

**SECURITY &
ROBUSTNESS TEST
INNOVATION; DRIVERS,
CONSIDERATIONS AND
CODENOMICON**



The Value of Security and Robustness Testing Innovation

Security Test and Measurement Innovation Awarded to Codenomicon DEFENSICS

MARKET OVERVIEW / KEY CHALLENGES

In today's connected and converged environment, threats to online applications, networks, mobile devices and critical infrastructure are evolving with alarming frequency and velocity. Hacks, bots, malware, worms, distributed denial of service (DDoS) attacks, and other threats are becoming more targeted, automated and sophisticated – with dire consequences ranging from service impact, lost sales, stolen data, legal liability and tarnished brand.

Increased attack volume and higher threat levels have elevated the need for a realistic security and robustness assessment of devices, applications and systems. Security testing at all levels has become a best practice.

By testing applications, network infrastructure and devices against potential threats and actual attacks; it is possible to identify exposures, capacity and quality issues. With the correct test procedures, security test equipment offers exceptional value; including improving development quality, problem resolution time savings, risk reduction, efficient resource allocation, and so on. However, developing and maintaining adequate testing capacity that help customers stay ahead of the threat still persists in the market.

Some of the key challenges faced by software developers, network equipment providers, carriers and enterprises include:

- Ever-changing attack techniques and vectors: security threats are highly dynamic, and new attacking techniques are constantly emerging which prove to be a significant challenge for signature and even behavior based security countermeasures. New threat vectors, such as wireless communications, web applications, client-side shareware and malware, expose undocumented application, network and media issues as well as facilitate zero-day threats.
- The industry is observing more distributed and accelerated deployment of corporate- and commercially-developed applications and respective infrastructure systems that contain protocol implementation and security faults: companies and service providers are deploying applications that leverage the use of networked, wireless, external and client-based open protocols. Many of the applications and devices have open (and even custom) protocol implementation issues that have resulted in resiliency and security exposures. This wide and less controllable attack surface creates a fertile ground for potential vulnerabilities to be exploited and breaches to occur – hence the notoriety of patches, attacks and service outages.
- Development pressures and lack of security resources: the number of vulnerabilities within applications highlights the current drive to quickly deliver innovation at the possible expense of greater security risks. These commercial innovation risks are also observed in internally developed corporate applications. Given limited development and operational security resources and expertise, it is arduous to keep up with known and new threats – as well as maintaining countermeasures and quality assurance.
- Extending layers of defense: while IT and security staff have moved beyond investments in perimeter defenses and have looked to minimize internal threats, many organizations are only recently investing in solutions which address more secure application development processes and pre-deployment security and availability exposures.

Given the issues and constraints detailed above, it is expected that investments in security test equipment will reach well over \$460 million by 2013. This paper addresses the drivers behind security test and measurement. It conveys the background behind the Frost & Sullivan test and measurement award and product details regarding Codenomicon DEFENSICS security and robustness testing platform.

AWARD CATEGORIES & RELEVANCE

Security test equipment currently offers significant advantages for those developing and deploying networked, wireless, and distributed applications, as well as organizations extending connectivity to customers, partners and users. Given the cost and resource savings advantages of testing applications, services and infrastructure prior to deployment - the world security test equipment market is in a high growth stage and is expected to experience accelerated growth in the near future. The emergence of new networking, virtualization, mobile and software as a service (SAAS) technologies, and the demand for a higher quality of service are expected to lead to the launch of new products, features and services by test equipment vendors. Bottom-line: with an increase in network convergence and service complexity, security and robustness testing has become critical.

In such a scenario, product differentiation innovation is likely to be among key competitive factors for test and measurement vendors, and more importantly – of value and importance to network equipment vendors, carriers and enterprises. A strategic analysis of factors such as product quality, product enhancement, and technology innovation has been performed by Frost & Sullivan to identify the vendor that leads the market in product differentiation innovation.

2007 GLOBAL FROST & SULLIVAN AWARD FOR PRODUCT DIFFERENTIATION INNOVATION

Award Description

The Frost & Sullivan Award for Product Differentiation Innovation is presented each year to the company that has best demonstrated the ability to develop and/or advance products with more innovative capabilities than competing vendors and products. This Award recognizes the company's successful adoption of new or existing technology that has become a part of its well-designed product family. Such innovation is expected to significantly contribute to the industry in terms of product performance and degree/rate of technical change.

Research Methodology

Before considering the recipient of this Award, our analyst team tracks competing market participants' product differentiation strategies through ongoing research. This research consists of market participant interviews, end-user surveys, end-user interviews, and extensive secondary research. The data compiled through this research is analyzed based upon specific measurement criteria for this Award. Participants are then ranked with respect to the measurement criteria. The Award recipient is ranked number one in the industry.

Measurement Criteria

In addition to the methodology described above, there are specific criteria used in determining the final ranking of industry competitors. The recipient of this Award has excelled based on one or more of the following criteria:

- Degree of differentiation innovation compared to other market participants
- Positive impact on sales directly related to product differentiation
- Time to market improvement based upon product differentiation strategy
- Benefit to end-users due to product differentiation
- Effect of product differentiation on ease of adaptability for new end-user applications
- Effect of product differentiation on market maturation

2007 GLOBAL FROST & SULLIVAN AWARD FOR PRODUCT DIFFERENTIATION INNOVATION

AWARD RECIPIENT: CODENOMICON LTD.



The 2007 Frost & Sullivan Product Differentiation Innovation Award is presented to Codenomicon

Ltd. (Codenomicon) for further extending the company's DEFENSICS security and robustness test platform. This black-box and negative testing solution is expected to have a major impact on the industry as it provides preemptive, pre-deployment security and robustness testing spanning IP, wireless, and digital media applications – and does so in a unique systematic, repeatable and rigorous method.

Codemicon, a leader in security and robustness testing, is headquartered in Oulu, Finland, with offices in Silicon Valley and Hong Kong. Founded in 2001, the company was born from the successful PROTOS test tools product and Oulu University Secure Programming Group research of the early 1990's. Codenomicon has been enhancing the platform for close to a decade and the current product is in its third generation.

The company's founders and research staff are highly regarded for their innovative approach to identifying known, and more importantly unknown, security and availability issues related to network, wireless and service application technologies. Outside of published analysis testing techniques dating back to the early 1980's, Codenomicon is widely recognized as the first company to create a new concept and deliver a programmatic security and resiliency test and analysis platform – Codenomicon DEFENSICS.

Years later, the world-proven Codenomicon DEFENSICS platform remains unmatched in its ability to find known and unknown quality, resiliency and security flaws within the broadest array of applications. The product complements quality assurance processes, secure programming initiatives and ISO security and risk management best practices.

Well over a hundred of large organization deployments and thousands of developers and security analysts across telecommunications, networking, manufacturing, financial services and defense industries rely on Codenomicon to reduce costly reputation, quality, compliance and liability risks.

Codemicon's customers are cross-industry heavyweights including Alcatel-Lucent, AT&T, Verizon, Cisco Systems, F5 Networks, Nordea, Nortel, Microsoft and Siemens AG among many others. These companies are using Codenomicon test platform to ensure that their products and services meet high quality and security standards.

Defensics: A Secure Innovation

Codemicon has an in-depth understanding of security testing at the infrastructure, protocol and network application protocol level. DEFENSICS goes beyond where security code and threat vulnerabilities scanners leave. The product is used within a quality assurance environment prior to release or in a staged test environment before a system or service is deployed – identifying exposures before liability and post-fix costs become significant.

The software offers a systematic blackbox and negative test methodology capable of revealing undesired behavior and issues in protocol implementation. Robustness describes how resilient a system under test is, given levels of testing which can expose flaws – flaws which can be exploited to result in zero-day or published threats. A published set of rules describing how to transmit and interpret/process data is commonly referred to as protocols. Organizations and vendors leverage open protocols, such as HTTPS, SSL, CIFS, to ensure interoperability and defined functionality.

Implementation risks are relative to the protocol’s newness, complexity, integration complexity and degree of change.

By offering a blackbox, negative test approach, DEFENSICS users can test systems, products and services without code-level knowledge – only having to know what protocols are under test. For example, a phone’s Bluetooth interface or a service’s secure connection interface can be tested without having knowledge of the underlying applications. This eliminates the need for expert resources and product expertise, defining additional test cases, and materially prolonging test processes. Test results can then be more efficiently provided to expert staff to resolve flaws, as well as validate fixes (prior to release or deployment).

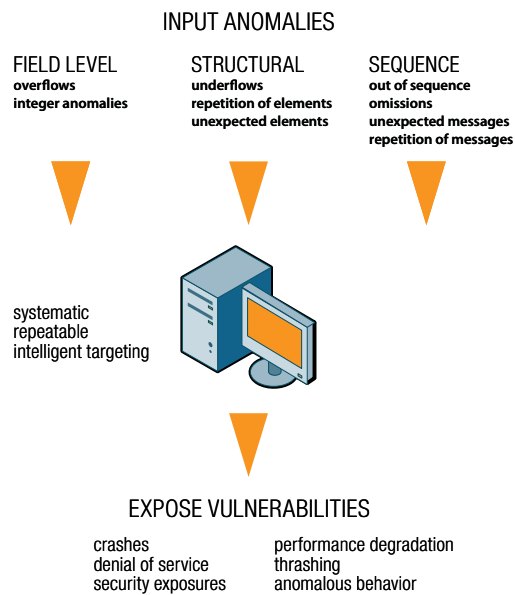
Inner Workings

The DEFENSICS security and robustness test software is the first of its kind to intelligently inject random data and sequences of data against application protocols to discover irregular responses, slower system reaction, or terminated functions across networked, wireless and media based systems – all of which can expose operational and security risks. This industry-first intelligence is derived by a systematic analysis of the protocol – not limited to mutating around known issues. By delivering random test input intelligently and systematically against a target protocol, users can more thoroughly and quickly identify flaws, failures and vulnerabilities as well as resolve issues with more assurance that can be repeatedly validated from the exact construct of a system under test.

By teaming Codenomicon’s patent-applied Protocol Modeling Engine and Attack Simulation Engine with the industry’s broadest protocol coverage, the company serves to ensure that users can more readily identify and understand known and zero-day vulnerabilities and availability risks associated with their products, services and networked infrastructure. Each protocol supported by Codenomicon DEFENSICS offers thousands of well-documented, modifiable test cases that yield volumes of programmatic test inputs.

Chart 1 highlights Codenomicon's DEFENSICS process to identify new and published threats and resiliency issues.

Chart 1: Codenomicon's DEFENSICS process to identify new and published threats and resiliency issues.



The platform is the only security and robustness solution that offers this type of security and robustness testing across three critical attack vectors: network, wireless, and digital media. DEFENSICS currently offers over 120 interfaces and formats packaged as suites or individual test sets, which allow extremely rigorous system testing from the link level to the application protocol level (new test and upgraded sets are introduced by the company on a monthly basis).

Chart 2 highlights Codenomicon's DEFENSICS breadth of network, wireless and media protocol support – the broadest in the industry.

To overcome the limits of appliance-based packaging, the DEFENSICS testing solution is software based to allow for more flexible licensing, greater distributed access, and easier integration into an organization’s existing testing environment. The solution offers flexible test interfaces that support a simple GUI, test parameter editing, comprehensive test documentation, a robust command line script,

as well as external system communication triggers such as the ability to remotely power-cycle systems under test. The DEFENSICS software runs on a variety of OS's and modest hardware.

Chart 2: Codenomicon's DEFENSICS breadth of network, wireless and media protocol support

DEFENSICS Core Internet	DEFENSICS Net Management	DEFENSICS Routing	DEFENSICS 3G	DEFENSICS Digital Media	DEFENSICS Email	DEFENSICS File Systems/Storage
IPv4 (TCP, UDP, IPv4, ICMP, IGMP, ARP), IPv6 (TCP, UDP, IPv6, ICMPv6), DNS (Server, Client, Zone Transfer), NTP (Client, Server), DHCP/BOOTP Client, DHCP/BOOTP Server, HTTP Server, HTTP Client, FTP Server, DHCPv6(Client,Server)	HTTP Server, HTTP Client, TLS/SSL Server, TLS/SSL Client, Taint Server, SSH1 Server, SSH2 Server, SNMPv1/v2 Server, SNMPv3 Server, TFTP Server, UPnP Server	IS-IS, DVMRP, GRE, OSPFv2, OSPFv3, PIM-SM/DM, RSVP, VRRP, BGP4, RIP, RIPvng, MPLS/LDP	SCTP, GRE, IPSec, Diameter Server, Diameter Client, LDAP Server, TLS/SSL Server, SIP UAS, SIP UAC, GTPv1, GTPv0, RADIUS (Server, Client)	A: AIFF, AU, AMR, IMY, MP3, VOC, WAV, BMP, GIF, JPEG, MBM, PCX, PNG, PIX, PNM, RAS, TIFF, WBMP, XBM, XPM, WMF V: AVI Quicktime, MOV, MPG1, MPG2 C: ZIP, CAB, JAR, LHA, GZIP	POP3 Client, POP3 Server, IMAP4 Client, IMAP4 Server, SMTP Client, SMTP Server	CIFS/SMB Server, iSCSI Server, SunRPC Server, NFS Server
DEFENSICS Remote Access	DEFENSICS VPN	DEFENSICS VoIP	DEFENSICS Bluetooth	DEFENSICS WLAN	DEFENSICS Link Management	DEFENSICS Industrial Automation
EAPOL Server, PPPoE, Diameter Server, Diameter Client, LDAPv3 Server, TACACS+ Server, TACACS+ NAS, RADIUS (Server, Client), Kerberos Server	IPSec, SSH1 Server, SSH2 Server, TLS/SSL Client, ISAKMP/IKEv1, IKEv2	SCTP, H.248, H.323, RTSP Server, TLS/SSL Server, TLS/SSL Client, SIP UAS, SIP UAC, SigComp, RTP/RTCP/SRTP, MGCP, UPnP Server	L2CAP, SDP, RFCOMM, OBEX, OPP, FTP, IrMC Synch, BIP, BPP, BNEP, HFP, HSP, DUN, PBAP, FAX, AVRCP, A2DP, HCRP, HID, SAP, HFP Client, HSP Client	802.11 Server, 802.11 Client	LACP, STP, MSTP, RSTP, ESTP	Modbus, TCP

Codenomicon Users; Satisfied and More Secure

Codenomicon markets its security and robustness solution directly and through international partners. Buyers of the DEFENSICS platform include quality assurance and security analysts across telecommunications, networking, manufacturing, software development, financial services and defense industries. As part of the research process, Frost & Sullivan interviewed customers in order to gauge relative product effectiveness, usability, implementation, advantages and value. These interviews reflect the decision factors leading up to the purchase of Codenomicon DEFENSICS and the benefits realized.

Leading Global Networking Equipment Manufacturer

Codenomicon has secured a good number of large network equipment manufacturers as customers – most in multiple divisions and a few enterprise-wide. The majority of these NEMs have conducted formal competitive and internal assessments prior to purchase. The main drivers were the means to extend quality assurance to reduce the cost and risks associated with zero-day attacks, security patches and post-fix issues. “No one wants to be a poster child at the next online hackfest regarding a potential threat naming your product.” The risk of reputation loss and incident response certainly plays a role in cost justification as bringing in Codenomicon as part of a best quality assurance practice.

Codenomicon clearly demonstrated that their product indeed captures potential flaws, which under different scenarios could pose future availability issues and security threats. In many cases, some departments had used the 1st generation freeware test solution PROTOS (these tools have not been updated for years) and were immediately able to observe the significant difference in the 3rd generation Codenomicon DEFENSICS platform. It is rare for any test target to walk away unscathed from DEFENSICS – and that is what quality assurance and testing is all about. The stable and extensible architecture of the Codenomicon test solution was among the business considerations in their purchase decision.

As a diverse and broad manufacturer, the fact that the solution is software-based, with no hardware dependencies (i.e. it can run on multiple platforms), offers immense value to the company. It facilitates company-wide deployment as a software tool that can be integrated into larger, remote test applications. This makes the product available to all product teams – avoiding extra travel and preparation costs. Given that Codenomicon’s blackbox solution is simple to use, customer do not need to employ code-level expertise - yielding more cost-conscious use of resources at different release stages. The ability to quickly implement it in engineering, security and quality assurance regression tests in multiple locations increases the effectiveness of the test teams.

The customer stated that the DEFENSICS solution is thorough and supports testing through each stage of development. Testers are able to escalate back to the development teams with regards to the issues being discovered. They avoid the situation where only part of the test resource has access to the tool. Also, since use is controlled, it avoids the possibility of an identified vulnerability being exported to a user with the possible risk of the vulnerability being exposed “in the wild”.

Both the test teams and engineers that have to fix identified bugs have access to all the built-in test documentation they need and the exact negative test scenario that generated the bug. This allows for a convenient, exact and efficient way to reproduce a bug – and avoids problems where the bug can only be reproduced under identical test environments (often an issue for externalized test applets). When problems are discovered in regression tests, the product yields significant documentation for engineers to reproduce the bug. Since the development engineers have access to the same tool, it is easy for them to reproduce it and fix it in a very prompt manner.

The scalability and flexibility of the solution was a strong advantage for Codenomicon in winning this customer over competition, but the company also appreciates the features and the integration capability of the product - as they are able to use their own implementation and verification functions. Other advantages of DEFENSICS over its competitors include the broad range and more thorough coverage of protocols. The customer had tested other tools that simply did not discover flaws, seem to require longer test cycles or did not generate a significant amount of test cycles. They discovered a common misinterpretation when comparing two tests against the same protocol – to not assume that the product that finished first is actually more rigorous than the slower module (it’s the breadth and number of test cases not just the total invalid test messages).

Other comparative factors were the system’s stability on test and concurrent support for multiple users, as well as the overall usability. Codenomicon DEFENSICS produces systematic testing and easy-to-interpret results. It offers a standardized way for this customer to utilize the reporting that comes out of the solution, which in most cases will become a part of a larger test report. While not containing flashy built-in charts and graphs, this user sees the output as more standard, detailed and flexible to incorporate the data needed by each department - enabling the company to put test results into its internal processes for tracking and presentation.

Finally, a number of alternative tools in the market require a training period that can take up to two weeks before users can be effective or in some cases requiring more code-level expertise. Codenomicon’s test solution is easy to learn without the need for formal training. Users can become productive with the tool quickly, simply by downloading the system and reviewing the built-in online documentation.

Codenomicon’s greatest strength is probably the fact that it can turn any non-security-oriented developer or test group into a security tiger team by giving them the right tools. And if the customer has questions and/or issues, Codenomicon’s support center will help. The company is very pleased with the response and quality of action provided by the support center. Overall, the customer would highly recommend Codenomicon as part of any organization’s quality assurance and risk reduction process.

Leading Global Telecommunications Provider

Various telecommunications and carrier organizations have opted to purchase and implement the DEFENSICS testing solution as a result of Codenomicon’s stellar reputation within the security testing industry. Such clients are quick to attribute Codenomicon’s status as a well-known, knowledgeable, and reliable supplier as a significant criterion in the formation of long-lasting partnerships. In DEFENSICS, customers are purchasing a test platform with vast capabilities in the efficient detection of vulnerabilities and flaws.

Working on a large project involving the rollout of over 200,000 routers, a leading Internet Service Provider (ISP) wanted to ensure the success of such an ambitious and expensive project in terms of

reducing risks toward availability and security. This customer was first drawn to Codenomicon as a result of its stellar reputation within the security testing industry, with how it discretely handled disclosure of security flaws and threats, and in particular of the positive feedback learned by current DEFENSICS customers and international users of the PROTOS freeware product.

As the company researched the marketplace, Codenomicon stood out for various reasons. First of all, the software-based solution is extremely convenient to the company, as it enables a more distributed use – even a tester can put it on a laptop when traveling. Also, unlike its competitors, Codenomicon offers all test configuration options in one easily-understood screen, which makes using the product more convenient and easy to describe to other test members. Ease-of-use, flexible implementation, strong test documentation and immediate regression testing were critical for the company because it has a number of test environments and large solutions with millions of customers on its network platform. Also, it is likely that in the future, even more departments in the organization will integrate the DEFENSICS test solution. Many of them may not be experts in security testing. Hence, it is of utmost importance that the solution be intuitive even for less-skilled users.

Another key reason that influenced their decision was the company's deep and wide protocol coverage. As the customer continued evaluating existing solutions in the market, they realized that the product available from other vendors were very limited in comparison to Codenomicon's. Not only is Codenomicon's solution completely protocol-aware, but it also efficiently analyzes more complex protocol implementations such as IPSec, OSPF, SIP and IPv6. Since the customer's main products and services involve a broad number of protocols, they needed a tool that is able to test each type of transaction and format of the protocol and keep up with emerging trends and RFCs/issues. This is among Codenomicon's competitive advantages.

The company also considered the testing capability of existing solutions in the market. Codenomicon's testing capability is very strong, enabling the company to perform over 40,000 test cases on the SIP protocol alone. Furthermore, the company considers the stability and test case visibility, when it comes to executing test cases and responding to potential flaws and bugs, extremely valuable. The tool allows the telecommunications customer to modify test parameters, obtain high level and detailed test results, and integrate DEFENSICS within a broader test harness.

Finally, the customer expected the supplier of their security and quality test solutions to be technically savvy, to be very responsive, and when needed, have expedited access to the technical staff as opposed to just second-level support experts. As a spin-off of Oulu University, Finland, Codenomicon fits the bill "to the T" as they have technical resources both in Europe, Asia and in the United States. These resources not only gain field expertise through custom professional service engagements (that are tied to security test verifications within client release of deployment cycles), but they are also involved in developing protocol test parameters and reviewing published threats on a daily basis.

To date, the telecommunications company has only used the solution for about a year, but the DEFENSICS platform has already delivered on its promises - exposing and helping to resolve numerous bugs in the first part of the project. The company is hence working with its suppliers and/or partners to have identified flaws fixed. Going forward, it expects Codenomicon to increase the value of the solution by adding case editing and enhanced reporting – all planned by Codenomicon within 2007. From a protocol coverage perspective, Codenomicon already covers more than 120 protocols and therefore it is difficult to identify additional protocols the company could cover – although the customer is impressed that Codenomicon has extended efforts in the wireless, digital media, network file system and applications arena.

CONCLUSION

Codemicon's objective is to ensure the security and robustness of any product or service implementation quickly and easily. Codenomicon DEFENSICS essentially closes the whitebox and VA/penetration test gap. The blackbox, negative testing approach reveals security threats and

operational weaknesses at post-production, which complements conventional whitebox solutions as they cover more programmatic threats. The Codenomicon solution can pinpoint exposures and facilitate fixing flaws up-stream where it is less expensive versus post-deployment vulnerability / penetration testing mechanisms.

Codenomicon's robustness testing platform offers a unique and powerful systematic blackbox, negative test methodology to identify and help resolve security issues and resiliency flaws which relate to published, new and unknown security threats. The company's DEFENSICS platform, based on its distinguished research heritage, platform depth and capabilities, is expected to have a major impact on the industry, and as such was awarded the 2007 Frost & Sullivan Product Differentiation Innovation Award. By teaming Codenomicon's patent-applied Protocol Modeling Engine and Attack Simulation Engine with the industry's broadest protocol coverage, the DEFENSICS solution demonstrated the ability to develop and/or advance products with more innovative capabilities than competing vendors and products.

Codenomicon DEFENSICS security and robustness test platform and application protocol suites provide a thorough and efficient methodology for developers, IT, security and business unit owners to reduce risks and increase quality – with nominal impact on resources and delivery / deployment schedule. The product complements quality assurance processes, secure programming initiatives and ISO security and risk management best practices.

It allows carriers, network equipment vendors, software product engineers and security analysts to probe the deepest architecture levels during the earliest stages of the development cycle in order to resolve the largest number of problems possible. The approach also allows software developers, corporate enterprises and government agencies to mitigate or avoid the very real costs associated with increased development demands, software upgrades, product recalls, brand damage, service interruptions, and legal exposure due to security breaches.

The testing platform was designed and developed with a high degree of innovation to address growing attack vectors and availability exposures that end user products and corporate services face within today's networked and converging service-oriented market. Codenomicon DEFENSICS' purchase criteria, implementation and value have been validated by leading, well-recognized brand name customers and through direct interviews during the course of Frost & Sullivan's research process.

The DEFENSICS solution is highly flexible, easy to use, shortens testing time, alleviates piecemeal tool compilations, and improves time to market for both corporate applications and end-user products. This powerful and easy to implement platform makes the DEFENSICS solution an obvious preference for testing systems and components.

With Codenomicon DEFENSICS, customers are realizing material cost savings, greater quality assurance, as well as reduced risk and liability. All the aforementioned factors make Codenomicon a worthy recipient of the 2007 Frost & Sullivan Product Differentiation Innovation Award in the world security test equipment industry – and a worthy test partner for vendors, developers and enterprises.

ABOUT BEST PRACTICES RESEARCH

Frost & Sullivan Best Practices Awards recognize companies in a variety of regional and global markets for demonstrating outstanding achievement and superior performance in areas such as leadership, technological innovation, customer service, and strategic product development. Industry analysts compare market participants and measure performance through in-depth interviews, analysis, and extensive secondary research in order to identify best practices in the industry.

ABOUT FROST & SULLIVAN

Frost & Sullivan, a global growth consulting company, has been partnering with clients to support the development of innovative strategies for more than 40 years. The company's industry expertise integrates growth consulting, growth partnership services and corporate management training to identify and develop opportunities. Frost & Sullivan serves an extensive clientele that includes Global 1000 companies, emerging companies, and the investment community, by providing comprehensive industry coverage that reflects a unique global perspective and combines ongoing analysis of markets, technologies, econometrics, and demographics. For more information, visit <http://www.frost.com>.

877.GoFrost

myfrost@frost.com

<http://www.frost.com>