

## Stratecast Perspectives and Insight for Executives

SPIE 2008 #26 – July 11, 2008

### Trend Micro's Cloud-Client Architecture: Better Security and Good Business Rolled into One

---

#### Introduction<sup>1</sup>

Recognized throughout the information security industry, cyber threats are on a continuous trend of extracting value from their victims. It is information of value that cyber-criminals increasingly covet (fortune), not the disruption of business operations or causing brand embarrassment (fame). Moreover, fame-seeking practices are too high profile and inconsistent with the objectives of cyber-criminals. Cyber-criminals instead aim to operate clandestinely as a mole within the enterprise's communication and computing environment for as long as possible. Publicity counteracts their covert operations.

To avoid detection as they conduct their information mining activities, cyber-criminals hide their tracks by blending several techniques together with each technique or step designed to register as benign when viewed in isolation.<sup>2</sup> Only when examined in total context is the true intent of blended threats visible. Cyber-criminals are also amorphous; they are constantly changing their pathways to valuable bits of information. Assuming that a pathway will eventually be discovered and blocked, top tier cyber-criminals will create alternative pathways to stay ahead of their pursuers.

The dynamic and sophisticated dimensions of cyber threats have an additional downside - they call into question the viability of the traditional approach of client-based pattern matching (i.e., security software running on end-users' devices/systems) to identify, block, and purge malware from end-users' devices. In this bulletin, Stratecast will describe why traditional client-based pattern matching must change to remain an effective means to protect end-user devices and the information contained within these devices. Tightly related, we will also spotlight Trend Micro's recently announced evolution in its client-based security approach to a new cloud-client architecture and, to a lesser extent, competing approaches from McAfee, SonicWALL, and Websense.

---

<sup>1</sup> In preparing this report, Stratecast conducted interviews with representatives of the following companies:

- McAfee
- SonicWALL
- Trend Micro
- Websense

Please note that the insights and opinions expressed in this assessment are those of Stratecast and have been developed through the Stratecast research and analysis process. These expressed insights and opinions do not necessarily reflect the views of the company executives interviewed.

<sup>2</sup> For example, an embedded link delivered to an unsuspecting end-user in an email directs the user to a compromised or counterfeit website or webpage where malware code is hosted and transparently downloaded onto the user's device. Once present on the end-user's device, this first-instance malware independently and transparently communicates with other compromised websites to download additional, more potent malware.

## Client-based Pattern Matching Under Attack

There are three primary reasons why client-based pattern matching is straining to be an effective deterrent to cyber-criminals.

- 1. Growing Pattern File Size** – Malware writers have long known that one means to stay ahead of pattern matching is to develop new malware or variant strains of existing malware. With time needed for anti-malware sleuths to discover and analyze new malware and malware variants, prepare accurate recognition patterns, and distribute updated pattern files or incremental file deltas to client devices, there is a window of time in which end-user devices are at a higher state of vulnerability. Also, because there are no rules on malware retirement (cyber-criminals do not play by rules), pattern files have no theoretical limit in size. Consequently, as the pattern files grow in size, the consumption of processing, memory, and storage on the client devices to scan messages and files for the existence of malware also increases. Absent a corresponding increase in computing resources, malware scans will take longer and can have a more noticeable impact on other end-user activities that share the same processors and memory.
- 2. Increasing File Update Frequency** – Correlated to the previous point, the uptick in malware production necessitates more frequent updates to pattern files. With more frequent file updates, end-users are more prone to interruptions in their daily routines due to more frequent instances of updating (e.g., from weekly to daily). In addition, a corresponding higher level of enterprise bandwidth usage will be demanded as end-users access updated pattern files from the anti-malware software provider. Depending on the number of end-users from the same location simultaneously retrieving new or incremental pattern files (e.g., at the start of the business day) and the size of the enterprise's Internet access link, bandwidth use for file updates can potentially crowd out other legitimate use of that finite resource – bad for other business operations. Conversely, if the enterprise attempts to restrict the amount of bandwidth available for pattern file updates (e.g., task-oriented bandwidth throttling), the time required by end-users to retrieve the updates will increase – also bad for business as users are potentially delayed in engaging in other job tasks. Both of these occurrences rise in prominence with NAC (Network Access Control) policies that require the most current pattern files be present on end-users' devices before access to the enterprise network is permitted. IT/security personnel will also be increasingly tasked with evaluating when a pattern file update should be an immediate update on end-user devices or can be delayed.
- 3. Threat Correlation Required** – The painful reality of blended threats is that they cannot be recognized in isolation (i.e., at the component level). Contextual understanding and correlation with other sources are necessary. Yet, this creates a dilemma for client-based security as greater volumes of information (e.g., more and larger data files) and a more sophisticated security application would need to be resident, maintained, and run on the end-user device. The net result is a higher consumption of the device's storage space, processing power, and memory to potentially impractical levels. In addition, the cost of updating data files and the security client software (size and frequency) further taxes the computing resources of the end-user device and the enterprise's Internet access link.

## Business Considerations also at Odds with Client-Based Pattern Matching

The previous three reasons are centered on issues end-users and enterprises encounter with an increase in the size and update frequency of pattern files and the lessening effectiveness of non-contextual pattern files to mitigate blended attacks. These are not the only reasons why anti-malware pattern files will lose favor. Security vendors also have reasons to be concerned about the implications to their businesses. One reason is related to anti-malware vendors' operational costs, another is related to the strategic direction of security, and the last reason relates to the mature market challenges of client-based anti-malware software.

- **Operational Costs** – Distribution of pattern file updates is a critical link in the effectiveness of anti-malware software. However, there is a fundamental problem with this linkage and that is that the cost of pattern file distribution is also correlated with the size and update frequency of these files. Larger and more frequently updated pattern files force the anti-malware vendor to increase its investment in distribution infrastructure. Unless there is a corresponding reduction in the cost of the distribution infrastructure on par with the increase in combined impact of file size and update frequency, anti-malware vendors are at risk of shrinking margins. In addition, a subset of anti-malware vendors has turned to Content Distribution Networks (CDNs) to reduce their investments in distribution infrastructure and to accelerate the delivery of pattern files to end-users. The latter objective clearly assists in lessening the first two issues listed in the previous section, but at the premium fees demanded by CDN providers.
- **Strategic Direction of Security** – The evolution of security is moving beyond just protecting systems, to protecting sensitive data/privileged information. Subsequently, data loss prevention (DLP) is a growing segment within the security industry. Measuring the effectiveness of DLP solutions is based on how well data is protected in three risk scenarios: data-at-rest, data-in-use, and data-in-motion. End-user devices (e.g., laptops and desktops) present a perplexing challenge for DLP effectiveness as privileged information stored (data-at-rest) in these devices is at risk when these devices are Internet-connected and when they are not. For example, privileged information can be transferred by the end-user from laptop and desktop hard drives to removable storage media (e.g., USB flashdrives) when these devices are offline. Online, privileged information is additionally at risk when end-users with malice, ignorance, or carelessness send privileged information to unauthorized persons (data-in-use risk) or send privileged information through an unprotected/unencrypted channel (data-in-motion risk). Consequently to effectively address all three of these risk scenarios regardless of online or offline state, laptops and desktops must be equipped with DLP software technology that resides on end-user devices and is persistently at work (i.e., whenever the device is turned on). Similar to anti-malware pattern matching, DLP software will consume storage, CPU cycles, and memory of client devices and therefore compete for these same device resources with other business applications. This creates a quandary for security vendors as they market client-based DLP solutions to enterprises that are already straining from the effects of existing client-based security software on device resources. Finding a means to protect privileged information and block malware without worsening the resource contention situation, or hopefully improve it, should, in our view, be a critical area of focus for security vendors.

- **Mature Market Challenges of Client-based Anti-virus Software** – Anti-virus software is among the most tenured of security software running on desktops and laptops. According to Stratecast’s parent company, Frost & Sullivan, the annual growth rate of worldwide sales of PC anti-malware software (includes anti-virus) has been declining since 2005 and is projected to continue to grow but at a declining rate over the foreseeable future.<sup>3</sup> Contributing to this trend are several factors. Among these are the high penetration of client-based anti-malware software and the market impact of Microsoft as a provider of security. Also victimizing this market is the ease at which individual end-users and enterprise IT organizations can switch anti-malware vendors. For a company like Trend Micro that has a large market share in client-based anti-malware software, future growth prospects are disconcerting unless the company can locate and penetrate new market opportunities and/or take market share away from its primary competitors. Based on the company’s business results, Trend Micro has been successful in market share take-aways. How long this trend will continue is uncertain as the market is extremely competitive.

## Trend Micro’s Cloud-Client Solution

Through a 20-year successful history as a vendor of client-based anti-virus software, Trend Micro become increasing aware of the growing issues client-based pattern files can have on its subscriber base and the company’s business. Trend Micro has responded with the introduction of a cloud-client architecture. With the company’s cloud-client architecture, now in enterprise beta stage, the functions of detection and removal of malware are transplanted from client devices to Trend Micro’s Smart Protection Network, a multi-subscriber environment hosted in the company’s globally-distributed security operation centers.

Trend Micro’s cloud-client architecture represents a continuation of the company’s foray into Software as a Service as a delivery model for security. Last year, the company launched SecureCloud; a multi-subscriber hosted platform that supports messaging security services (anti-virus, spyware, spam, and phishing) and on-demand vulnerability scanning of eCommerce websites.

According to Trend Micro, its cloud-client architecture and Smart Protection Network resolve several of the previously described issues of client-based pattern matching:

- **End-user device requirements are materially reduced** – With a more limited role at the end-user devices, demand on CPU and memory is cut materially. Storage requirements are also reduced. Locally on end-user devices, Trend Micro’s anti-malware software will have a partial role in detecting malware based on a smaller sized pattern file representing a subset of the company’s pattern inventory. The client software will also function as a communicator between the end-user device and the Smart Protection Network to detect and purge end-user devices for additional instances of malware.
- **Bandwidth consumption for pattern updates is also materially reduced** – Since the pattern file on end-user devices is reduced in size and the detection of newly discovered malware will be conducted in the cloud, the frequency of pattern file updates on end-user devices is correspondingly reduced.

---

<sup>3</sup> “Worldwide Anti-Malware Products Market,” July 2007.

- **End-user transparency in the functioning of anti-malware protect returns** – With less frequent pattern file updates and reduced demand on device resources (CPU and memory), end-user interference from the operation of client-based anti-malware software is reduced. However, as the company discloses, file scanning times will take longer due to the communication between end-user devices and the cloud environment. Additionally, this client-to-cloud communication will consume bandwidth, offsetting a portion of the bandwidth savings associated with less frequent pattern file updates. For large enterprise locations, Trend Micro will advocate the deployment of a Trend Micro appliance within the enterprise network perimeter to replicate the functionality of the cloud environment. The Trend Micro appliance, named Scan Server, will receive frequent updates from the Smart Protection Network. Currently, Scan Server updates occur hourly. In the future the company will increase the frequency to every 15 minutes.
- **Accelerate time to protect** - By relying on a more nimble cloud environment (or Trend Micro Scan Server appliance) to detect recently discovered malware and blended attacks (next bullet point), Trend Micro accelerates the time to protect its customers. Delays in protection due to missed or postponed pattern file updates will, in concept, become inconsequential. With production speed of new malware being cyber-criminals' ally, the quickened pace of cloud or appliance file updates will further close enterprises' window of vulnerability from new malware.
- **Effectiveness in combating blended attacks is improved** – Due to the higher degree of scalability and greater level of available computing resources, the cloud portion of cloud-client architecture (i.e., Smart Protection Network), is a more conducive environment to combat blended attacks than end-user devices.
- **Reduced distribution expense in pattern file updates** – By lessening the size and frequency of pattern file updates to end-user devices and, in large enterprise settings, leveraging the Scan Server appliance to interface with end-user devices, Trend Micro's operational costs for pattern file distribution will be less. Certainly this cost reduction will not reward Trend Micro's net income on a dollar-for-dollar basis. A portion, if not all, of the distribution cost savings will be re-directed to enhance the company's Smart Protection Network. If the protection benefits of the Smart Protection Network materialized (i.e., accelerated time to protect its customers and improved effectiveness in combating blended attacks), the company competitiveness in the security market will improve and lead to an increase in subscribership. In this scenario, the redirection of operational expenses to product development expense is favorable to Trend Micro.

Regarding the point of improving effectiveness in combating blended attacks and relative to client-based computing, the larger and more sophisticated computing resources in the Smart Protection Network enable Trend Micro to combine and correlate a greater number of malware detection sources from which to discover and then take action against blended attacks. Here too, Trend Micro's previous and recent research and development efforts directly support the Smart Protection Network. For example, the company has steadily expanded its reputation scope. In 2005, the company introduced email reputation and followed the next year with web reputation. This year Trend Micro added file reputation. In addition to reputations of email destinations, web addresses, and files, the company combines other sources and types of analysis to create a broad and deep

perspective on Internet threats. As to be expected with the company's expanding reputation rating efforts, Trend Micro conducts analysis of malware, spam, and URLs. The company also maintains a white list of trustworthy Internet destinations, incorporates customer feedback, hosts honeypots, and conducts web crawlers – all to improve its accuracy to stop the bad.

## **Trend Micro is Not Alone**

In the security industry where mergers, acquisitions, and technology partnerships are common, creating and sustaining competitive differentiation based solely on unique product attributes or architecture is challenging. Ideas that show promising market acceptance quickly spread among security companies. Even more common, security companies hear and respond to similar needs from their current base of customers and prospects. While each security company will respond differently to satisfy the perceived need, the net result is several companies claiming “a better mousetrap.” These same phenomena are present in relation to Trend Micro's Cloud-Client architecture initiative. Following are three competitive examples.

### ***McAfee***

As a primary competitor to Trend Micro in anti-virus client software, McAfee also understands the same difficulties which larger and more frequent updates to pattern files represent. McAfee, however, is taking a different approach. McAfee's approach is to use behavioral technology that the company developed through its Avert Labs to slow the growth in signatures. According to Jeff Green, Senior Vice President of McAfee Avert Labs, the use of behavioral technology enables the company to condense thousands of signatures to hundreds without compromising detection accuracy.

It is also important to note that McAfee is already a player in perimeter security appliances with McAfee Total Protection (ToPS) for Network. ToPS for Network is a pair of hardware solutions that support Email and Web security, intrusion prevention, and patch mitigation. For comparison, Trend Micro is not as well-established in perimeter security appliances/platforms. Moreover, if McAfee senses that its customers demand a reduction in the processing and memory burden placed on McAfee-equipped endpoints, we anticipate that McAfee would examine ways to re-direct a portion of that computing demand to the ToPS for Network platforms.

### ***SonicWALL***

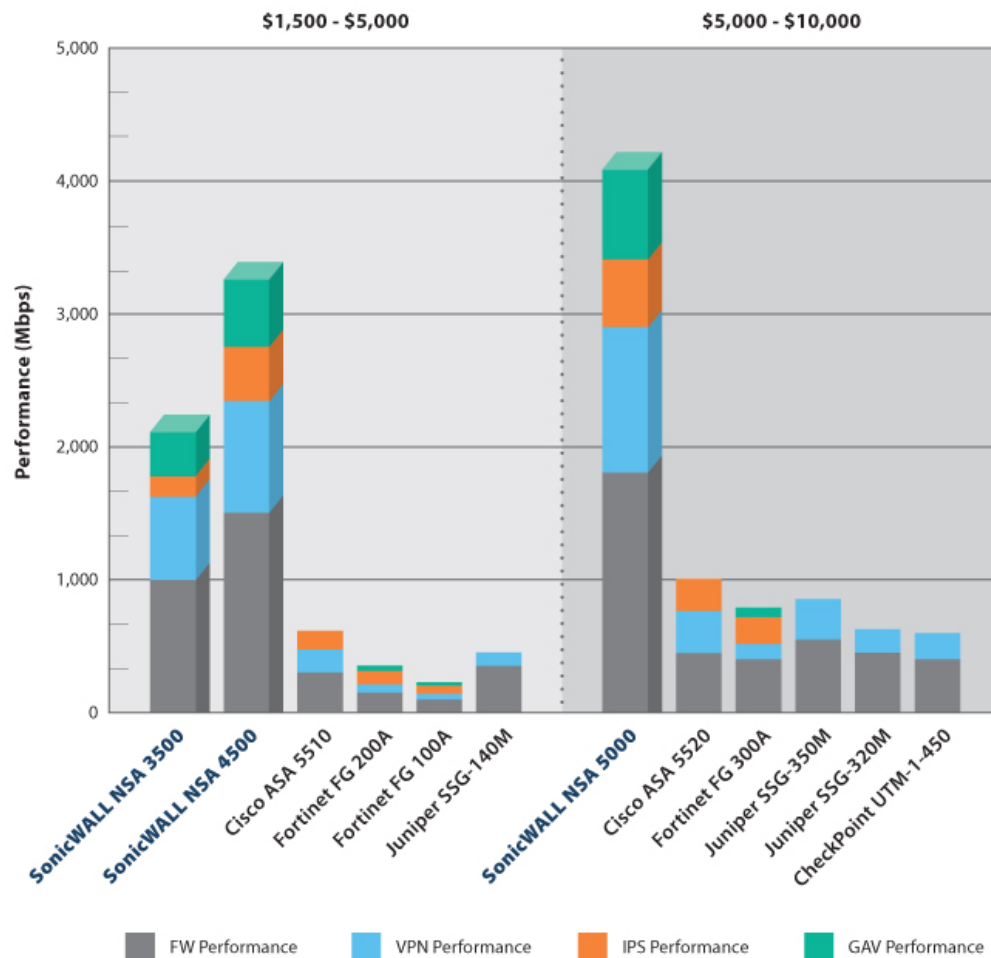
SonicWALL has a well-established gateway appliance presence within business networks and one that is moving up market with its 2007 acquisition of Aventail. Aventail, known for its SSL VPN product, primarily focused its product and channel strategy on the large enterprise segment. In addition to the talent and technology from Aventail, SonicWALL has been upping the performance dimensions of its NSA (Network Security Appliances) Series Appliances. These appliances deliver UTM (Unified Threat Management) protection. Based on performance data from competitors' product datasheets and shown in the following Figure 1, the combination of SonicWALL's Reassembly-Free Deep Packet Inspection technology and multi-core processing, delivers combined processing performance on VPN, Firewall, IPS, and anti-virus functions that is factors greater than several of the company's largest UTM competitors (Cisco, Juniper, Fortinet, and Check Point).

With this performance scalability, SonicWALL is positioned well to examine strategies that push processing demands from end-points to its gateway platforms or cooperatively share processing duties among endpoints and the gateway platform.

**Figure 1**

**SonicWALL NSA Series Performance Comparison**

**Performance: SonicWALL NSA Series vs. Competition**



Source: Compiled by SonicWALL based on Competitor's Datasheets

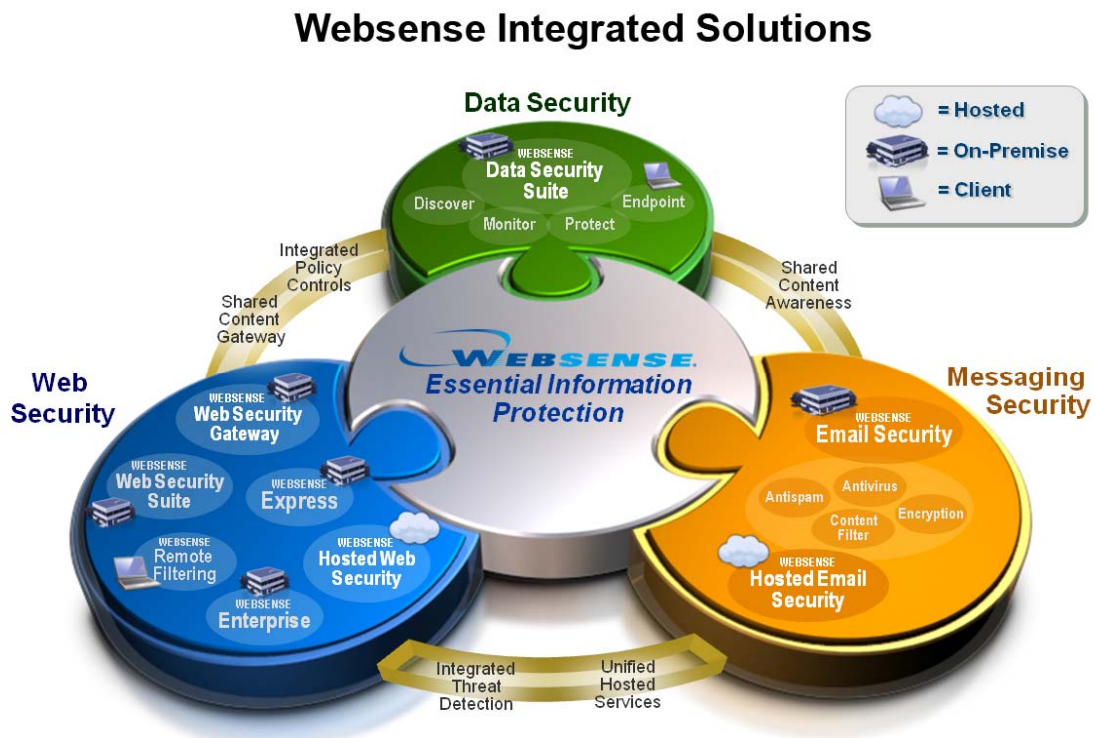
**Websense**

Websense is a unique example of a company that is executing on a strategy that places its security technologies in three locations: end-points (client), in gateway platforms (on-premise), and in the cloud (hosted). The depiction that follows in Figure 2 illustrates Websense's intersection of security functionality (Data Security, Web Security, and Message Security) and location (client, on-premise, and hosted). With this product strategy, Websense places itself in a rich position to:

- Consolidate and integrate the management and computing footprint of security functionality (data, web, and message) at common locations (client, on-premise, and hosted),<sup>4</sup> and
- Synergize functionality across locations.

**Figure 2**

**Websense’s Multi-Location Security Approach**



Source: Websense

<sup>4</sup> McAfee also has a growing product suite in data leakage prevention from which to pursue a similar consolidated footprint at endpoints, where the company’s principal location focus exists, and potentially at gateways in the future. Trend Micro entered the data leakage prevention market in 2007 with the acquisition of Provilla.

## Stratecast The Last Word

Dormancy is intolerable in the security industry. The threat environment is changing; how and where users communicate is changing; regulations are changing, and competition is fiercer. Approaches to security that were suitable a decade ago are no longer adequate. Change in how security is designed and conducted must be a strategic imperative for all security companies.

Trend Micro's cloud-client architecture and the product strategies of McAfee, SonicWALL, and Websense, briefly described in this bulletin, signal that sole reliance on client software to combat cyber threats is an inadequate product strategy. However, where threat mitigation should optimally be conducted remains an open question. Client-based software still has an important role due to proximity to users and locally stored data, and running of business applications. Plus, as indicated, persistent operations, particularly in data leakage prevention, is needed. Gateways and cloud-based environments offer several attributes that are, at minimum, harder if not impractical to duplicate at end-user devices: performance, scalability, uniformity, extensibility, and centralization of policy management and enforcement. In addition, this attribute gap will widen as handheld devices which complement or replace laptops, desktops and unmanaged devices with limited processing, memory, and storage also require protection (e.g., wireless access points and printers). In addition, gateways and cloud environments offer the added benefit of shielding network access bandwidth from unwanted traffic by virtue of being at the ends of the access link - at the enterprise network (gateway) and at the Internet edge (cloud). A gateway also has the benefit of reducing redundant use of Internet access bandwidth and speeding protection to client systems by being the single repository for signature files and other security software updates for LAN-connected end-user devices.

As part of Stratecast's on-going analysis of the network and information security industry, the advancement of distributed or collaborative security that spans multiple operational locations (endpoints, gateways, and cloud) will remain an important focal point for us. In addition, this focal point will have several perspectives as demonstrated in this SPIE: how security is improved, how security vendors will respond to this trend, and what will be the impact to the competitive landscape.

### ***Michael Suby***

Director

Stratecast (a Division of Frost & Sullivan)

[msuby@stratecast.com](mailto:msuby@stratecast.com)

**About Stratecast**

Stratecast assists clients in achieving their strategic and growth objectives by providing critical, objective and accurate strategic insight on the global communications industry. As a division of Frost & Sullivan, Stratecast's strategic consulting and analysis services complement Frost & Sullivan's Market Engineering and Growth Partnership services. Stratecast's product line includes subscription-based recurring analysis programs focused on Business Communication Services (BCS), Consumer Communication Services (CCS), Communications Infrastructure and Convergence (CIC), OSS and BSS Global Competitive Strategies (OSSCS), and our weekly opinion editorial, Stratecast Perspectives and Insight for Executives (SPIE). Stratecast also produces research modules focused on a single research theme or technology area such as IMS and Service Delivery Platforms (IMS&SDP), Managed and Professional Services (M&PS), Mobility and Wireless (M&W), Multi-Channel Video Programming Distribution (MVPD), Network Infrastructure and Operations (NIO), Secure Networking (SN) and Unified Communications (UC). Custom consulting engagements are available. Contact your Stratecast Account Executive for advice on the best collection of services for your growth needs.

**About Frost & Sullivan**

Frost & Sullivan, a global growth consulting company founded in 1961, partners with clients to create value through innovative growth strategies. The foundation of this partnership approach is our Growth Partnership Services platform, whereby we provide industry research, marketing strategies, consulting and training to our clients to help grow their business. A key benefit that Frost & Sullivan brings to its clients is a global perspective on a broad range of industries, markets, technologies, econometrics, and demographics. With a client list that includes Global 1000 companies, emerging companies, as well as the investment community, Frost & Sullivan has evolved into one of the premier growth consulting companies in the world.

**CONTACT US**

For more information, visit [www.stratecast.com](http://www.stratecast.com), dial 877-463-7678, or email [inquiries@stratecast.com](mailto:inquiries@stratecast.com).