Analysis of the EMEA Managed Security Services Market
Threat Intelligence and Threat Remediation Will Drive Revenue Growth

MA60-74
July 2014
Research Team

Lead Analyst

Mario Fernandez
Senior Industry Analyst
Information and Communication Technologies
(+48) 22 481 6271
mario.fernandez@frost.com

Frank Dickson
Industry Principal
Information and Network Security
(+1) 469 387 0256
frank.dickson@frost.com

Contributing Analyst

Research Director

Adrian Drozd
Research Director
Information and Communication Technologies
(+44) 1865 398 699
adrian.drozd@frost.com

Strategic Review Committee Leader

Michael Suby
Stratecast Vice President of Research
Information and Network Security
(+1) 720 344 4860
michael.suby@frost.com
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Slide Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Summary</td>
<td>4</td>
</tr>
<tr>
<td>Market Overview</td>
<td>9</td>
</tr>
<tr>
<td>Total MSS Market</td>
<td></td>
</tr>
<tr>
<td>• Drivers and Restraints</td>
<td>21</td>
</tr>
<tr>
<td>• Forecast and Trends</td>
<td>28</td>
</tr>
<tr>
<td>• Market Share and Competitive Analysis</td>
<td>49</td>
</tr>
<tr>
<td>Security Asset Monitoring and Management Segment Analysis</td>
<td>54</td>
</tr>
<tr>
<td>The Last Word</td>
<td>59</td>
</tr>
<tr>
<td>Appendix</td>
<td>63</td>
</tr>
</tbody>
</table>
Executive Summary
Key Findings

• The managed security services (MSS) market in Europe, the Middle East, and Africa (EMEA) is forecast to grow from $2.81 billion in 2013 to $4.99 billion in 2018.

• Threat intelligence, research, detection, and remediation, and advanced MSS will be major growth drivers. Organizations increasingly demand managed security service providers (MSSPs) to go beyond notifying the organization of security alerts to take an active role in threat remediation.

• Standard MSS, including security asset monitoring and management, and risk and compliance management, represent approximately 80% of the total market but are expected to expand at high, single-digit growth rates.

• Regulatory compliance, in particular data protection and data privacy compliance, continues to be both a driver and a restraint. While the complexity of maintaining regulatory compliance compels organizations to adopt MSS, misperceptions on regulations—particularly on data protection and data privacy—often deter organizations to engage in MSS.

• From a regional standpoint, the United Kingdom and Germany represent the largest MSS markets in EMEA.

• From a vertical perspective, financial services and government command the MSS market in terms of size.

Source: Frost & Sullivan
# Market Engineering Measurements


### Market Overview

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Growth</td>
<td>$2.81 B</td>
<td>$280,000</td>
<td>$4.99 B</td>
</tr>
</tbody>
</table>

### Market Growth Rate

- **Base Year Market Growth Rate**: 13.8% (CAGR, 2013–2018)
- **Compound Annual Growth Rate**: 12.2%

### Price Sensitivity

- **Customer Price Sensitivity**: 6 (scale: 1 [Low] to 10 [High])

### Degree of Technical Change

- **Degree of Technical Change**: 7 (scale: 1 [Low] to 10 [High])

---

For a tabular version [click here](#).

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Market Engineering Measurements (continued)

**Market Overview**
- **Market Concentration**
  - 22.4%
  - (% of market share held by top 3 companies)

**Competitor Overview**
- **Number of Competitors***
  - 50+
  - (active market competitors in 2013)

**Total Addressable Market**
- **Replacement Rate**
  - 3.3 Years
  - (average contract period for MSSP)

**Industry Advancement**
- **Average Renewal Rate**
  - 93.9%
  - (Average renewal rate per customer)

- **Average Product Development Time**
  - 9 Months

*Companies with revenue of more than $1 M revenue.

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
# CEO’s Perspective

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Threat intelligence and research consolidate as core elements of MSSPs’ offerings.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>MSSPs continue to shift from simply providing security alert notifications to proactively remediating security incidents.</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>The EMEA MSS market will progressively consolidate. MSSPs aim to fortify their portfolios or enlarge their customer base.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Misperceptions of or uncertainties around regulations may limit the growth of MSSPs in Europe.</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Standard, customer-premises equipment management constitutes the largest MSS segment.</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan
Market Overview
Market Definitions

Market Description

• MSSPs monitor events (log stream data) of security appliances (security products) from a security operations center (SOC). In many instances, MSSPs also manage the security appliances throughout the appliances’ lifecycle.

• Traditionally, MSSPs have helped customers reduce their capital expenditure (CAPEX) while providing in-depth expertise on security and maintaining efficient security asset management.

• MSSPs are expected to have expertise in a wide number of product vendors because initially they are hired to monitor and manage customer’s existing equipment.

  o As highlighted in Frost & Sullivan’s 2013 Analysis of the EMEA MSS Market, MSSPs’ portfolios are undergoing a transformation, whereby security intelligence, threat analysis, and proactive incident response become core elements of MSS offerings.

  o In the 2014 Analysis of the EMEA MSS Market, Frost & Sullivan sees a consolidation and continuation of this transformation. Hence, Frost and Sullivan has changed the segmentation of the MSS market to reflect this transformation.

  o Frost & Sullivan splits MSS into 4 segments: 1) security asset monitoring and management; 2) threat intelligence, research, detection, and remediation; 3) risk and compliance management; and 4) advanced and emerging managed security services.

Source: Frost & Sullivan
Market Definitions (continued)

Segment Definitions

- Security asset monitoring and management refers to traditional MSS.

- More specifically, it refers to event collection, event correlation, event analysis, and security alert notification; security asset maintenance and upgrades; and security assets policy management.

- Security asset monitoring and management has 2 sub-segments, which are customer-premises equipment (CPE)-based and hosted service delivery modes.
  - CPE-based delivery modes refer to managing, monitoring, and maintaining security equipment, which is owned by the client and housed in the client’s premises (CPE) from a SOC or by dedicated onsite personnel.
  - Hosted service delivery modes refer to shared-customer (i.e., multi-tenant security equipment) or dedicated-customer security services, which is delivered based on single-customer equipment housed in the service provider’s premises (service provider premises equipment) or at a third-party location. Regardless of equipment location, the services rendered are fully managed through the service provider’s SOC.

Source: Frost & Sullivan
Market Definitions (continued)

Segment Definitions

• Threat intelligence, research, detection, and remediation consists of the following:
  
  o Threat intelligence and research refers to the generation of intelligence through the investigation of security events, malware, exploits, vulnerabilities, and attack behaviors (techniques and patterns) across technologies, industries, and geographies.
  
  o Threat detection and remediation refers to event correlation coupled with threat intelligence to identify a targeted attack or advanced threat.

• Risk and compliance management involves vulnerability assessments and scanning (performed regularly as a part of a MSS program), compliance audits and reporting support (including ISO 27001, Payment Card Data Industry Security Standard (PCI DSS), and others), and partner program management.

• Advanced and emerging managed security services include managed identity and access management (IAM), managed mobile endpoint security, managed data loss prevention (DLP), among with other next-generation managed security services.

Source: Frost & Sullivan
Segment Definitions

• Professional security services (PSS) are excluded from the scope of this study.
  o PSS providers deliver value-added professional services, such as assessment, benchmarking, design, planning, and configuration services.
  o In addition, PSS providers may offer customized or off-the-shelf maintenance and service contracts for customer-premises equipment PSS providers to install.
  o PSS are typically delivered as relatively short-term projects, with targeted end dates.

• Frost & Sullivan segments the professional security services into security advisory, technical services, and implementation services.
  o Frost & Sullivan will address the PSS market in the second half of 2014.

Source: Frost & Sullivan
Market Definitions (continued)

Region Definitions

• Europe, the Middle East, and Africa (EMEA) includes countries in Western and Eastern Europe, Western Asia, and Africa.

• The following regions are included within the study:
  o ACH refers to Austria and Switzerland.
  o Benelux refers to Belgium, the Netherlands, and Luxembourg.
  o Nordics refers to Denmark, Sweden, Norway, and Finland.
  o Central and Eastern Europe (CEE) refers to the Baltic countries, Bulgaria, the Czech Republic, Hungary, Poland, Romania, and Slovakia.
  o Middle East and Africa (MEA) refers to countries in North and Sub-Saharan Africa, as well as countries in Western Asia.
  o Southern Europe refers to Italy, Spain, and Portugal.

Source: Frost & Sullivan
Market Definitions (continued)

Revenue Definitions

• Projected revenue is segmented according to service portfolio distribution, vertical market distribution, and region/country.

• Frost & Sullivan’s MSS market revenue models include the installation costs incurred in the procurement of services.

• Enterprise refers to an organization with 1,000 or more users, while SMB refers to small and medium businesses with fewer than 1,000 users. Within the SMB segment, small business refers to organizations with less than 100 users, and medium business refers to organizations having between 100 and 999 users.

• Frost & Sullivan provides analyses of the MSS market in the following areas: growth, demand, pricing, channel distribution, legislation, and technology trends. These include regional and vertical market forecasts as well as an in-depth look at the competition within the MSS market.

• The base year for this study is 2013, and revenue forecasts and trends are provided through 2018. Historical data is quantified to reveal trends since 2011.

Source: Frost & Sullivan
Key Questions This Study Will Answer

- What is the total addressable MSS market by region/country in EMEA?
- How fast will the individual market segments grow over the next 5 years?
- Which services are experiencing the greatest demand? How will the demand for services change over the forecast period?
- What are the most prominent verticals for MSSPs?
- What trends are and will continue to shape the future of MSSPs and MSS offerings?
- Who are the leading competitors in the EMEA MSS market?

Source: Frost & Sullivan
Total MSS Market: Market Segmentation, EMEA, 2013

Managed Security Services

- Security asset monitoring and management
- Threat intelligence, research, detection, and remediation
- Risk and compliance management
- Advanced and emerging MSS

*Professional and technical services are excluded from the scope of this study.

Source: Frost & Sullivan
AEM: Advanced and emerging managed security services
TIRDR: Threat intelligence, research, detection, and remediation
RCM: Risk and compliance management
SAMM: Security asset monitoring and management

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Market Overview—Service Technology Roadmap

Total MSS Market: Service Technology Roadmap, EMEA, 2011–2018

- Expansion of hosted MSS offerings
- Advanced security analytics
- Expansion and enhancement of managed IAM services
- Expansion and enhancement of managed DLP services
- Consolidation of threat research and intelligence as core offering
- Expansion of MSS support to virtual and cloud environments
- Enhancements to MSS activity reporting portals

2011  2012  2013  2014  2018

Source: Frost & Sullivan
Key Takeaway: Understanding a client’s specific risk environment, building a strong relationship with the client, and controlling the quality of MSS represent the main factors to rely on direct sales.

Total MSS Market: Distribution Channel Analysis, EMEA, 2013

*Key: VARs — Value-added Resellers; SI — System Integrators; ISPs — Internet Service Providers

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Drivers and Restraints—Total MSS Market
# Drivers and Restraints

## Total MSS Market: Key Market Drivers and Restraints, EMEA, 2014–2018

<table>
<thead>
<tr>
<th>Market Drivers</th>
<th>1–2 Years</th>
<th>3–4 Years</th>
<th>5th Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increasing sophistication of threats and targeted attacks</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
<tr>
<td>Shortage of in-house security experts and human talent</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Necessity to cost-effectively monitor and manage a myriad of IT assets and solutions</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Evolving industry and regulatory compliance frameworks</td>
<td>M</td>
<td>M</td>
<td>M</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Market Restraints</th>
<th>1–2 Years</th>
<th>3–4 Years</th>
<th>5th Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of awareness of the threat landscape and its impact</td>
<td>H</td>
<td>H</td>
<td>M</td>
</tr>
<tr>
<td>Inability to build a business case around MSS</td>
<td>M</td>
<td>H</td>
<td>L</td>
</tr>
<tr>
<td>Uncertainty about the legal implications of adopting MSS</td>
<td>M</td>
<td>M</td>
<td>L</td>
</tr>
<tr>
<td>Unwillingness to cede control over security monitoring and management</td>
<td>M</td>
<td>L</td>
<td>L</td>
</tr>
</tbody>
</table>

**Impact:**

- **H** High
- **M** Medium
- **L** Low

Note: Drivers and Restraints are in order of impact. Source: Frost & Sullivan
Drivers Explained

Increasing Sophistication of Threats and Targeted Attacks

- Well-funded, technologically-sophisticated, and highly-skilled intruders continue to develop tools, techniques, and malware to carry out targeted attacks.

- Organizations often lack a full view on the threat landscape and knowledge of security intelligence to detect and prevent stealthy attacks in a timely manner.

- Some organizations tend to respond to threats by investing in more security appliances and security software. However, these organizations soon realize that they cannot cope with sophisticated threats and targeted attacks with more security appliances and software.

- Instead, deploying more security appliances and software can result in a more complex IT infrastructure, which would be more challenging to protect.

- Hence, to effectively protect their IT infrastructure, organizations seek to establish partnerships with MSSPs.

- By having a large, cross-industry, cross-region customer base, MSSPs have developed strong security intelligence capabilities and have a wider view on the threat landscape. These two elements, security intelligence and threat research, have become core elements of MSSPs’ value proposition.

- Moreover, MSSPs have developed the expertise, technology, and procedures to defend complex IT infrastructures from targeted attacks.

Source: Frost & Sullivan
Shortage of In-house Security Experts and Human Talent

- Protecting IT infrastructure from sophisticated threats and targeted attacks requires people, processes, and technology working in a concerted manner.

- Regardless of the amount of resources allocated to acquire advanced IT security technology and to design effective security policies and procedures, without human expertise, organizations’ security posture will be weak.

- In particular, security experts play a fundamental role in identifying actual attacks from false positives.
  - Prioritizing alerts is a key value-add for MSSPs.

- Organizations often lack the resources or willingness to hire, train, and retain these security experts, who likely do not contribute considerably to the organizations’ core business.

- Conversely, MSSPs consider human security expertise crucial for their operations. MSSPs invest time and money to hire, retain, and train security experts.

- MSSPs tend to use certifications and number of years of experience as variables to describe the scope and depth of security professionals’ capabilities.

Source: Frost & Sullivan
Drivers Explained (continued)

Necessity to Cost-effectively Monitor and Manage a Myriad of IT Assets and Solutions

• Despite the awareness of security among organizations’ board members, budgets for IT security are not growing enough to counter the growth and sophistication of threats and the complexity of the IT environment. IT security staff have to protect an evolving IT security infrastructure where the only constant is a greater presence of virtual and cloud environments and mobile endpoints.

• The continuous evolution of the IT infrastructure demands more time, experts, and technology from internal IT staff. To cost-effectively defend their IT infrastructure, organizations form partnerships with MSSPs, who have the know-how, experts, and technology to provide security services at price points that internal IT staff cannot.

Evolving Industry and Regulatory Compliance Frameworks

• Industry and regulatory compliance remain key drivers of adoption for MSS.

• Some organizations still require legislation or compulsory accreditation to approach security seriously. The complexity of complying with a regulation or standard compels these organizations to adopt an MSS partnership; these organizations, however, tend to adopt basic MSS offerings.

• Other organizations proactively protect their infrastructure, intellectual property, and customers’ data by adopting sophisticated MSS. Although these second types of organizations adopt sophisticated MSS offerings, they also demand risk and compliance management services from MSSPs, who are best placed to assist organizations with their compliance requirements.

Source: Frost & Sullivan
Lack of Awareness of the Threat Landscape and its Impact

- Although the media has extensively covered security breaches, many organizations still believe they are not, or will be not, be subject to a targeted attack.
- Hence, some organizations believe that they do not require protection against advanced threats.
- This approach towards security has curtailed the adoption of MSS.

Inability to Build a Business Case Around MSS

- Organizations see budgets for IT security largely as cost with little to no effect to the organizations’ revenue-generating activities.
- The IT staff from some organizations find it hard to justify the investments in partnering with a MSSP. The inability to show the return on investment has limited the adoption of MSS.
- Unfortunately, the return on investment is clear only once an organization is the subject of a targeted attack and the organization is aware of the situation, or in other words, the organization knows that intruders have penetrated their systems and accomplished their goals.

Source: Frost & Sullivan
Restraints Explained (continued)

Uncertainty About the Legal Implications of Adopting MSS

- Evolving regulatory and compliance frameworks also have the unintended effect of causing confusion among organizations.

- Strict data privacy laws in the European Union often lead organizations to hesitate whether they can outsource part of their security operations to MSSPs or not.

- In light of the news on the US National Security Agency’s (NSA) PRISM program and the US Patriot Act, the uncertainties and misperceptions around compliance with data privacy laws have grown.

- As a result, the adoption of MSS has been negatively affected, especially among US-headquartered MSSPs operating in European countries.

Unwillingness to Cede Control over Security Monitoring and Management

- IT security staff from certain organizations fear that by ceding control over security monitoring and management, the importance or headcount of their departments will be reduced.

- Moreover, internal IT staff from some organizations fear that an engagement with an MSSP for security monitoring and management will be the first of many deals that will decrease the footprint of their internal IT teams.

Source: Frost & Sullivan
Forecast and Trends—Total MSS Market
Forecast Assumptions

• Frost & Sullivan’s revenue forecast is primarily based on the analysis of aggregated information obtained during in-depth interviews with leading and second-tier MSSPs.

• IT service providers (ITSPs), communication service providers (CSPs), and security specialists shared their opinions on the total addressable market, the size of MSS segments, the maturity of countries or regions in terms of MSS adoption, and the demand of MSS by segment.

• Extensive analyses of annual reports, financial result releases, and Frost & Sullivan’s databases have complemented the results of the primary research.

• The forecast model includes MSS revenue from direct and indirect sales. Likewise, the forecast model includes revenue from security asset monitoring and management; threat intelligence, research, detection, and remediation; risk and compliance management; and advanced and emerging managed security services.

• Professional security services are excluded from this study.

• The forecast model also intends to estimate the corresponding value of managed security services when delivered as a part of larger managed services deals or larger IT/network security deals.

Source: Frost & Sullivan
Forecast Assumptions (continued)

- The MSS market revenue and growth rates are based on multiple assumptions including the following:
  - The current and expected maturity of countries in terms of the adoption of IT security services
  - The positive and negative effects of legislation on businesses’ willingness to outsource security services
  - The current and expected expansion of virtualized IT environments and cloud-based services among businesses
  - The current and expected penetration of security appliances among businesses
  - The commoditization of traditional MSS, such as monitored and managed firewalls

Source: Frost & Sullivan
Key Takeaway: The increasing sophistication of threats and targeted attacks coupled with a lack of in-house expertise will drive growth for the EMEA MSS market.

Total MSS Market: Revenue Forecast, EMEA, 2011–2018
CAGR 2013–2018 = 12.2%

<table>
<thead>
<tr>
<th>Year</th>
<th>Total MSS Market Revenue ($ Million)</th>
<th>Revenue Growth Rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>2,170.7</td>
<td>13.4</td>
</tr>
<tr>
<td>2012</td>
<td>2,471.3</td>
<td>13.8</td>
</tr>
<tr>
<td>2013</td>
<td>2,811.2</td>
<td>13.8</td>
</tr>
<tr>
<td>2014</td>
<td>3,195.5</td>
<td>13.7</td>
</tr>
<tr>
<td>2015</td>
<td>3,627.2</td>
<td>13.5</td>
</tr>
<tr>
<td>2016</td>
<td>4,079.8</td>
<td>12.5</td>
</tr>
<tr>
<td>2017</td>
<td>4,547.2</td>
<td>11.5</td>
</tr>
<tr>
<td>2018</td>
<td>4,992.1</td>
<td>9.8</td>
</tr>
</tbody>
</table>

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Revenue Forecast Discussion

- Frost & Sullivan estimated that the value of the MSS market was $2.81 billion in EMEA in 2013. The market is expected to grow at compound annual growth rate (CAGR) of 12.2% from 2013 to 2018.

- The majority of interviewed MSSPs provided more details on the operations and financial results associated to MSS than last year. The granularity of information enabled Frost & Sullivan to fine-tune its market-sizing model and forecast to reflect an even more accurate picture of the market.

- In general, all MSSPs agreed on the drivers and restraints discussed in the previous section of this document.

- The increasing awareness of security driven by extensive media coverage on cyber espionage and security breaches has not necessarily translated into larger budgets for IT security.

- Considering the proliferation of employee-owned and corporate-owned mobile devices, the increasing virtualization of IT infrastructure, and the adoption of cloud services, IT security staff feel compelled to establish a collaboration with MSSPs to cost-effectively deal with security.

- Indeed, these areas—mobile devices, cloud, and virtualization—have been the major growth drivers of MSS adoption and will continue to drive the deployment of high-end MSS.

- When compared to the results of the 2013 MSS in EMEA study, the estimated value of the MSS market in 2013 is slightly lower.

- The underlying reason for this is the availability of more granular data, which enabled the exclusion of professional security services in revenue figures that included both MSS and professional security services. These changes have been reflected in the base year and historical year as well.

- In terms of growth, the changes in the inputs of the market sizing model did not have a statistically significant difference.

Source: Frost & Sullivan
Key Takeaway: Service-level agreements (SLAs), the complexity of the client’s IT infrastructure, and degree of involvement are the major determinants of annual contract values.

Total MSS Market: Pricing Factors, EMEA, 2013

- Service-level Agreements (SLAs)
- Complexity of IT infrastructure
- Degree of involvement
- Integration of other managed services
- Geographic coverage
- Delivery mode
- Contract length

Annual contract sizes range between tens of thousands dollars to single-digit, million-dollar figures.

Source: Frost & Sullivan
Pricing Factors Discussion

- SLAs, which are broadly defined by parameters such as average response time to security events and average response time to service failures, vary according to different service packages—for example, standard or premium—offered by MSSPs. Higher guaranteed service parameters are, naturally, reflected in higher contract values.

- Customers' geographical footprint—be it global, regional, or local—and the corresponding requirements regarding regulatory compliance and the possibility of off-shoring, also have an effect on the annual contract size.

- Several MSSPs reported that organizations which require particular procedures to collect, store, and manage log data—for example to comply with a local regulation—are often given higher contract values.

- Other factors such as the length of the subscription service and the integration with other services—managed, professional/technical security, or system integration—affect the annual contract size.

- The longer the time span of the contract, the lower the annual contract value. Frost & Sullivan’s research indicates that, on average, MSSPs and their client organizations prefer 3-year contracts; however, the length of the contract can vary within 1 to 10 years.

- Once-off set-up fees, either per site or per device, can also be part of the annual contract.

- The integration with other services and greater volume of monitored/managed devices often results in price discounts.

Source: Frost & Sullivan
Pricing Factors Discussion (continued)

- Price discounts are applied depending on the core business of the MSSP.
- If the MSSP is a security specialist, pricing discounts often apply to professional and technical security services to attract new customers. In contrast, if the MSSP is an ITSP or CSP, pricing discounts often apply to the MSS offer itself, as MSS is only a part of a larger managed services/system integration deal.
- Frost & Sullivan estimates that the average annual value of an MSS contract in EMEA is $280,000.
- Frost & Sullivan uses the total annual revenue and number of customers as some of the variables to analyze annual contract size.
- By analyzing MSSPs’ annual revenue per customer, the annual value of the majority of contracts should be within the $120,000 and $450,000 range. However, it is important to mention that some annual value contracts fall outside this range; for example, the value of an annual contract for a small business may be lower than $10,000, while the value of an annual contract for multinational corporation may be above $1,000,000.
- Likewise, by analyzing MSSPs’ annual revenue per customer, Frost & Sullivan research indicates that ITSPs and security specialists’ annual value contracts are 20% to 30% higher than CSPs’ annual value contracts. Frost & Sullivan’s believe that the differences in clients’ organization size, vertical market, and degree of expertise in IT security explain this difference.
Key Takeaway: Advanced and emerging managed security services are expected to grow exponentially over the forecast period and become a key focus area for MSSPs.

Total MSS Market: Percent Revenue by Segment, EMEA, 2013

- **SAMM**: 58.9%
- **TIRDR**: 17.5%
- **RCM**: 19.6%
- **AEM**: 4.0%

Total MSS Market: Percent Revenue Forecast by Segment, EMEA, 2018

- **SAMM**: 50.2%
- **TIRDR**: 22.3%
- **RCM**: 17.2%
- **AEM**: 10.3%

AEM: Advanced and emerging managed security services
TIRDR: Threat intelligence, research, detection, and remediation
RCM: Risk and compliance management
SAMM: Security asset monitoring and management

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Key Takeaway: Security asset monitoring and management represents the largest segment; however, threat intelligence, research, detection, and remediation is a crucial growth area for MSSPs.

Total MSS Market: Revenue Forecast by Segment, EMEA, 2011–2018

AEM: Advanced and emerging managed security services
TIRDR: Threat intelligence, research, detection, and remediation
RCM: Risk and compliance management
SAMM: Security asset monitoring and management

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Revenue Forecast by Segment Discussion

- Overall, standard MSS—namely security asset monitoring and management, and risk and compliance management—are expected to grow at moderate, yet healthy rates over the forecast period. Precisely, these segments will expand at CAGRs of 8.7% and 9.3%, respectively, from 2013 to 2018.

- Conversely, high-end MSS—namely threat intelligence, research, detection, and remediation; and advanced and emerging managed security services—are forecasted to develop at high, double-digit growth rates.

- Threat intelligence, research, detection, and remediation is expected to expand at a CAGR of 17.7% from 2013 to 2018. Threat intelligence and research underpin targeted attacks’ detection; as such, threat intelligence and research are, and will continue to be, of paramount importance to MSSPs.

- It is important to note that threat intelligence and research may not necessarily be services that MSSPs monetize. MSSPs often factor in threat intelligence and research when determining the value of a contract for a client organization that requires assistance in protection from targeted attacks.

- However, some MSSPs offer threat intelligence and research as a standalone service to some client organizations.

- In particular, leading MSSPs with strong security intelligence arms offer threat research as a standalone service—generally as a subscription service—to organizations who own their SOCs and have a sufficient pool of in-house security experts. These organizations typically are large financial institutions or government agencies.

Source: Frost & Sullivan
Revenue Forecast by Segment Discussion (continued)

• Furthermore, proactive and continuous threat remediation and incident responses are becoming increasingly important items in MSSPs’ contracts with client organizations.

• Organizations increasingly require MSSPs to go beyond alert notifications. MSSPs and internal IT security staff increasingly work in tandem to respond to a security incident.

• Operationally, the shift from alert notification to proactive remediation has implications. Leading MSSPs have reorganized their internal staff so that MSS and professional security services teams work in a more integrated manner.

• Despite the increasing integration of MSS and professional security services, MSSPs still recognize revenue from MSS and professional security services as 2 separate lines of services.

• Frost & Sullivan expects rapid growth in the advanced and emerging managed security services segment which will expand at an impressive CAGR of 35.3% from 2013 to 2018.

• Monitored managed mobile endpoints, identity access management, and advanced threat protection against data leaks will be key growth drivers in the AEM segment.

• Leading MSSPs have developed targeted attack protection services specifically designed to prevent data leaks in their service roadmaps. In MSSPs’ view, the development of MSS offerings exclusively focused on preventing data leaks is the next step of MSSPs’ shift from technology-oriented to risk- and business-oriented security services because organizations are increasingly data-centric.

Source: Frost & Sullivan
Revenue Forecast by Region

Key Takeaway: The Nordics and MEA constitute the fastest-growing regions for MSSPs in EMEA. The United Kingdom and Germany remain the largest regional markets.

Total MSS Market: Revenue Forecast by Region, EMEA, 2011–2018

<table>
<thead>
<tr>
<th>Year</th>
<th>Rest of EMEA</th>
<th>MEA</th>
<th>Nordics</th>
<th>Benelux</th>
<th>France</th>
<th>Germany</th>
<th>UK</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011</td>
<td>614.2</td>
<td>189.0</td>
<td>173.7</td>
<td>175.5</td>
<td>280.0</td>
<td>358.1</td>
<td>380.3</td>
</tr>
<tr>
<td>2012</td>
<td>699.3</td>
<td>215.1</td>
<td>197.7</td>
<td>199.8</td>
<td>318.8</td>
<td>407.7</td>
<td>432.9</td>
</tr>
<tr>
<td>2013</td>
<td>795.4</td>
<td>244.7</td>
<td>224.9</td>
<td>227.2</td>
<td>362.6</td>
<td>463.8</td>
<td>492.5</td>
</tr>
<tr>
<td>2014</td>
<td>904.2</td>
<td>278.2</td>
<td>255.7</td>
<td>258.3</td>
<td>412.2</td>
<td>527.2</td>
<td>559.8</td>
</tr>
<tr>
<td>2015</td>
<td>1,026.3</td>
<td>315.8</td>
<td>290.2</td>
<td>293.2</td>
<td>467.9</td>
<td>598.4</td>
<td>635.4</td>
</tr>
<tr>
<td>2016</td>
<td>1,154.4</td>
<td>355.2</td>
<td>326.4</td>
<td>329.8</td>
<td>526.2</td>
<td>673.1</td>
<td>714.7</td>
</tr>
<tr>
<td>2017</td>
<td>1,286.6</td>
<td>395.8</td>
<td>363.8</td>
<td>367.6</td>
<td>586.5</td>
<td>750.2</td>
<td>796.6</td>
</tr>
<tr>
<td>2018</td>
<td>1,392.8</td>
<td>469.3</td>
<td>434.3</td>
<td>394.4</td>
<td>599.1</td>
<td>853.6</td>
<td>848.7</td>
</tr>
</tbody>
</table>

Rest of EMEA include Southern Europe, ACH, CEE, and Rest of Europe. Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan.
Regional Revenue Forecast Discussion

- The United Kingdom MSS market was valued at $492.5 million in 2013 and is expected to grow at a CAGR of 11.5% from 2013 to 2018.

- Despite the UK MSS market seeing double-digit growth rates in 2013, towards the end of the forecast period, the UK market will start growing at single-digit growth rates. UK MSS market maturity explains the slow down of growth in 2018.

- Germany, the second-largest MSS market in EMEA, had an estimated value of $463.8 million in 2013. The German MSS market is anticipated to grow at a CAGR of 13.0% from 2013 to 2018; therefore by 2018, the German MSS market should become the largest MSS market in EMEA.

- The higher penetration of MSS among large enterprises and medium-sized business will drive growth in Germany.

- France ranks third in the EMEA region in terms of size; the French MSS market reached $362.6 million in 2013.

- The French MSS market is expected to grow at a CAGR of 10.6%, which is a comparatively low CAGR. Strong national sentiment and strict data privacy laws explain the lower growth rates in France.

- The Benelux MSS market size was calculated at $227.2 million and region’s market will grow at CAGR of 11.7% from 2013 to 2018.

Source: Frost & Sullivan
Regional Revenue Forecast Discussion (continued)

- The MEA and Nordics constitute the fastest-growing regions for MSSPs in EMEA. The Nordic and MEA regions are expected to grow at CAGRs of 14.1% and 13.9%, respectively, between 2013 and 2018.

- Within the others category, it is worth mentioning the size of the MSS market in Spain and Portugal ($212.9 million), Italy ($211.6 million), and ACH ($187.4 million) in 2013.

- The CEE MSS market closes the top three-fastest growing regions with a CAGR of 14.0% from 2013 to 2018. The value of the MSS market in CEE was $134.9 million in 2013.

- While the greater adoption of high-end MSS—threat intelligence, research, detection, and remediation; and advanced and emerging managed security services—explains the rapid growth in the Nordics and the Middle East, the higher penetration of standard MSS—specifically security asset monitoring and management—explains the growth in CEE, Southern Europe, and Africa.

Source: Frost & Sullivan
Key Takeaway: The manufacturing and healthcare verticals will drive growth in the MSS market.

Total MSS Market: Revenue Forecast by Vertical Market, EMEA, 2011–2018

*A list of “Other” vertical markets can be found in the appendix. Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Vertical Market Revenue Forecast Discussion

• The financial services and government verticals represented the largest vertical markets for MSSPs, reaching $752.6 million and $443.0 million, respectively, in 2013.

• The financial services vertical will expand at a CAGR of 9.3% from 2013 to 2018, while the government vertical will grow at a CAGR of 11.5% for the same period.

• Both verticals have relatively moderate, yet healthy CAGRs in relation to all other verticals. Maturity and the considerable size of these verticals explain the moderate growth rates.

• The majority of MSSPs experienced strong growth in the manufacturing vertical. Moreover, MSSPs expect to continue registering high growth rates, driven by the need to protect intellectual property from targeted attacks in a cost-effective manner.

• The manufacturing vertical totaled $394.0 million in EMEA in 2013 and is forecast to grow at a CAGR of 14.3%.

• Regulatory compliance and the protection of intellectual property will drive growth in the healthcare vertical. The value of healthcare was $379.2 million in 2013 and has an anticipated CAGR of 13.8%.

Source: Frost & Sullivan
Within the others category, it is important to mention the rapid growth of the energy and utilities verticals towards the end of the forecast period. As energy and utilities organizations deploy Internet-connected devices and sensors to optimize their operations and increase the quality of their services, new attacks that exploit vulnerabilities in these devices and sensors will emerge.

Leading MSSPs are already tailoring MSS offerings to detect and remediate attacks targeted at “smart” critical infrastructure. Overall, Frost & Sullivan estimates that MSSPs will experience growth rates in the utilities and energy verticals similar to those of the manufacturing and healthcare verticals.

Retail is another prominent vertical which is expected to witness high growth rates. The increasing adoption of MSS in retail is, however, associated with the need to cost-effectively comply with regulatory and industry frameworks as well as the shift from standalone ‘enterprise security’ to ‘supply-chain security’.

Source: Frost & Sullivan
Percent Revenue Forecast by Business Size

Key Takeaway: The distribution of revenue by business size will not experience major change.

Total MSS Market: Percent Revenue by Business Size, EMEA, 2013
- SMB: 19.1%
- Enterprise: 80.9%

Total MSS Market: Percent Revenue Forecast by Business Size, EMEA, 2018
- SMB: 19.9%
- Enterprise: 80.1%

Key: SMB: Small to Medium Business: fewer than 1,000 users. Enterprise: greater than 1,000 users
Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Key Takeaway: Large enterprises will continue to represent the major source of revenue for MSSPs.

Total MSS Market: Revenue Forecast by Business Size, EMEA, 2011–2018

Key: SMB: Small to Medium Business: fewer than 1,000 users. Enterprise: greater than 1,000 users

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Revenue Forecast by Business Size Discussion

- Frost & Sullivan estimated the value of the enterprise segment at $2.27 billion in 2013 and anticipates the segment will grow at a CAGR of 11.9% from 2013 to 2018.
- Accordingly, the value of the SMB segment was calculated at $536.3 million in 2013 which will develop at a CAGR of 13.1%.
- Further segregating the SMB segment, medium businesses (100 to 999 employees) and small businesses (up to 99 employees) represented 15.4% and 3.7% of the MSS market, respectively, in 2013.
- Frost & Sullivan’s research indicates that the adoption of MSS among medium-sized businesses will drive growth in the SMB segment. The growth attributed to the adoption of MSS among small organizations will be relatively low.
- Despite the faster growth of the SMB segment as a whole, the corresponding shares of enterprise and SMB segments as a percentage of the total market will remain practically unchanged throughout the forecast period.
- While a greater number of small and medium organizations adopting MSS will drive growth in the SMB segment, higher contract values will fuel growth in the enterprise segment.
- Overall, the value of MSS contracts for enterprises tend to be far larger than those for small and medium business. Enterprises' comparatively complex IT infrastructure and specific SLA requirements drive the value of MSS contracts up.
- Moreover, enterprises are typically more likely to opt for standard and high-end MSS, while SMBs tend to demand standard MSS only, usually bundling MSS with a communication services offering.

Source: Frost & Sullivan
Market Share and Competitive Analysis—Total MSS Market
Competitive Analysis Assumptions

• Frost & Sullivan calculated market shares for MSSPs based on MSS-only revenue figures.

• Revenue from MSSPs’ professional security services were excluded from the market share calculations.

• The calculations also intend to estimate the corresponding value of MSS when delivered as a part of larger managed services deals or larger IT/network security deals.

• Likewise, the calculations also intend to estimate and exclude revenue associated with security appliances and security software delivered as a part of a MSS deal.

• In the 2014 EMEA MSS update, the granularity of information provided by MSSPs, in terms of operations and revenue by region and by service, enabled Frost & Sullivan to estimate market shares more accurately.

Source: Frost & Sullivan
Market Share

Key Takeaway: The MSS market remains largely fragmented. The top 8 MSSPs do not account for more than 50% of the total market.

Total MSS Market: Percent of Sales, EMEA, 2013

- BT 8.6%
- Atos 8.1%
- IBM 5.7%
- HP 5.3%
- OBS 4.8%
- Verizon 3.9%
- T-Systems 3.5%
- Telefónica 2.7%
- Others* 57.4%

n = 50+

*A list of “other” companies can be found in the appendix.

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Market Share Analysis

- All the top 8 MSSPs have a global footprint, provide services from at least 3 SOCs, and primarily target multinational corporations.
- BT, OBS, T-Systems, and Telefónica all have a strong foothold in their local markets, namely the United Kingdom, France, Germany, and Spain, respectively. Atos has a well-distributed presence across the United Kingdom, France, Germany, and the Benelux region.
- The US-based MSSPs—IBM, HP, and Verizon—also have a well-distributed presence across EMEA countries and sub-regions.
- Atos acquired Bull, an European IT service provider specializing in cloud computing, Big Data, and cyber security solutions.
- OBS acquired Atheos, a French IT service provider with strong expertise in identity management and security management. After acquiring Atheos, OBS strengthened its capabilities in security consulting, incident response, and advanced threat detection.

**Total MSS Market: Company Market Share Analysis of Top 8 Participants, EMEA, 2013**

<table>
<thead>
<tr>
<th>Companies</th>
<th>Revenue (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BT</td>
<td>8.6</td>
</tr>
<tr>
<td>Atos</td>
<td>8.1</td>
</tr>
<tr>
<td>IBM</td>
<td>5.7</td>
</tr>
<tr>
<td>HP</td>
<td>5.3</td>
</tr>
<tr>
<td>OBS</td>
<td>4.8</td>
</tr>
<tr>
<td>Verizon</td>
<td>3.9</td>
</tr>
<tr>
<td>T-Systems</td>
<td>3.5</td>
</tr>
<tr>
<td>Telefónica</td>
<td>2.7</td>
</tr>
<tr>
<td>Others*</td>
<td>57.4</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

*All figures are rounded. The base year is 2013. Source: Frost & Sullivan*
# Competitive Environment

## Total MSS Market: Competitive Structure, EMEA, 2013

<table>
<thead>
<tr>
<th><strong>Number of Companies in the Market</strong></th>
<th>50+</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Competitive Factors</strong></td>
<td>Ability to fulfill SLAs, threat intelligence, and threat research capabilities</td>
</tr>
<tr>
<td><strong>Key End-user Groups</strong></td>
<td>Financial services, government, manufacturing, healthcare, technology, energy, utilities, and retail</td>
</tr>
<tr>
<td><strong>Major Market Participants</strong></td>
<td>BT, Atos, IBM, HP, OBS, Verizon, T-Systems, Telefónica</td>
</tr>
<tr>
<td><strong>Market Share of Top 8 Competitors</strong></td>
<td>42.6%</td>
</tr>
<tr>
<td><strong>Distribution Structure</strong></td>
<td>Primarily direct sales</td>
</tr>
<tr>
<td><strong>Notable Acquisitions and Mergers</strong></td>
<td>OBS acquired Atheos; Atos acquired Bull</td>
</tr>
</tbody>
</table>

*Source: Frost & Sullivan*
Security Asset Monitoring and Management Segment Breakdown

Key Takeaway: The CPE-based delivery mode continues to dominate security asset monitoring and management.

Important Segment Characteristics

<table>
<thead>
<tr>
<th>Factors</th>
<th>Assessment</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opportunity Size ($B)</td>
<td>1.65</td>
<td>▲</td>
</tr>
<tr>
<td>Primary Needs</td>
<td>Expertise, support to manage and monitor security devices from multiple vendors</td>
<td>---</td>
</tr>
<tr>
<td>Price Sensitivity</td>
<td>Medium</td>
<td>▲</td>
</tr>
<tr>
<td>Demand for Innovation</td>
<td>Medium</td>
<td>●</td>
</tr>
<tr>
<td>Market Share</td>
<td>58.9%</td>
<td>▼</td>
</tr>
</tbody>
</table>

Security Asset Monitoring and Management Segment: Percent Revenue by Delivery Mode, EMEA, 2013

- Hosted: 36.9%
- CPE-based: 63.1%

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
## Market Engineering Measurements


<table>
<thead>
<tr>
<th>Measurement Name</th>
<th>Measurement</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment Stage</td>
<td>Mature</td>
<td>---</td>
</tr>
<tr>
<td>Segment Revenue (2013)</td>
<td>$1.65 B</td>
<td>▲</td>
</tr>
<tr>
<td>Segment Forecast (2018)</td>
<td>$2.51 B</td>
<td>▲</td>
</tr>
<tr>
<td>Base Year Segment Growth Rate</td>
<td>9.7%</td>
<td>▼</td>
</tr>
<tr>
<td>Compound Annual Growth Rate (CAGR, 2013–2018)</td>
<td>8.7%</td>
<td>---</td>
</tr>
<tr>
<td>Price Sensitivity (scale of 1 to 10, Low to High)</td>
<td>7</td>
<td>▲</td>
</tr>
<tr>
<td>Degree of Competition (scale of 1 to 10, Low to High)</td>
<td>7</td>
<td>▲</td>
</tr>
<tr>
<td>Degree of Technical Change (scale of 1 to 10, Low to High)</td>
<td>6</td>
<td>●</td>
</tr>
<tr>
<td>Customer Loyalty (scale of 1 to 10, Low to High)</td>
<td>9</td>
<td>●</td>
</tr>
</tbody>
</table>

**TREND**

- Decreasing ▼
- Stable ●
- Increasing ▲

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Key Takeaway: Organizations will progressively adopt hosted security asset monitoring and management.

Security Asset Monitoring and Management Segment: Revenue Forecast by Delivery Mode, EMEA, 2011–2018

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
Revenue Forecast by Delivery Mode Discussion

- CPE-based security asset monitoring and management was estimated at $1.04 billion in 2013. This delivery mode is expected to grow at a CAGR of 7.7% from 2013 to 2018.

- However, the share from the CPE-based modes is expected to decrease from 63.1% in 2013 to 60.5% in 2018, while the share from hosted modes will increase 36.9% in 2013 to 39.5% in 2018.

- Likewise, the value of the hosted sub-segment was estimated at $610.7 million in 2013, which is forecast to expand at a CAGR of 10.1% from 2013 to 2018.

- ITSPs and security specialists tend to have a large portion of their customer base, and consequently revenue, coming from CPE-based security asset monitoring and management.

- Organizations’ preferences and regulatory requirements explain the comparatively high share of the CPE-based sub-segment throughout the forecast period. Many organizations choose CPE-based over hosted methods because they feel they have greater control over their assets and security operations.

- CSPs tend to have a relatively high portion of their customer base, and revenue, coming from hosted delivery modes. CSPs’ strong value proposition in connectivity and managed network services explain this trend.

- The adoption of third-party cloud services will have an impact on the delivery of hosted security asset monitoring and management. This increasing adoption will require a concerted effort and clear contractual clauses between third-party cloud service providers, MSSPs, and common client organizations.

- MSSPs will collect data from the third-party cloud service provider’s infrastructure that serve common client organizations to build a complete picture of the IT infrastructure, both cloud-based and on-premise.

Source: Frost & Sullivan
The Last Word
The Last Word—Predictions

1. Threat intelligence and incident remediation will be the major growth drivers in the MSS market.

2. MSSPs will continue looking for merger and acquisition targets either to fortify their MSS portfolio or to expand into new geographies or verticals.

3. The manufacturing, healthcare, energy, and utilities verticals will command the MSS market in terms of growth rates.

Source: Frost & Sullivan
The Last Word—Recommendations

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>MSSPs should concentrate on building up, organically or through acquisitions, their threat intelligence and incident response capabilities.</td>
</tr>
<tr>
<td>2</td>
<td>Many EMEA-based CSPs and ITSPs with an MSS offering suffer from low brand awareness of their security capabilities. MSSPs should effectively communicate and demonstrate their MSS capabilities to current and potential customers.</td>
</tr>
<tr>
<td>3</td>
<td>EMEA-based MSSPs highlight their lack of affiliations to the US government as a competitive advantage. US-headquartered MSSPs should prepare marketing programs to clear organizations’ unfounded concerns.</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan
Legal Disclaimer

Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Our customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for customers’ internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the permission of the publisher.

For information regarding permission, write to:

Frost & Sullivan
331 E. Evelyn Ave. Suite 100
Mountain View, CA 94041
Appendix
Market Engineering Methodology

One of Frost & Sullivan’s core deliverables is its Market Engineering studies. They are based on our proprietary Market Engineering Methodology. This approach, developed across the 50 years of experience assessing global markets, applies engineering rigor to the often nebulous art of market forecasting and interpretation.

A detailed description of the methodology can be found [here](#).
# Market Engineering Measurements


### Market Overview

<table>
<thead>
<tr>
<th>Measurement Name</th>
<th>Measurement</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market Stage (Nascent, Growth, Mature)</td>
<td>Growth</td>
<td>—</td>
</tr>
<tr>
<td>Market Revenue (2013)</td>
<td>$2.81 B</td>
<td>▲</td>
</tr>
<tr>
<td>Average Package Deal Size</td>
<td>$280,000</td>
<td>▼</td>
</tr>
<tr>
<td>Market Size at End of Forecast Period (2018)</td>
<td>$4.99 B</td>
<td>▲</td>
</tr>
<tr>
<td>Base Year Market Growth Rate</td>
<td>13.8%</td>
<td>▼</td>
</tr>
<tr>
<td>Compound Annual Growth Rate (CAGR, 2013–2018)</td>
<td>12.2%</td>
<td>—</td>
</tr>
<tr>
<td>Customer Price Sensitivity (scale of 1 to 10, Low to High)</td>
<td>6</td>
<td>•</td>
</tr>
<tr>
<td>Degree of Technical Change (scale of 1 to 10, Low to High)</td>
<td>7</td>
<td>•</td>
</tr>
<tr>
<td>Market Concentration (% of base year market controlled by top 3 competitors)</td>
<td>22.4%</td>
<td>▲</td>
</tr>
</tbody>
</table>

**Note:** All figures are rounded. The base year is 2013. Source: Frost & Sullivan
## Market Engineering Measurements (continued)

### Competitor Overview

<table>
<thead>
<tr>
<th>Measurement Name</th>
<th>Measurement</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Competitors (active market competitors in base year)</td>
<td>50+</td>
<td>⬤</td>
</tr>
</tbody>
</table>

### Total Addressable Market

<table>
<thead>
<tr>
<th>Measurement Name</th>
<th>Measurement</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replacement Rate (average contract period for MSS)</td>
<td>3.3 years</td>
<td>▲</td>
</tr>
<tr>
<td>Average Renewal Rate (per customer)</td>
<td>93.9%</td>
<td>▼</td>
</tr>
</tbody>
</table>

### Industry Advancement

<table>
<thead>
<tr>
<th>Measurement Name</th>
<th>Measurement</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Product Development Time</td>
<td>9 Months</td>
<td>○</td>
</tr>
</tbody>
</table>

*TREND

<table>
<thead>
<tr>
<th>TREND</th>
<th>Decreasing</th>
<th>Stable</th>
<th>Increasing</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>▼</td>
<td>○</td>
<td>▲</td>
</tr>
</tbody>
</table>

*Companies with revenue of more than $1 M revenue.

Note: All figures are rounded. The base year is 2013. Source: Frost & Sullivan
List of Items Included in “Others”

List of all vertical markets included in “Others” for Total MSS Market—Revenue Forecast by Vertical Market

- Business services (including legal)
- Consumer
- Energy
- Entertainment
- Gaming
- Media
- Retail
- Utilities

Source: Frost & Sullivan
### Partial List of Other Companies Included for Market Sizing Purposes

<table>
<thead>
<tr>
<th>Above Security</th>
<th>HCL Technologies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accenture</td>
<td>NTT Com Security</td>
</tr>
<tr>
<td>Accumuli Security</td>
<td>KPN</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>Open Systems</td>
</tr>
<tr>
<td>BAE Systems</td>
<td>Sentor</td>
</tr>
<tr>
<td>Belgacom SA</td>
<td>SecureData</td>
</tr>
<tr>
<td>CompuCom</td>
<td>Symantec</td>
</tr>
<tr>
<td>Computacenter</td>
<td>Tata Communications</td>
</tr>
<tr>
<td>Dell SecureWorks</td>
<td>Unisys</td>
</tr>
<tr>
<td>Dimension Data</td>
<td>Wipro</td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan
# Table of Acronyms Used

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
<th>Abbreviation</th>
<th>Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACH</td>
<td>Austria and Switzerland</td>
<td>MSSP</td>
<td>Managed Security Service Provider</td>
</tr>
<tr>
<td>BT</td>
<td>BT Global Services</td>
<td>PSS</td>
<td>Professional Security Services</td>
</tr>
<tr>
<td>CAGR</td>
<td>Compound Annual Growth Rate</td>
<td>OBS</td>
<td>Orange Business Services</td>
</tr>
<tr>
<td>CAPEX</td>
<td>Capital Expenditure</td>
<td>SI</td>
<td>System Integrator</td>
</tr>
<tr>
<td>CEE</td>
<td>Central and Eastern Europe</td>
<td>SLA</td>
<td>Service-level Agreement</td>
</tr>
<tr>
<td>CPE</td>
<td>Customer-premises Equipment</td>
<td>SMB</td>
<td>Small and Medium Business</td>
</tr>
<tr>
<td>CSP</td>
<td>Communication Service Provider</td>
<td>SOC</td>
<td>Secure Operating Center</td>
</tr>
<tr>
<td>DLP</td>
<td>Data-loss Prevention</td>
<td>VAR</td>
<td>Value-added Reseller</td>
</tr>
<tr>
<td>EMEA</td>
<td>Europe, Middle East, and Africa</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IAM</td>
<td>Identity Access Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ITSP</td>
<td>IT Service Provider</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MEA</td>
<td>Middle East and Africa</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSS</td>
<td>Managed Security Service</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: Frost & Sullivan
Learn More—Next Steps

• Obtain Frost & Sullivan’s Network Security Subscription.

• View and access Frost & Sullivan’s Market Engineering Research.

• Attend events such as the Frost & Sullivan Growth, Innovation, and Leadership (GIL) Conference.

• Request a proposal for Growth Partnership Services or Growth Consulting Services to support you and your team to accelerate the growth of your company: myfrost@frost.com; 1-877-GoFrost (1-877-463-7678).


Source: Frost & Sullivan