FROST & SULLIVAN

# Evolving Expectations for Enterprise Security

*Key Insights on Securing Networks Against Modern Cyber Threats*

Frost & Sullivan Analysis by Chris Rodriguez

## INTRODUCTION

The threat landscape is ever changing. Enterprises must defend against a range of threats such as zero-day attacks, advanced persistent threats (APTs), polymorphic malware, evasion tactics, bots/automated attacks, and insider threats. These security challenges are then compounded by unprecedented levels of infrastructure extensions introduced by new technologies such as cloud and mobile devices. The resulting borderless networks present myriad opportunities for threat actors to exploit to gain illicit access, steal data, or commit fraud. It is in the context of this harrowing threat landscape that the need for the next evolution of enterprise security solutions is more pressing than ever.

As new threats emerge, network security technologies also must evolve—a reactive evolutionary process that resembles a "cat-and-mouse" game. Security vendors solve an emerging problem then move on to the next.

As a result, network security infrastructures now resemble a random, massive, and growing patchwork of security technologies. This complex architecture conceals a festering problem: each new security technology introduced adds yet another layer of confusion and complexity. Complexity gives way to "human error," and lack of standardization means that enterprise security infrastructures are ripe with overlooked security gaps. Despite ongoing advancements in cyber security, the *2015 (ISC)$^2$ Global Information Security Workforce Study*[1] found that more than half of the almost 14,000 security professionals surveyed believed that their organizations did not improve their defenses against threat actors compared to the prior year.

Enterprises have many of the requisite security technologies, but now need to integrate and standardize across the entire enterprise IT environment. As the foundation of a network security infrastructure, the firewall is the logical convergence point for new network security solutions and the optimal focal point for standardization. Essentially, the Enterprise Firewall must be the foundation of an evolved network security infrastructure.

Yet, modern firewalls are nearly unrecognizable from the earliest packet filters, constantly evolving in response to changing threats and technological trends. A wide range of security solutions have emerged to address each new threat, each of which can be considered within the "firewall family." An unfortunate byproduct of this vast selection is customer confusion. During a recent end-user survey, when asked to describe the benefits of an Enterprise Firewall in their own words, 30% of respondents replied "not sure."

This insight will identify market-based requirements, expected capabilities, and associated benefits of an evolved network security infrastructure with an Enterprise Firewall at its core. Additionally, the research provides an opportunity to assess enterprise security challenges and to develop appropriate strategic responses, thereby charting a course for future market development.

## ENTERPRISE FIREWALLS DELIVER ESSENTIAL SECURITY REQUIREMENTS

An evolved network security infrastructure requires an Enterprise Firewall that fulfills demanding expectations for security efficacy, performance, and new security capabilities. Frost & Sullivan conducted primary market research, surveying 764 enterprise IT decision makers and influencers in order to determine these needs. The survey revealed that there is no "one-size-fits-all" Enterprise Firewall as needs varied based on deployment type, geographic region, and the security readiness of the organization. However, the responses provide a useful launching point for determining the necessary role of an Enterprise Firewall in supporting the evolving security infrastructure.

1 *2015 (ISC)$^2$ Global Information Security Workforce Study*, Frost & Sullivan, 16 April 2015, available here.

All rights reserved © 2016 Frost & Sullivan

### *Enterprise Firewall as the Security Foundation*

Leveraging the open-ended responses from survey respondents confirms the Enterprise Firewall as a "security and protection" solution first and foremost. When asked to describe the expected benefits of Enterprise Firewall in their own words, responses repeatedly included or related to the terms "security" and "protection," including terms such as "peace of mind," "privacy," "filtering," and "control," as shown in Exhibit 1. These responses indicate that Enterprise Firewall is firmly rooted in the security architecture.

Exhibit 1 also reveals that Enterprise Firewall demands a high caliber of product performance, both in terms of security efficacy and network performance demands. Respondents listed benefits such as "fast/faster," "improved/enhanced/maximum security," and "trustworthy/reliable" when describing Enterprise Firewall benefits.

***Exhibit 1: Summary of Open-ended Responses, Describing Enterprise Firewall Benefits, Global***

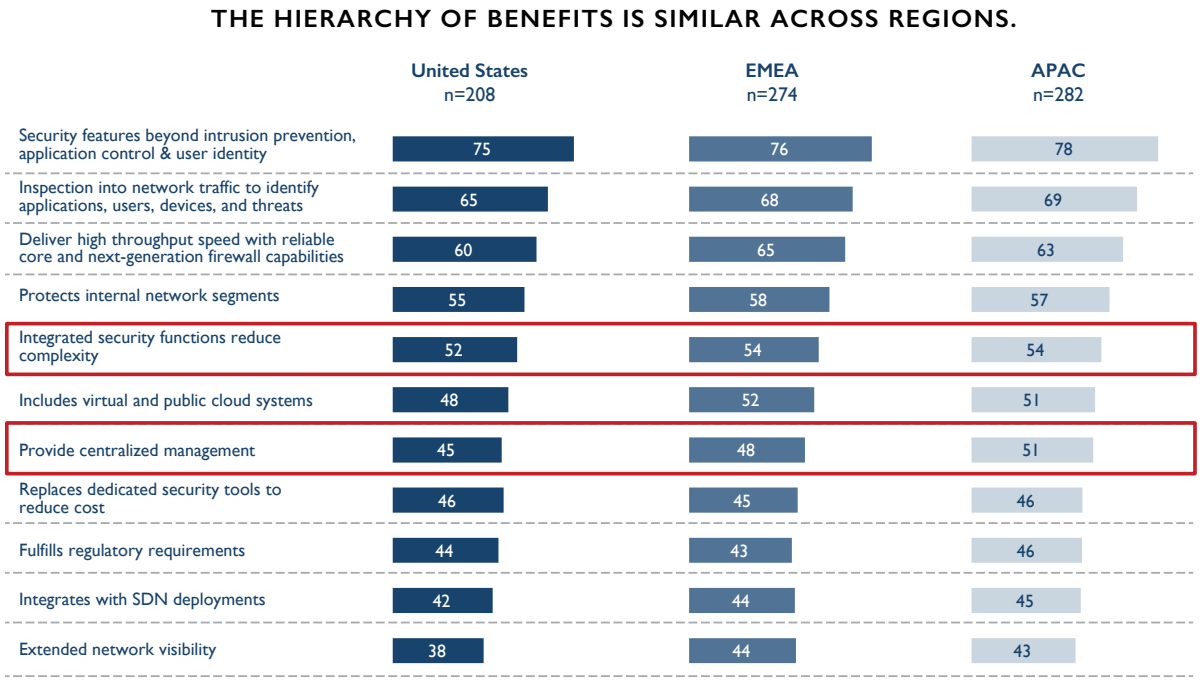
| Coded Response Category | % of Total |
|---|---|
| Safety/security/protection (unspecified) | 12% |
| Comprehensive/protects entire network/company | 7% |
| Data protection/prevents data breaches | 7% |
| Intrusion prevention/protects against external threats | 6% |
| Privacy/protects confidential/sensitive information | 5% |
| Detects/prevents viruses | 4% |
| Fast/faster/saves time | 3% |
| Protects against/reacts to advanced Web attacks | 3% |
| Traffic filtering/control of network traffic | 3% |
| Improved/enhanced/maximum security | 3% |
| Centralized management control | 2% |
| Blocks/protects against hackers | 2% |
| Low/lower cost/saves money | 2% |
| Trustworthy/reliable | 2% |
| Peace of mind/reassurance | 2% |
| Protects client/customer information | 2% |

*Source: Frost & Sullivan*

Respondents also listed "flexible" and "easy to use" as key benefits. Flexibility and ease of use are inherent product requirements that enable the Enterprise Firewall to provide reliable protection without becoming a distraction or nuisance.


All rights reserved © 2016 Frost & Sullivan

***Exhibit 2: Benefits Associated with Enterprise Firewall, All Regions***




*Source: Frost & Sullivan*

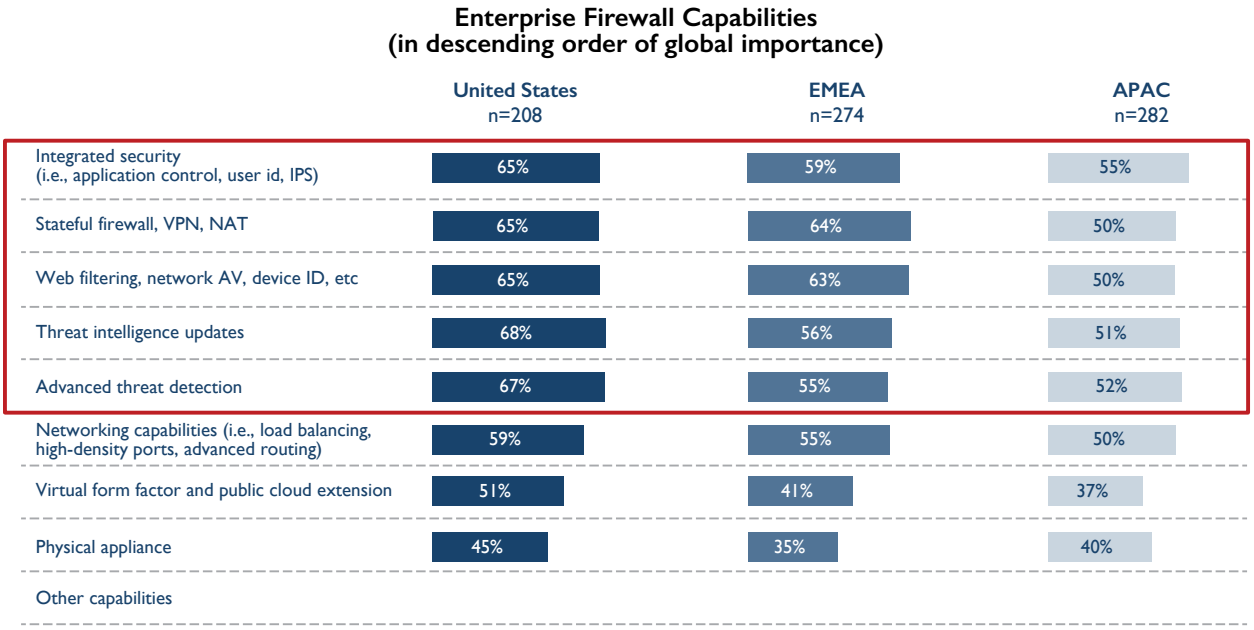
While three of the top four benefits listed by survey respondents were security- and protection-related in Exhibit 2, the expected benefits of an Enterprise Firewall go beyond security functionality. According to the survey, Enterprise Firewall should also "provide centralized management" and "integrated security functions to reduce complexity." These results indicate the desire that **Enterprise Firewall should provide consolidation and simplification.**

All rights reserved © 2016 Frost & Sullivan

### *Requisite Security Technologies for Enterprise Security*

The survey results include data that is helpful to triangulate the specific features expected from an Enterprise Firewall. According to Exhibit 3, stateful inspection, VPN, Web filtering, network AV, integrated IPS, and application control were consistently listed as expected core features. Threat intelligence and advanced threat detection also appeared as top expectations for Enterprise Firewall.

***Exhibit 3: Expected Enterprise Firewall Capabilities, All Regions***




*Source: Frost & Sullivan*

Survey respondents also indicated the features that they believe will provide valuable additions to the Enterprise Firewall. Exhibit 4 shows the most popular answers from US-based respondents, as a representative sample. Top responses included application control, SSL inspection, and integrated intrusion detection and prevention. Advanced malware sandboxing and network segmentation capabilities were in high demand as well. Many firewall vendors already offer these capabilities—a sign that the next step is to integrate and offer these security capabilities as an Enterprise Firewall. **The addition of new security technologies will provide customers with the evolved security and protection that they need to defend against modern threats.**


All rights reserved © 2016 Frost & Sullivan

***Exhibit 4: Desired Enterprise Firewall Features, US***

| | Data center n=143 | Network edge n=134 | Distributed n=95 | Cloud n=148 | Internal in front if network segments n=133 |
|---|---|---|---|---|---|
| Stateful packet filtering | 22% | 23% | 23% | 28% | 25% |
| Virtual private networking (VPN) | 15% | 16% | 20% | 15% | 19% |
| Network segmentation | 19% | 16% | 26% | 20% | 23% |
| Integrated intrusion detection and prevention | 27% | 20% | 21% | 24% | 21% |
| Application control | 29% | 24% | 21% | 35% | 22% |
| User identity and device aware controls | 24% | 25% | 23% | 26% | 21% |
| Sandboxing | 23% | 25% | 17% | 24% | 20% |
| Anti-virus | 18% | 19% | 17% | 21% | 17% |
| Web filtering | 20% | 20% | 15% | 18% | 13% |
| SSL Inspection | 22% | 27% | 16% | 27% | 22% |

*Source: Frost & Sullivan*

## *Enterprise Security Requirements are Influenced by Deployment Type*

Many organizations follow a piecemeal approach to security, stitching together various firewall products to support the unique security needs of different network environments, sometimes from multiple vendors, and hoping it works. This approach creates a disjointed security architecture that is difficult to manage and leaves gaps for threat actors to exploit. Exhibit 5 shows how the exact mix of security technologies utilized in an Enterprise Firewall vary based on deployment type.

***Exhibit 5: Enterprise Firewall Technologies Utilized, based on Deployment Type, US***

| | Data center n=143 | Network edge n=134 | Distributed n=95 | Cloud n=148 | Internal in front if network segments n=133 |
|---|---|---|---|---|---|
| Stateful packet filtering | 49% | 38% | 46% | 36% | 44% |
| Virtual private networking (VPN) | 74% | 63% | 61% | 69% | 55% |
| Network segmentation | 64% | 61% | 52% | 51% | 53% |
| Integrated intrusion detection and prevention | 60% | 54% | 63% | 51% | 52% |
| Application control | 51% | 54% | 49% | 40% | 44% |
| User identity and device aware controls | 63% | 53% | 53% | 47% | 54% |
| Sandboxing | 38% | 35% | 40% | 40% | 38% |
| Anti-virus | 70% | 63% | 64% | 59% | 60% |
| Web filtering | 66% | 66% | 61% | 59% | 59% |
| SSL Inspection | 59% | 52% | 65% | 48% | 50% |

*Source: Frost & Sullivan*

All rights reserved © 2016 Frost & Sullivan

The results show that certain network environments demand additional protection, such as distributed networks where the coverage of SSL inspection, IPS, and sandboxing point products may not extend. On the other hand, VPN was more popular in data centers and cloud, where applications and data reside. Network AV was one of the top two most utilized security technologies across all deployment types, which indicates the practice of checking for threats at multiple layers. Similarly, advanced threat sandboxing capabilities were adopted at a low but almost universal rate across all deployments (ranging from 35% to 40%).

The wide range of responses shows that some security technologies are preferred for certain deployment types, but all security technologies should at least be an option for any particular network environment. **Enterprise Firewalls should be flexible enough to support any deployment type, thereby enabling standardization of security capabilities across the entire enterprise.**

### *Enterprise Security Needs Vary Based on Maturity of the Organization*

The maturity of an enterprise's security organization will dictate a hierarchy of Enterprise Firewall needs and expectations. "Somewhat well prepared" organizations require traditional firewall, IPS, application control capabilities, advanced threat detection, rapid updates, and integrated threat intelligence in order to defend against the most sophisticated threat actors. Better prepared organizations are deploying virtual firewalls and require sophisticated networking capabilities to support their needs. Exhibit 6 shows the varying stages of enterprise security readiness and desired Enterprise Firewall capabilities.

***Exhibit 6: Enterprise Firewall Expectations by Enterprise Security Readiness Stages, Global***

| | Somewhat well prepared | Very well prepared | Extremely well prepared |
|---|---|---|---|
| Capabilities expected in an enterprise firewall | | | |
| Statefull firewall, VPN, NAT | ✓ | ✓ | ✓ |
| Integrated security (i.e., application control, user id, IPS) | ✓ | ✓ | ✓ |
| Web filtering, network AV, device ID, etc | ✓ | ✓ | ✓ |
| Advanced threat detection | ✓ | ✓ | ✓ |
| Threat intelligence updates | ✓ | ✓ | ✓ |
| Virtual form factor and public cloud extension | | ✓ | ✓ |
| Networking capabilities (i.e., load balancing, high density ports, advanced routing) | | ✓ | ✓ |

*Source: Frost & Sullivan*

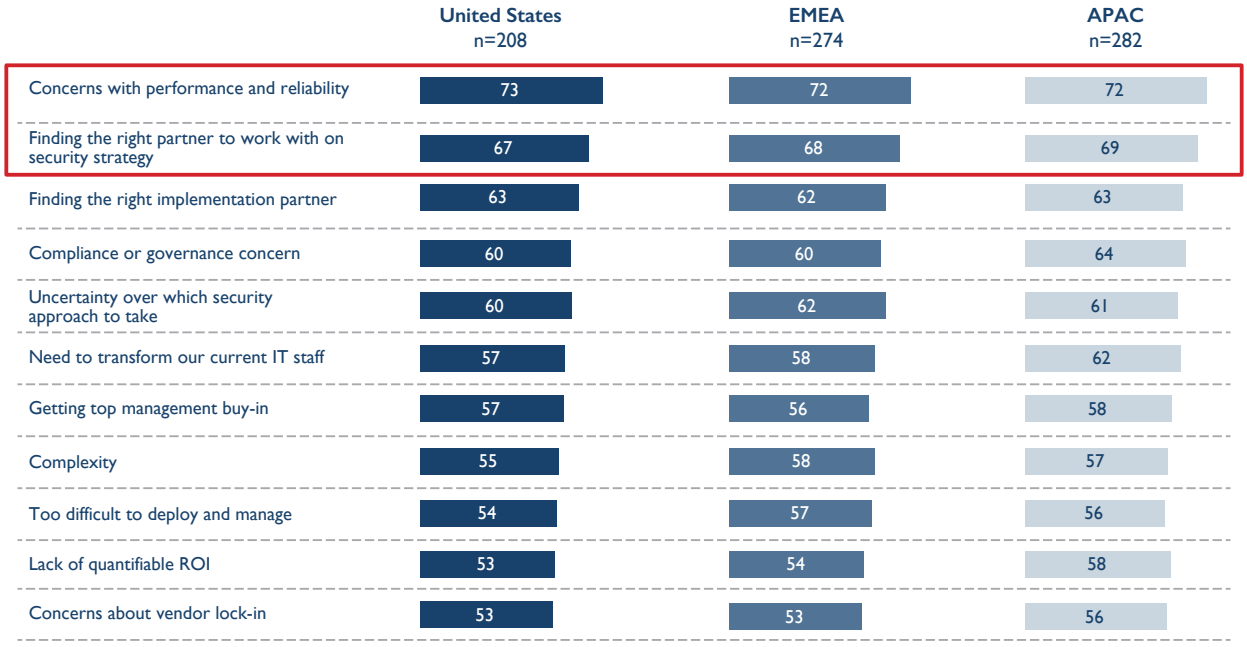

All rights reserved © 2016 Frost & Sullivan

### *Enterprise Security Challenges and Strategic Adjustments*

The survey also provides an opportunity to identify top customer challenges. Exhibit 7 shows these customer challenges, ranked, and for all regions.

***Exhibit 7: Customer Identified Challenges of Enterprise Firewall, All Regions***

**The hierarchy of challenges is similar across regions. IT staff training is also a key concern in APAC.**




*Source: Frost & Sullivan*

### *Recognize Performance and Reliability as Core Characteristics of Security*

Across all three regions, performance and reliability was the top-rated challenge for Enterprise Firewall. The need to balance new security capabilities against performance is clear. Security solutions that cannot operate without impeding legitimate traffic and end users are incomplete, whether a result of false positives, poor quality, or inefficient inspection processes. In these cases, security features are disabled, and the worst case scenario is that the solution is bypassed completely or replaced.

Enterprise Firewall should deliver advanced security technologies and provide the ability to use these capabilities. **Enterprise Firewalls should provide the performance, reliability, and security efficacy to be an enabler for new IT practices rather than a hindrance.** Additionally, performance and reliability must be considered as central to the concept of security and as core characteristics of Enterprise Firewalls. Enterprises must prioritize these characteristics when evaluating new Enterprise Firewall deployments.

### *Simplification and Integration to Mitigate Human Error and Complexity*

As shown in Exhibit 7 above, enterprises cited difficulty in deploying and managing Enterprise Firewall. Though not the highest-rated challenge, this challenge was ranked by enough respondents to indicate a material impact on Enterprise Firewall adoption. Enterprise Firewalls should provide simplification through consolidation of management of multiple security technologies into a single management console. Ideally, Enterprise Firewalls will

All rights reserved © 2016 Frost & Sullivan

offer a unified, single policy engine that enables enterprises to coordinate, identify, and manage threats in a timely manner, thereby yielding superior security efficacy.

Additionally, Enterprise Firewall vendors can aid customers through development of API-level integrations with adjacent security technologies to enable speedier deployment and integration. **The ability for Enterprise Firewall to integrate with and support a broader security ecosystem will help advance enterprises through the levels of "security preparedness,"** particularly in organizations with limited resources and personnel.

### *Prioritize Strategic Partnerships in Pursuit of Solutions*

Enterprises face a wide range of cyber threats, compounded by dissolving network perimeter borders. The ability to stay ahead of these security trends is a challenge for all but the most sophisticated organizations. Accordingly, enterprises will need a stable of sources aiding in the process of determining risk and developing appropriate strategies. Yet, the necessary security expertise is a valuable and rare resource. For most organizations, building an internal security team is a difficult proposition. Unfortunately, survey respondents indicated that finding the right partner to plan security strategy and implementation is a top challenge.

Enterprises require trusted partners that can help with security strategy and implementation, including both solutions providers and strategic partners. For example, managed security service providers (MSSPs) can help customers select and deploy the appropriate Enterprise Firewall and features needed for their specific organization and deployment type, helping enterprises deploy the solution correctly and maximize the value of their investments. This strategy will allow Enterprise Firewall vendors to deliver solutions rather than simply sell products.

## FROST & SULLIVAN: THE LAST WORD

Three of the top four customer listed benefits of an Enterprise Firewall were protection or security oriented. The security capabilities provided by an Enterprise Firewall are numerous. The Enterprise Firewall must be the foundation of modernized network security architectures and one that can function and coordinate within a broader security ecosystem in order to deal with the next evolution of threats. Based on enterprise IT security needs and expectations derived from primary market data, multi-faceted, but clear requirements for this next evolutionary stage of Enterprise Firewalls emerge.

**To provide the foundation of an evolved security architecture, the Enterprise Firewall should deliver:**

- Consolidation and simplification of security technologies and processes
- Advanced security capabilities/protection from evolving threats
- Standardization of security capabilities across all modern IT environments, deployments, and extensions
- Performance and reliability that supports security objectives
- Integration and coordination within the broader enterprise security architecture

Most importantly, the next evolutionary stage of security requires an Enterprise Firewall that is agile and flexible enough to support future needs without requiring a massive upgrade to the "next generation" of discrete and disparate security tools. The security landscape is already shrouded in confusion and hampered by disjointed security infrastructures composed of disparate tools. Frost & Sullivan expects security vendors to demonstrate leadership and vision in the marketplace by introducing an Enterprise Firewall that provides the evolved security needed to protect against modern cyber threats, yet is also flexible in order to adapt to future requirements.


All rights reserved © 2016 Frost & Sullivan

FROST & SULLIVAN

Auckland
Bahrain
Bangkok
Beijing
Bengaluru
Buenos Aires
Cape Town
Chennai
Dammam
Delhi
Detroit
Dubai
Frankfurt
Herzliya
Houston
Irvine
Iskander Malaysia/Johor Bahru
Istanbul
Jakarta
Kolkata
Kotte Colombo
Kuala Lumpur
London
Manhattan
Miami
Milan
Moscow
Mountain View
Mumbai
Oxford
Paris
Pune
Rockville Centre
San Antonio
São Paulo
Seoul
Shanghai
Shenzhen
Singapore
Sydney
Taipei
Tokyo
Toronto
Valbonne
Warsaw


**SILICON VALLEY**
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

**SAN ANTONIO**
7550 West Interstate 10,
Suite 400
San Antonio, TX 78229
Tel 210.348.1000
Fax 210.348.1003

**LONDON**
4 Grosvenor Gardens
London SW1W 0DH
Tel +44 (0)20 7343 8383
Fax +44 (0)20 7730 3343

877.GoFrost
myfrost@frost.com
www.frost.com


Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?


*For information regarding permission, write:*
Frost & Sullivan
331 E. Evelyn Ave., Suite 100
Mountain View, CA 94041