVICES 116
6.3.1 PROFESSIONAL SERVICES 118
6.3.1.1 Professional services offer expert team support and dedicated project consultancy for deployment 118
6.3.1.2 Consulting and deployment 120
6.3.1.3 Pen testing 121
6.3.1.4 Vulnerability assessment 122
6.3.1.5 Incident response 123
6.3.1.6 Support and maintenance 124
6.3.2 MANAGED SERVICES 125
6.3.2.1 Managed services ensure expert technical support for seamless integration and operation of security and vulnerability management 125
7 SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY TYPE 127
7.1 INTRODUCTION 128
7.1.1 TYPE: SECURITY AND VULNERABILITY MANAGEMENT MARKET DRIVERS 128
7.2 ENDPOINT SECURITY 129
7.2.1 INCREASING NEED TO IDENTIFY RISKS ON DEVICES TO PREVENT UNAUTHORIZED ACCESS 129
?
7.3 NETWORK SECURITY 130
7.3.1 VULNERABILITY MANAGEMENT IMPROVES NETWORK SECURITY BY REDUCING ATTACK SURFACE 130
7.4 APPLICATION SECURITY 131
7.4.1 APPLICATION SECURITY PROTECTS USER PRIVACY, UPHOLDS TRUST,
AND ASSURES BUSINESS CONTINUITY 131
7.5 CLOUD SECURITY 132
7.5.1 EFFICIENT VULNERABILITY MANAGEMENT VITAL TO PRESERVE INTEGRITY, AVAILABILITY, AND CONFIDENTIALITY OF CLOUD-BASED ASSETS 132
8 SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY TARGET 134
8.1 INTRODUCTION 135
8.1.1 TARGET: SECURITY AND VULNERABILITY MANAGEMENT MARKET DRIVERS 135
8.2 CONTENT MANAGEMENT VULNERABILITIES 136
8.2.1 RISE IN AMOUNT OF CONTENT GENERATED IN INTER- AND INTRA-ORGANIZATIONS DUE TO DIGITALIZATION 136
8.3 IOT VULNERABILITIES 137
8.3.1 VULNERABILITY MANAGEMENT HELPS MITIGATE RISKS BY CONTINUOUSLY SCANNING IOT NETWORKS 137
8.4 API VULNERABILITIES 138
8.4.1 INCREASING CYBERATTACKS ON APIS TO DRIVE ADOPTION OF SECURITY AND VULNERABILITY MANAGEMENT SOLUTIONS 138
8.5 OTHER TARGET VULNERABILITIES 139
9 SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY DEPLOYMENT MODE 141
9.1 INTRODUCTION 142
9.1.1 DEPLOYMENT MODE: SECURITY AND VULNERABILITY MANAGEMENT MARKET DRIVERS 142
9.2 ON-PREMISES 143
9.2.1 ON-PREMISE SOLUTIONS PROVIDE ORGANIZATIONS WITH FULL CONTROL OVER ALL PLATFORMS 143
9.3 CLOUD 144
9.3.1 CLOUD DEPLOYMENT BENEFICIAL FOR ORGANIZATIONS WITH LIMITED SECURITY BUDGETS 144

10 SECURITY AND VULNERABILITY MANAGEMENT MARKET,
BY ORGANIZATION SIZE 146
10.1 INTRODUCTION 147
10.1.1 ORGANIZATION SIZE: SECURITY AND VULNERABILITY MANAGEMENT MARKET DRIVERS 147
10.2 LARGE ENTERPRISES 148
10.2.1 COMPLEX IT INFRASTRUCTURE OF LARGE ENTERPRISES TO DRIVE DEMAND FOR VULNERABILITY MANAGEMENT SOLUTIONS 148
10.3 SMES 149
10.3.1 ADOPTING VULNERABILITY MANAGEMENT SOLUTIONS HELPS SMES MINIMIZE CYBER THREATS, EXPAND EXISTING CUSTOMER BASE, AND ENHANCE BUSINESS EFFICIENCY 149
11 SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY VERTICAL 151
11.1 INTRODUCTION 152
11.1.1 VERTICAL: SECURITY AND VULNERABILITY MANAGEMENT MARKET DRIVERS 152
11.2 BFSI 154
11.2.1 BFSI VERTICAL PRIORITIZES CUSTOMER PRIVACY AND SECURITY, ONLINE TRANSACTIONS, AND SENSITIVE INFORMATION 154
11.3 HEALTHCARE 155
11.3.1 HEALTHCARE SECTOR SECURES PERSONAL HEALTH INFORMATION AND CRITICAL DATA ABOUT PATIENTS 155
11.4 GOVERNMENT 156
11.4.1 VULNERABILITY MANAGEMENT HELPS GOVERNMENT AGENCIES COMPLY WITH STRICT CYBERSECURITY LAWS 156
11.5 MANUFACTURING 157
11.5.1 TECHNOLOGICAL ADVANCEMENTS IN MANUFACTURING VERTICAL TO DRIVE DEMAND FOR VULNERABILITY MANAGEMENT 157
11.6 ENERGY & UTILITIES 158
11.6.1 ENERGY COMPANIES FACE HIGHER RISKS OF CYBERATTACKS DISRUPTING POWER DISTRIBUTION, INCREASING SECURITY DEMAND 158
11.7 IT & ITES 159
11.7.1 IT ORGANIZATIONS HANDLE SIGNIFICANT SENSITIVE DATA AND CRITICAL OPERATIONS FOR GLOBAL CLIENTS, REQUIRING ADVANCED SECURITY SOLUTIONS 159
11.8 RETAIL & E-COMMERCE 160
11.8.1 INCREASING ATTACK SURFACE IN RETAIL SECTOR DUE TO WIDESPREAD USE OF INTERNET AND SMARTPHONES 160
11.9 TELECOMMUNICATIONS 161
11.9.1 VULNERABILITY SOLUTIONS LIKE THREAT INTELLIGENCE INTEGRATION OFFER TELECOM OPERATORS REAL-TIME INSIGHTS INTO EMERGING CYBER THREATS 161
11.10 TRAVEL & HOSPITALITY 162
11.10.1 SECURITY SOLUTIONS SAFEGUARD TRAVEL INDUSTRY NETWORKS, ENSURING CONTINUOUS AND SECURE CLIENT SERVICES 162
11.11 OTHER VERTICALS 163
12 SECURITY AND VULNERABILITY MANAGEMENT MARKET, BY REGION 165
12.1 INTRODUCTION 166
12.2 NORTH AMERICA 167
12.2.1 NORTH AMERICA: SECURITY AND VULNERABILITY MANAGEMENT MARKET DRIVERS 168
12.2.2 NORTH AMERICA: MACROECONOMIC OUTLOOK 168
12.2.3 US 176
12.2.3.1 Strong presence of security and vulnerability management vendors to drive market 176
12.2.4 CANADA 183
12.2.4.1 Increase in online fraud and malicious attacks to drive market 183
12.3 EUROPE 189

12.3.1 EUROPE: SECURITY AND VULNERABILITY MANAGEMENT MARKET DRIVERS 190
12.3.2 EUROPE: MACROECONOMIC OUTLOOK 191
12.3.3 UK 197
12.3.3.1 Increase in investments in cyber defenses to drive market 197
12.3.4 GERMANY 204
12.3.4.1 Advancement towards digitalization across all business areas to drive market 204
12.3.5 FRANCE 211
12.3.5.1 Increasing government initiatives and support to drive market 211
12.3.6 ITALY 217
12.3.6.1 Increasing cyberattacks due to rapid digitalization to drive market 217
12.3.7 SWEDEN 224
12.3.7.1 Increasing demand for security and vulnerability management solutions due to rising cyber terrorism threats to drive market 224
12.3.8 DENMARK 230
12.3.8.1 Deals and initiatives to enhance security and vulnerability management landscape to drive market 230
12.3.9 REST OF EUROPE 237
12.4 ASIA PACIFIC 243
12.4.1 ASIA PACIFIC: SECURITY AND VULNERABILITY MANAGEMENT MARKET DRIVERS 244
12.4.2 ASIA PACIFIC: MACROECONOMIC OUTLOOK 244
12.4.3 CHINA 252
12.4.3.1 Increasing investments in advanced tools for security and vulnerability management to drive market 252
12.4.4 JAPAN 259
12.4.4.1 Need for advanced security and vulnerability management solutions to minimize attack surfaces to drive market 259
12.4.5 INDIA 266
12.4.5.1 Increasing complexity of cyber threats to drive market 266
12.4.6 AUSTRALIA 272
12.4.6.1 Increasing awareness and demand for security and vulnerability management solutions and services to drive market 272
12.4.7 SOUTH KOREA 279
12.4.7.1 Rising adoption of internet-enabled products to drive market 279
12.4.8 REST OF ASIA PACIFIC 285
12.5 MIDDLE EAST AND AFRICA 292
12.5.1 MIDDLE EAST AND AFRICA: SECURITY AND VULNERABILITY MANAGEMENT MARKET DRIVERS 292
12.5.2 MIDDLE EAST AND AFRICA: MACROECONOMIC OUTLOOK 293
12.5.3 GCC COUNTRIES 300
12.5.3.1 Rise in government initiatives to reduce cybersecurity attacks to drive market 300
12.5.3.2 KSA 307
12.5.3.3 UAE 314
12.5.3.4 Rest of GCC Countries 320
12.5.4 SOUTH AFRICA 327
12.5.4.1 Increase in cyberattacks due to growing internet penetration to drive market 327
12.5.5 REST OF MIDDLE EAST AND AFRICA 333
12.6 LATIN AMERICA 340
12.6.1 LATIN AMERICA: SECURITY AND VULNERABILITY MANAGEMENT MARKET DRIVERS 340
12.6.2 LATIN AMERICA: MACROECONOMIC OUTLOOK 341
12.6.3 BRAZIL 347
12.6.3.1 Increase in hacking incidences due to rise in digital penetration to drive market 347
12.6.4 MEXICO 354

12.6.4.1 Increase in adoption of cloud-based services and broadband to drive market 354
12.6.5 REST OF LATIN AMERICA 360
13 COMPETITIVE LANDSCAPE 367
13.1 KEY PLAYER STRATEGIES/RIGHT TO WIN 367
13.2 BRAND/PRODUCT COMPARISON 369
13.2.1 MICROSOFT 370
13.2.2 AT&T 370
13.2.3 CROWDSTRIKE 370
13.2.4 IBM 370
13.2.5 TENABLE 370
13.3 COMPANY VALUATION AND FINANCIAL METRICS 371
13.3.1 COMPANY VALUATION 371
13.3.2 FINANCIAL METRICS 371
13.4 REVENUE ANALYSIS 372
13.5 MARKET SHARE ANALYSIS 373
13.6 COMPANY EVALUATION MATRIX: KEY PLAYERS, 2023 375
13.6.1 STARS 375
13.6.2 EMERGING LEADERS 375
13.6.3 PERVASIVE PLAYERS 376
13.6.4 PARTICIPANTS 376
13.6.5 COMPANY FOOTPRINT: KEY PLAYERS, 2023 377
13.6.5.1 Overall company footprint 377
13.6.5.2 Software footprint 378
13.6.5.3 Deployment mode footprint 378
13.6.5.4 Vertical footprint 379
13.6.5.5 Region footprint 380
13.7 COMPANY EVALUATION MATRIX: STARTUPS/SMES, 2023 381
13.7.1 PROGRESSIVE COMPANIES 381
13.7.2 RESPONSIVE COMPANIES 381
13.7.3 DYNAMIC COMPANIES 381
13.7.4 STARTING BLOCKS 381
13.7.5 COMPETITIVE BENCHMARKING: STARTUPS/SMES, 2023 383
13.7.5.1 Detailed list of key startups/SMEs 383
13.7.5.2 Competitive benchmarking of key startups/SMEs 384
13.8 COMPETITIVE SCENARIO 385
13.8.1 PRODUCT LAUNCHES AND ENHANCEMENTS 385
13.8.2 DEALS 388
14 COMPANY PROFILES 390
14.1 INTRODUCTION 390
14.2 MAJOR PLAYERS 390
14.2.1 TENABLE 390
14.2.1.1 Business overview 390
14.2.1.2 Products/Solutions/Services offered 391
14.2.1.3 Recent developments 392
14.2.1.3.1 Product launches and enhancements 392
14.2.1.3.2 Deals 392
14.2.1.4 MnM view 393

14.2.1.4.1 Key strengths 393
14.2.1.4.2 Strategic choices 393
14.2.1.4.3 Weaknesses and competitive threats 393
14.2.2 MICROSOFT 394
14.2.2.1 Business overview 394
14.2.2.2 Products/Solutions/Services offered 395
14.2.2.3 Recent developments 396
14.2.2.3.1 Product launches and enhancements 396
14.2.2.4 MnM view 396
14.2.2.4.1 Key strengths 396
14.2.2.4.2 Strategic choices 396
14.2.2.4.3 Weaknesses and competitive threats 396
14.2.3 AT&T 397
14.2.3.1 Business overview 397
14.2.3.2 Products/Solutions/Services offered 398
14.2.3.3 Recent developments 399
14.2.3.3.1 Product launches and enhancements 399
14.2.3.3.2 Deals 399
14.2.3.4 MnM View 399
14.2.3.4.1 Key strengths 399
14.2.3.4.2 Strategic choices 400
14.2.3.4.3 Weaknesses and competitive threats 400
14.2.4 CROWDSTRIKE 401
14.2.4.1 Business overview 401
14.2.4.2 Products/Solutions/Services offered 402
14.2.4.3 Recent developments 403
14.2.4.3.1 Product launches and enhancements 403
14.2.4.3.2 Deals 403
14.2.4.4 MnM view 403
14.2.4.4.1 Key strengths 403
14.2.4.4.2 Strategic choices 403
14.2.4.4.3 Weaknesses and competitive threats 404
14.2.5 IBM 405
14.2.5.1 Business overview 405
14.2.5.2 Products/Solutions/Services offered 406
14.2.5.3 Recent developments 407
14.2.5.3.1 Product launches and enhancements 407
14.2.5.3.2 Deals 408
14.2.5.4 MnM view 408
14.2.5.4.1 Key strengths 408
14.2.5.4.2 Strategic choices 408
14.2.5.4.3 Weaknesses and competitive threats 408
14.2.6 CISCO 409
14.2.6.1 Business overview 409
14.2.6.2 Products/Solutions/Services offered 410
14.2.6.3 Recent developments 411
14.2.6.3.1 Deals 411

14.2.7 RAPID7 412
14.2.7.1 Business overview 412
14.2.7.2 Products/Solutions/Services offered 413
14.2.7.3 Recent developments 414
14.2.7.3.1 Product launches and enhancements 414
14.2.7.3.2 Deals 414
14.2.8 CHECK POINT SOFTWARE TECHNOLOGIES 415
14.2.8.1 Business overview 415
14.2.8.2 Products/Solutions/Services offered 416
14.2.8.3 Recent developments 417
14.2.8.3.1 Product launches and enhancements 417
14.2.9 QUALYS 418
14.2.9.1 Business overview 418
14.2.9.2 Products/Solutions/Services offered 419
14.2.9.3 Recent developments 420
14.2.9.3.1 Product launches and enhancements 420
14.2.9.3.2 Deals 421
14.2.10 MANAGEENGINE 422
14.2.10.1 Business overview 422
14.2.10.2 Products/Solutions/Services offered 423
14.2.11 DXC TECHNOLOGY 424
14.2.11.1 Business overview 424
14.2.11.2 Products/Solutions/Services offered 425
14.2.12 RSI SECURITY 426
14.2.13 FORTRA 427
14.2.14 IVANTI 428
14.2.15 TANIUM 429
14.3 OTHER PLAYERS 430
14.3.1 OUTPOST24 430
14.3.2 SKYBOX SECURITY 431
14.3.3 SECPOD 432
14.3.4 BRINQA 433
14.3.5 HOLM SECURITY 434
14.3.6 NOPSEC 435
14.3.7 BALBIX 436
14.3.8 INTRUDER 437
14.3.9 INVICTI 438
14.3.10 VULCAN CYBER 439
14.3.11 NUCLEUS SECURITY 440
15 ADJACENT MARKETS 441
15.1 INTRODUCTION TO ADJACENT MARKETS 441
15.2 LIMITATIONS 441
15.3 CYBERSECURITY MARKET 442
15.3.1 CYBERSECURITY MARKET ? GLOBAL FORECAST TO 2028 442
15.4 SECURITY INFORMATION AND EVENT MANAGEMENT MARKET 448
16 APPENDIX 452
16.1 DISCUSSION GUIDE 452

16.2 KNOWLEDGESTORE: MARKETSANDMARKETS' SUBSCRIPTION PORTAL 456
16.3 CUSTOMIZATION OPTIONS 458
16.4 RELATED REPORTS 458
16.5 AUTHOR DETAILS 459

Security and Vulnerability Management Market by Software (Vulnerability Scanner, Patch Management, SIEM, Risk assessment, Threat Intelligence), Type (Network Security, Application Security, Endpoint Security, and Cloud Security) - Global Forecast to 2030

Market Report | 2024-10-14 | 460 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*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	

Zip Code*		Country*	
		Date	2025-05-19
		Signature	