FROST & SULLIVAN

2015

silent circle

2015 Global Privacy-Enabled Smartphones New Product Innovation Award

Contents

Background and Company Performance

Industry Challenges

With the growth of mobile computing platforms and next generation networks in the Information Age, digital information is now collected, processed, and disseminated faster than any time in history. Personal, private, and corporate information alike can be captured (directly or indirectly) during digital interactions, and users often do not realize the severity of sensitive information being compromised until it actually causes damage, which often is too late. While the desire for reasonable expectation of privacy is nothing new in human society, the rate and complexity at which private information is now being collected and exploited by third party entities can be frightening.

While there are legitimate scenarios in which anonymized user data is collected and used for targeted advertising campaigns in order to justify free or deeply discounted consumer services, the need for enterprise platforms that deliver secure mobile communications with centralized management controls continues to grow among global businesses and governments. The potential for exposure of improperly implemented mechanisms to intentionally bypass security—including lawful interception management systems (LIMS), such as Stingrays—via inadvertent exposure or nefarious exploitation of private communications, confidential corporate information, and intellectual property, can cause cataclysmic damage to a company's image and business operations.

Enterprises understand the value of mobility in the workplace, but they cannot simply ignore the risks. IT managers demand solutions which give them more control over the permissions, features, and apps that directly impact their network security. However, it is impractical for developers, content providers, and telecommunications companies to decide what an acceptable level of privacy for a diverse user base should be. Under the current privacy climate and rapid rate of software innovation, there is an unsatisfied market for secure smartphones that are as flexible as possible while purposely built with security in mind. Frost & Sullivan calls this the privacy-enabled smartphone market.

Privacy-enabled smartphones are phones that allow IT managers and users to enjoy all the benefits of a regular consumer smartphone and associated ecosystem benefits—such as popular apps, near field communication (NFC) payments, social media integration, and GPS—but with an emphasis on practical security controls that do not affect functionality or force the user to drastically alter their behavior. As a result, smartphone users can safely communicate sensitive confidential information while enjoying all the popular apps and maintaining the functionality that users still want on their mobile devices while also complying with enterprise mobile device management (MDM) policies.

Frost & Sullivan has observed a significant increase in both sophistication and frequency in which cyber criminals target, exploit, and monetize off of attacking large enterprises and their data. While considering the increase in high-performing information systems and cyber-criminal activity, combined with lackadaisical app design, privacy is potentially at the highest risk in all of human history. Now the rapid expansion of big data analytics and monetization of metadata raises concerns for many. While strict security policies help, sometimes simple security hygiene on the users end will suffice. Instead of trusting the developers, content providers, and network infrastructure maintainers, enterprises now must seek the ability to control the amount of private information they share.

Significant challenges that negatively impact enterprise IT managers decision to allow mobile devices in the workplace are:

- Leaky apps: Either through careless design or intentionally built to facilitate personalized advertisement platforms, apps emit all kinds of exploitable information that may place the enterprise's confidentiality at increased risk.
- Zero-sum permissions doctrine: While allowing users to enjoy an immense selection of apps on their storefront, standard Android apps require the user to either accept all the potentially invasive app permissions, or not use the app at all.
- Political agendas: Cyber criminals are typically motivated by financial gain to exploit network vulnerabilities and enterprise data, which is logic based. There is an alarming amount of illogical attacks where the main motivation is political, and employed to embarrass, shame, and/or harm the target—such as doxing. These types of attacks tend to focus on exploitation of confidentiality.
- Expectation of publicity: There is a disturbing trend of privacy being either completely disabled by default or if enabled, minimal at best, exposing the user to unnecessary risk. Users may "willingly" share private data without knowing it or how that information is used—i.e. data mining.
- Security-as-a-disservice: In decisions that pit security versus convenience, profit, or performance, security tends to lose. Generally speaking, security seems to be an afterthought in seemingly harmless apps and leads skeptical enterprise IT managers to disallowing the application or mobile device altogether.

New Product Attributes and Customer Impact of Silent Circle

Silent Circle is a Switzerland-based encrypted communications company that offers the Blackphone product line—Silent Circle's privacy-focused smartphone. The most recent iteration—the Blackphone 2—received various accolades when it launched in September 2015. Privacy-enabled smartphones are the answer for users who want more control of what information is on their smartphone, how it is used, where that information goes, and who can see it. While becoming a certified Google for Work partner, Silent Circle and its Blackphone 2 represent a much needed paradigm shift towards restoring control of how devices handle their private information, and addresses the enterprise confidentiality problem: it builds on the inherent security advantages of mobile, while giving enterprises the ability to keep critical information and work products separate from employees' personal apps, services, and data on one device. Silent Circle is a premium partner of Google in regards to Android device security and enterprise-friendly features, setting a new standard for how smartphones should address privacy in both the enterprise and consumer markets, while retaining the strongly desired ecosystem of Android devices.

Match to Needs: Making the Market

While ultra-secure hardened communications is a well-established market, the technology, burden to user productivity, and security doctrine required to maintain that heightened level of security makes the devices extremely restrictive by nature. This is ideal for government agents and security forces whose lives depend on a no compromise military-grade solution, but does not meet the functionality requirements of enterprise markets who wish to leverage the productivity solutions in the Android ecosystem.

The majority of smartphones are designed to optimize convenience at the specific cost of privacy, so that this task is not an easy one for even a tech savvy user. Similarly, vetting various third party apps and security features can become quite cumbersome. This becomes even more problematic on the enterprise scale, where companies must balance end-point management policies and the productivity benefit of implementing Android devices into the workplace.

This also offers an opportunity to move away from the "bolt-on security" approach of desktop-focused productivity, and embrace the significant security advantages of a mobile working environment for a corporate IT structure. Silent Circle realized the market demand for a privacy-enabled smartphone and captured it. Silent Circle's Enterprise Privacy Platform is protected with a native 256-bit symmetric encryption and a bespoke 414-bit elliptic curve—"Curve41417." This is being submitted for international standard by its designers, Daniel Bernstein and Tanja Lange.

Silent Circle's Silent OS lets Blackphone 2 users enjoy the immensely popular and flexible platform of the Android smartphone with minimally obstructing security, focusing instead on privacy by design. The company's Silent Store features privacy-focused apps that have been reviewed by Silent Circle for privacy and security best practices. Apps are verified for Android signing and privacy claims, and placed through a static analysis process for malware detection before appearing in the store. The Blackphone 2 can access the Google Play app store so users can still access popular apps and take full advantage of the Android app ecosystem.

Applications that run on Silent OS are subject to control via the Blackphone 2 Security Center. The amount of permissions that some apps require can be invasive. Instead of placing an ultimatum between a user and their Clash of Clans or other favorite app, the Blackphone 2's native permissions manager allows the user to decide which permissions to allow. This gives users fine-grain control over app permissions such as location, camera, or contact access. Blackphone 2-recommended settings are applied to newly installed apps by default, and users can customize permissions from there. This is a feature that was previously absent on Android devices, and was not implemented until the release of the

Marshmallow 6.0 update. The Blackphone series offers Spaces, which lets the user compartmentalize their Blackphone 2 into multiple virtual workspaces. Spaces gives companies a way to let employees carry multiple “phones” on one device. By creating a managed Space for work apps and data, companies can remain confident in the security and privacy of their work information and product, while giving employees the flexibility of a smartphone that can maintain a separate Space for personal use. This also makes it easy to “quarantine” suspicious apps in a Space that does not have access to more important data on the phone.

As with individual apps, the permissions granted to individual Spaces can also be managed from the Blackphone 2 Security Center. Users can create Spaces that lack network or location access, for example, or set up a Space so that phone calls can’t be placed from it. This also makes it possible to test third party apps while minimizing the risk from installing malware or potentially unwanted applications (PUAs) that could compromise other data on the phone.

Every unique feature of the Blackphone 2 promotes enterprise confidentiality from the ground up, rather than security after the fact, or convenience at the cost of privacy. This clearly differentiates Silent Circle from its competitors in the secure mobile device market, and gives companies a clear path to privacy as a combination of security and policy. Competitors in this market implement much stricter features and restrict third party apps to address specific needs in the vertical markets, while the Blackphone 2 focuses on practicality and leaving those decisions to the user and organizational IT manager. While app providers require the user to accept all permissions to use the app, Blackphone 2 natively allows granular control of permissions.

Silent Circle addresses the overwhelming industry challenges to privacy and has created this niche in the market out of customer need for functionality, practicality, and control.

Pioneering Practicality: Design, Reliability, and Quality

Silent Circle designs powerful features that directly impact privacy control. These features were developed with the idea of choice and control from the start, rather than outright restriction and policy enforcement. This allows for a more practical implementation of privacy as a combination of security and policy, that does not adversely affect employee productivity or burden user behavior. As an enterprise solution, the Blackphone 2’s practicality while being able to facilitate MDM makes it an ideal BYOD option for professionals who need mobile productivity and nonintrusive security. Frost & Sullivan research has observed that when enterprises enforce stricter security doctrines upon their employees, an alarming amount of them willfully neglect, defeat, or workaround security mechanisms to maintain productivity. The Blackphone 2 addresses this problem by giving users access to their own Space on the phone, while letting employers manage work-specific Spaces with the Security Center.

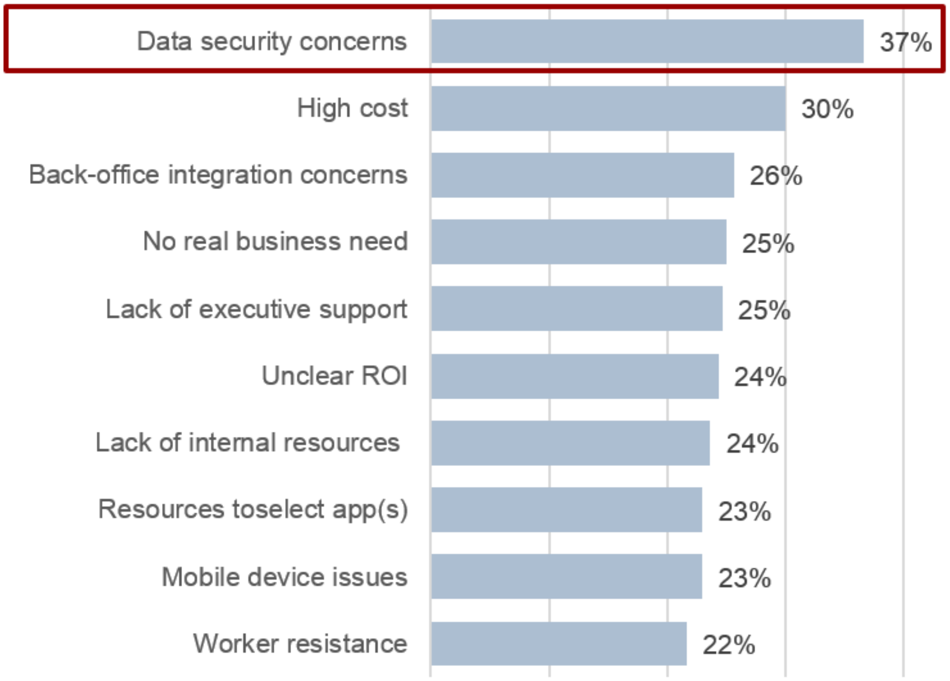
Silent Circle's recently released Enterprise Privacy Platform (EPP) provides businesses with a variety of enhanced cloud-based software and service capabilities. The EPP platform enables secure communications with innovative enterprise management controls for general oversight and auditing. A new feature of the EPP platform is Silent Manager which provides a web-based management interface for administrators to efficiently monitor/manage the Silent Circle platform and add/remove users. Active Directory Single Sign-On and LDAP integration are now included in Silent Manager.

The Blackphone 2 works best when users communicate through Blackphones, as this provides the highest level of security from man-in-the-middle (MitM) attacks. However, non-Blackphone communicants may still use the Silent Phone app—which is available for iOS and Android—to maintain Silent Circle's secure communications technology on non-Silent OS devices. The Silent Phone app has recently been re-engineered to include enterprise-specific features, as well as peer-to-peer encrypted calling, video, text and file transfers. The Silent Phone app is available in two subscription levels – basic and plus.

Silent World is another feature within Silent Phone. Silent World is a new type of calling capability that allows users to call anywhere in the world from within the silent phone app. It creates flexibility, as users can call any land line or mobile in the world, and generates cost savings by eliminating roaming charges. Silent World has expanded to include 439 destinations. Secure video and conference calling is available, as well as Silent Phone telephone numbers which allow each user to have two different phone numbers (virtual dual SIM) on the same mobile phone.

The Blackphone 2 seamlessly integrates with Citrix, Good Technologies, and SOTI MDM systems. It offers privacy that protects the enterprises from eavesdropping and offers enough practicality that makes it easier forenterprise employees and IT managers to comply with acceptable use policies. Finally, Silent OS also includes a built-in Remote Wipe feature, so that the phone's contents can be deleted remotely in the case of loss or theft.

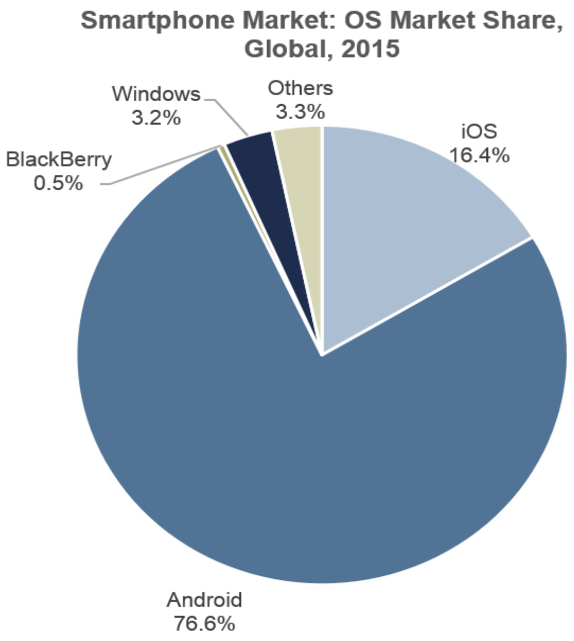
Reasons Against Providing Mobile Apps to Employees-Percent Very Important: NA, 2015



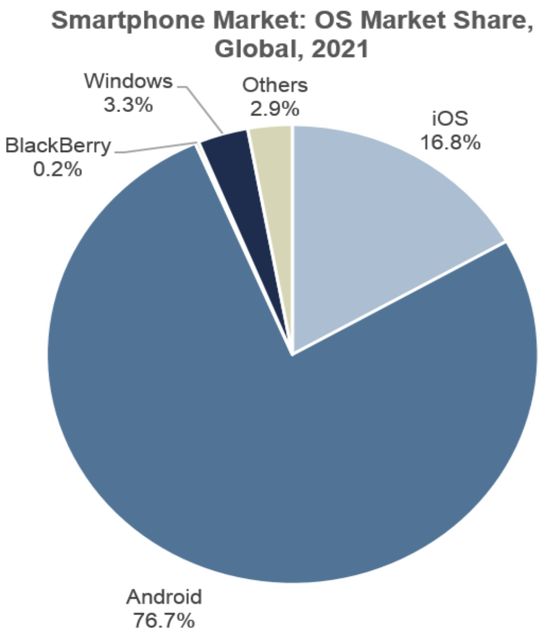
Performance Value: Security Investment that Redefines the Standard

Frost & Sullivan research conducted in 2014 for Android security trends illustrates that 23% of Android apps scanned between March and August of 2013 were malicious in nature; the majority being PUAs. Employees at various organizations also express the desire to use their own devices for workplace productivity. While this alleviates the capital expense for the enterprise, the security implications for IT managers draws ire. Nonetheless, Frost & Sullivan observes that organizations are increasingly embracing BYOD initiatives into their workplaces, however, data security remains the primary concern against mobile application adoption by enterprises.

The trend for employees seeking to use personal smartphones to access sensitive corporate data and networks is not expected to abate, as Frost & Sullivan projects that more than three-quarters of organizations will have BYOD activity on their networks over the next three years. With the smartphone marketplace being led by the Android OS at the close of 2014, the bottom line here is that Android devices are penetrating the workplace and corporate network. A Frost & Sullivan smartphone study titled "Global Smartphone & Mobile OS Markets" in December 2015, has reinforced the belief that the Android smartphones will continue to lead the market through 2021.



Smartphone Market: OS Market Share, Global, 2015



Smartphone Market: OS Market Share, Global, 2021

In February 2015, $1 billion was stolen by multinational cyber criminals over 100 banks, in 30 countries, over the course of two years[1]. Investing in security is no longer just a luxury. However, investing wisely in security practices that have the minimalist of impact on user behavior and productivity is critical to earning the maximum return on security investment. With Silent Circle's Blackphone 2 open and secure by design solution, it is the smartphone that average users would actually want to use. Blackphone 2 alleviates the need to sacrifice functionality for security and gives the user control of both.

Customer Ownership: Mobility for the Modern Market

Silent Circle aims to release over-the-air patches to reported vulnerabilities within 72 hours. This is a significant differentiator, as traditional vulnerability patches by Google are only released in the monthly patch. These patches can still become further delayed depending on the device manufacturer's turnaround. During this time the device user is left exposed to such vulnerabilities that are now publically known. By comparison, Silent Circle issues patches in response to major vulnerabilities much faster, and through its Android for Work partnership, works with Google as a subject matter expert on vulnerabilities and how best to address them. Once the phone is set to a level of security that the user is comfortable with, it really is just as robust as other phones.

[1] Reuters *Cybercrime ring steals up to $1 billion from banks: Kaspersky*: http://www.reuters.com/article/2015/02/15/us-cybersecurity-banks-idUSKBN0LJ02E20150215

Positioning: A Paradigm Shift in Privacy Philosophy

Different users have different needs, expectations, and concerns regarding privacy on their smartphones, making it impossible to implement a practical one-size-fits-all doctrine. The Blackphone 2 lets users make such decisions for themselves, while giving companies control over work-specific data and apps. By taking this approach, the company essentially positions Silent Circle in a league of its own in the smartphone industry via its novel architecture and continually developing portfolio focusing on privacy without compromising smartphone functionality. The Blackphone 2 is currently marketed as an enterprise smartphone solution. Silent Circle's VoIP network infrastructure is based in Geneva, Switzerland, and provides its service to an audience that is already well aware of the benefits of privacy while encouraging progressive concepts, such as the "Right to be Forgotten" throughout the European Union.

By introducing a competitively priced, functionally secure, enterprise-ready smartphone into regions with developing markets, Silent Circle is further positioned for explosive growth. The Blackphone 2 is capable of fully leveraging TCP/IP protocols to provide consistent and secure voice and text-based communications over underdeveloped metro-networks that still depend on legacy equipment and may have considerable 3G and 4G coverage gaps. Frost & Sullivan coverage of the South American telecommunications industry consistently shows both the prevailing trends of TCI/IP-based communication over traditional public switched telephone network (PSTN) services, and explosive growth in the tech industry. Silent Circle has chosen wisely to position itself in a market with such potential with an ideal solution that can function with or without use of a subscriber identification module, or SIM card, which is required to access a carrier's telephone network.

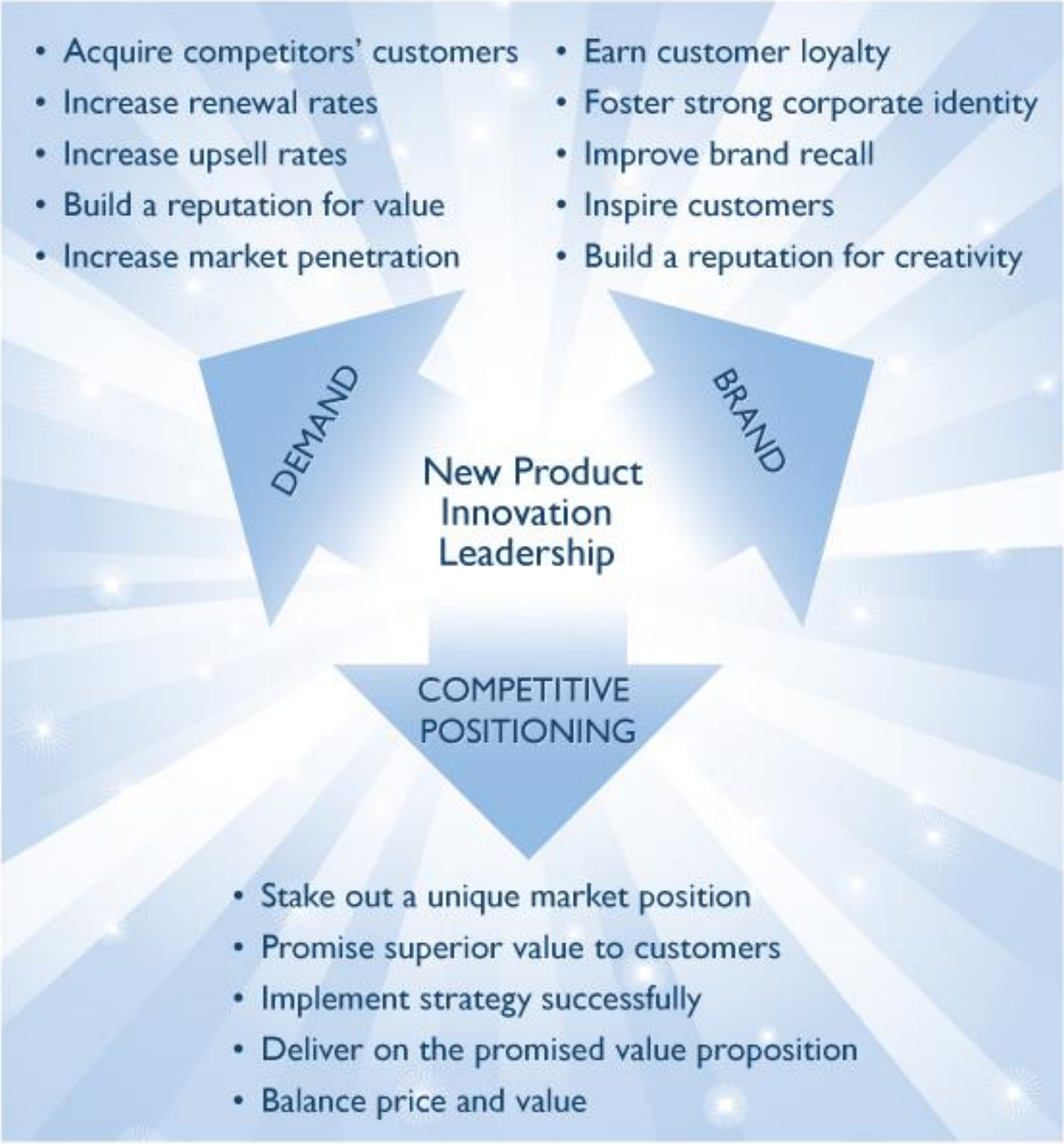
Conclusion

With the introduction of the Blackphone 2 into the smartphone arena, Silent Circle is capitalizing on a long embattled and unaddressed market of enterprise privacy. Whether for enterprise or personal use—or with the Blackphone 2, both—communicants no longer have to leave their trust in carriers, phone manufacturers, or application developers, whose focus is convenience rather than privacy. Silent Circle lets the user decide what level of privacy they want instead confining them to a one-size-fits-all compromise. Silent Circle has made a market for itself by emphasizing security with retained functionality, establishing a new set of best practices for all Android smartphone manufacturers to follow.

Because of its strong customer loyalty, tactical approach to an underserved and oft manipulated market, Frost & Sullivan recognizes Silent Circle with its 2015 Global New Product Innovation Award in the now defined privacy-enabled smartphone market.

Significance of New Product Innovation

Ultimately, growth in any organization depends upon continually introducing new products to the market, and successfully commercializing those products. For these dual goals to occur, a company must be best-in-class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition.



- Acquire competitors' customers
- Increase renewal rates
- Increase upsell rates
- Build a reputation for value
- Increase market penetration

- Earn customer loyalty
- Foster strong corporate identity
- Improve brand recall
- Inspire customers
- Build a reputation for creativity

- Stake out a unique market position
- Promise superior value to customers
- Implement strategy successfully
- Deliver on the promised value proposition
- Balance price and value

Understanding New Product Innovation

Innovation is about finding a productive outlet for creativity—for consistently translating ideas into high quality products that have a profound impact on the customer.

Key Benchmarking Criteria

For the New Product Innovation Award, Frost & Sullivan analysts independently evaluated two key factors— New Product Attributes and Customer Impact—according to the criteria identified below.

New Product Attributes

Criterion 1: Match to Needs
Criterion 2: Reliability
Criterion 3: Quality
Criterion 4: Positioning
Criterion 5: Design

Customer Impact

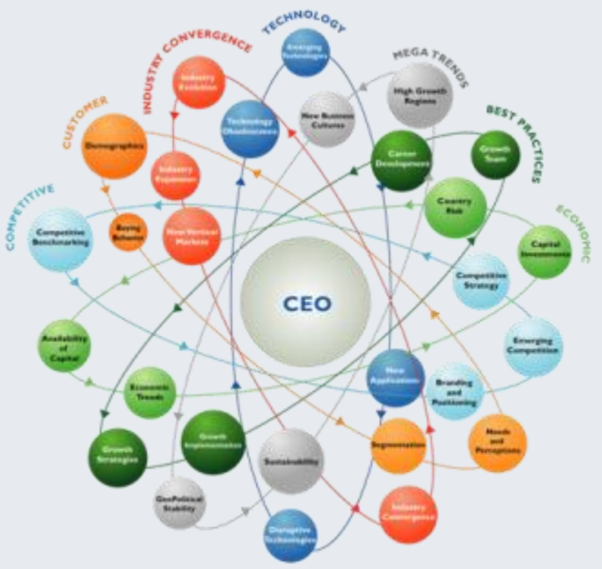
Criterion 1: Price/Performance Value
Criterion 2: Customer Purchase Experience
Criterion 3: Customer Ownership Experience
Criterion 4: Customer Service Experience
Criterion 5: Brand Equity

The Intersection between 360-Degree Research and Best Practices Awards

Research Methodology

Frost & Sullivan's 360-degree research methodology represents the analytical rigor of our research process. It offers a 360-degree-view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan's research methodologies. Too often, companies make important growth decisions based on a narrow understanding of their environment, leading to errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry players and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS



Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

Frost & Sullivan Awards follow a 10-step process to evaluate award candidates and assess their fit with select best practice criteria. The reputation and integrity of the Awards are based on close adherence to this process.

STEP		OBJECTIVE	KEY ACTIVITIES	OUTPUT
1	**Monitor, target, and screen**	Identify award recipient candidates from around the globe	Conduct in-depth industry research Identify emerging sectors Scan multiple geographies	Pipeline of candidates who potentially meet all best-practice criteria
2	**Perform 360-degree research**	Perform comprehensive, 360-degree research on all candidates in the pipeline	Interview thought leaders and industry practitioners Assess candidates' fit with best-practice criteria Rank all candidates	Matrix positioning all candidates' performance relative to one another
3	**Invite thought leadership in best practices**	Perform in-depth examination of all candidates	Confirm best-practice criteria Examine eligibility of all candidates Identify any information gaps	Detailed profiles of all ranked candidates
4	**Initiate research director review**	Conduct an unbiased evaluation of all candidate profiles	Brainstorm ranking options Invite multiple perspectives on candidates' performance Update candidate profiles	Final prioritization of all eligible candidates and companion best-practice positioning paper
5	**Assemble panel of industry experts**	Present findings to an expert panel of industry thought leaders	Share findings Strengthen cases for candidate eligibility Prioritize candidates	Refined list of prioritized award candidates
6	**Conduct global industry review**	Build consensus on award candidates' eligibility	Hold global team meeting to review all candidates Pressure-test fit with criteria Confirm inclusion of all eligible candidates	Final list of eligible award candidates, representing success stories worldwide
7	**Perform quality check**	Develop official award consideration materials	Perform final performance benchmarking activities Write nominations Perform quality review	High-quality, accurate, and creative presentation of nominees' successes
8	**Reconnect with panel of industry experts**	Finalize the selection of the best-practice award recipient	Review analysis with panel Build consensus Select winner	Decision on which company performs best against all best-practice criteria
9	**Communicate recognition**	Inform award recipient of award recognition	Present award to the CEO Inspire the organization for continued success Celebrate the recipient's performance	Announcement of award and plan for how recipient can use the award to enhance the brand
10	**Take strategic action**	Upon licensing, company may share award news with stakeholders and customers	Coordinate media outreach Design a marketing plan Assess award's role in future strategic planning	Widespread awareness of recipient's award status among investors, media personnel, and employees

About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best in class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages almost 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from 31 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.