2016 Global Network Access Control Market Leadership Award

Contents

Background and Company Performance

Industry Challenges

Networks come in different sizes and in many different varieties. The network of today often includes Wi-Fi access, bring-your-own devices (BYOD), and access to public and private clouds.

Traditional cyber defenses include firewall, advanced threat detection (ATD), antivirus (AV), vulnerability management (VM), security information and event management (SIEM), mobile device management (MDM), among others. Each defense offers some deterrence, but the modern cyber defense posture is challenged to meet the sophistication of the new attacker. When these types of technologies are implemented as security "silos," the potential breach environment becomes much more inviting.

One of the foundational defenses in today's networks is network access control (NAC). NAC began as a highly structured technology that was used primarily to help determine network access and establish access control for managed devices. NAC vendors are quick to mention the technology is evolving to protect new network architectures. The leading NAC vendors (including Cisco) prefer the term next generation NAC, offering four essential network protection benefits:

1. **Endpoint visibility.** The next generation NAC offers endpoint and network infrastructure visibility. The NAC provides unique visibility in that it ingests data after traffic has passed perimeter defenses, but before data is homogenized for indexing in the SIEM. Visibility becomes knowledge; next generation NAC platforms can use network protocols to discover devices on the network. The NAC helps to enforce endpoint compliance, and is often used to gain crucial information about endpoints on the network including configuration assessment about corporate assets, specialized devices, their location and the security posture of endpoints.

2. **Bidirectional communication with IT and security platforms.** Next generation NAC platforms are often integrated with an IT/security platform through an API or sometimes more tightly integrated in a formal module. If the integration is successful, NAC integrates with firewalls, advanced threat detection (ATD), vulnerability management (VM), SIEM, mobile device management (MDM), and other platforms, improving the efficacy of both NAC and the integrated platforms and allowing these platforms to trigger NAC defense actions.

3. **Contextual awareness.** With true endpoint visibility and improved posture assessment, NAC adds "context" to controls. IT Directors can establish very granular policy; can build risk management onto NAC; quiet the number of alerts; and anticipate potential weaknesses in the network through posture assessment and visibility into configurations.

4. **Network orchestration**. Network orchestration is endpoint visibility, bidirectional communication, and contextual awareness in evidence. The next generation NAC can be the central console of IT and Security operations. The bidirectional

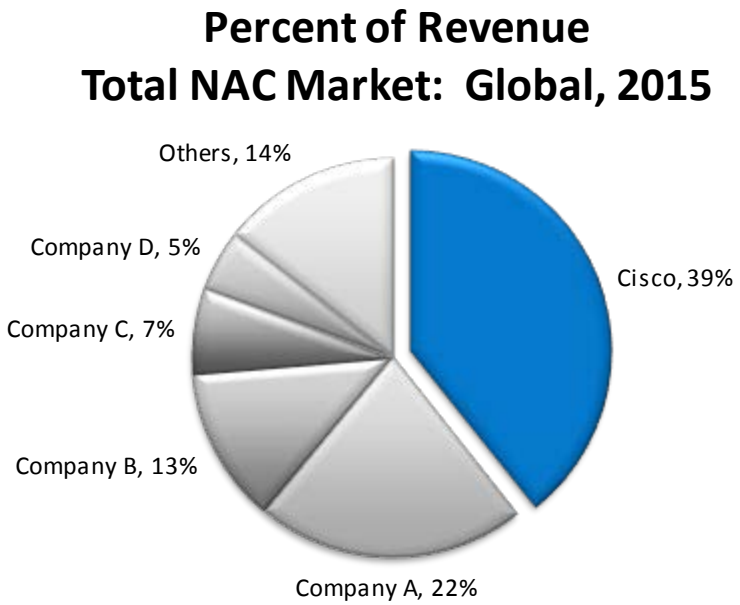
communication with other cyber defense platforms fortifies the efficacy of these tools, and, in turn, firewall/VM/etc. data can be used to improve access controls. One cool function of the NAC is it can be used as a single, central deployment point to push new applications, patches, agents, software, and operating systems (OS) upgrades from the network onto endpoints.

The next generation NAC is a necessarily technically elegant solution. Successful NAC platforms will help to reduce the time it takes to add endpoints onto the network, and largely automate access controls. Network orchestration has to be done without adding latencies onto the network, applications, or to the performance of the end user's device. NAC processes (analytics, access controls, and authentication) have to be transparent to the end user.

Market Leadership

Frost & Sullivan began charting market share for NAC vendors in 2010, and Cisco was then, and remains the revenue market leader.

In cyber security technologies, market leadership is gained when technologists develop and market software platforms that address a specific need. (Colloquially, that would be the first guys to market with a good idea). Market leadership is maintained when an incumbent leader adapts its platforms to meet with new security conditions, rises to the challenges of competing vendors in terms of technology implementations and pricing, and continues to develop its products to meet with the IT and security protocols used by its customers.



This Best Practice analysis explains how Cisco achieved and maintains its NAC market leadership.

Brand Strength

The next generation NAC market has several strong contenders attempting to supplant Cisco from its NAC market share throne, but Cisco has several key advantages moving forward.

- **First mover.** In 1992, Cisco introduced Cisco ACS which addressed access control. The term "network access control" comes from Remote Authentication Dial-In User Service (RADIUS) architecture. A generation of IT and security professionals have worked with Cisco NAC.

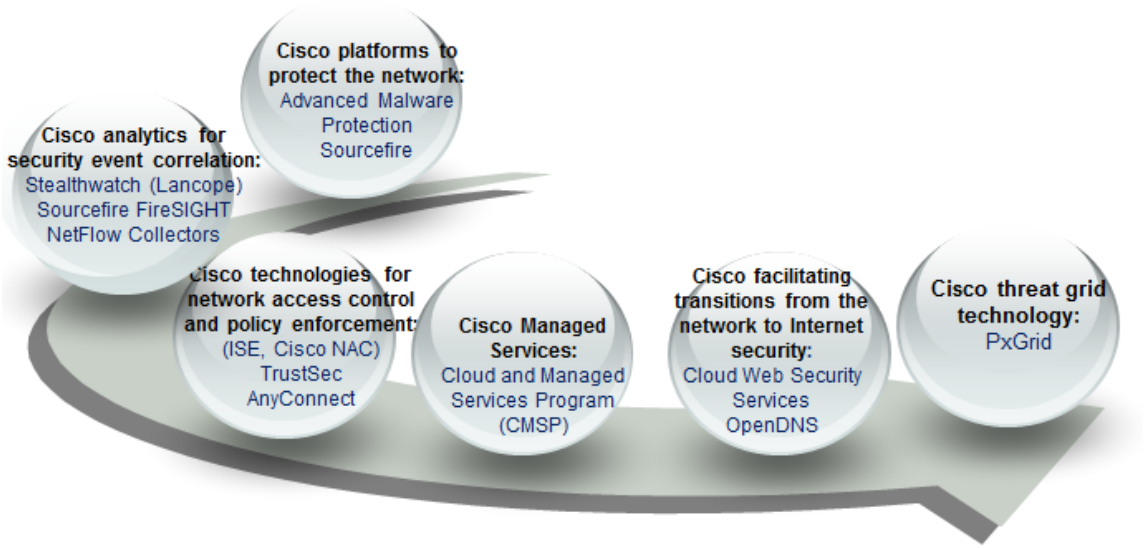
- **Support for industry consortia.** Cisco has been a strong contributor to Institute of Electrical and Electronics Engineers (IEEE) 802.1 and IEEE 802.3 standards which are the working groups that create the internationally accepted standards for local area and wide area network traffic management (LAN/WAN) and MAC layer and Ethernet switching rules and security respectively.

- **Expertise.** The Internet is thought to be an ephemeral technology, when in fact, the Internet represents the best in engineering and in hardware. Cisco routers and Ethernet switches guide traffic on the Internet. While Cisco largely powers the point-to-point connections on the Internet, it stands to reason that Cisco has considered what is required to make for efficient individual enterprise networks. Cisco becomes a trusted authority on network architecture and platform installations.

- **Integrated security platform**. From a high-conceptual level, network security can mean managed services, secure point-to-point communications, strong firewalls and intrusion detection and prevention systems, malware detection, network orchestration, and crowdsource sharing of information between enterprise networks, government agencies, and the knowledge gained from network security platforms—Cisco has current products and roadmaps forward in all of the above.

The graphical representation of Cisco security technologies on the right side is representative, but not comprehensive. Additionally, because Cisco uses standards-based technologies, further integration with third-party IT and security technologies is possible, meaning that Cisco technologies can be used to enable or enhance any type on network security technology including (data loss protection, behavioral analytics, file management, etc.).

Cisco Security Platforms and Approaches



Source: Cisco and Frost & Sullivan.

In terms of network security, Cisco Identity Service Engine (ISE) NAC is the 802.1X; RADIUS based NAC platform used to bring end users (devices) onto a network securely, enforce endpoint compliance, coordinate security appliances, and provide contextual awareness to proactively find Indicators of Compromise (IOC), or to help facilitate a post-breach forensics investigation.

Implementation Excellence

As mentioned, the Cisco ISE NAC platform is fundamentally an 802.1X, RADIUS technology based platform.[1]The platform is used in pre- and post-admission NAC controls. In a network, rogue devices are a concern. To mitigate the on-boarding of rogue devices onto a network, Cisco uses a proprietary technology to associate an endpoint with the right server in the network preventing race conditions. Cisco ISE ensures a tie-together of RADIUS authentication and Transport Layer Security (TLS) communication to ensure all devices are policy compliant before they can access the network. In non 802.1X NAC deployments, endpoints are often dynamically discovered using network protocols like Simple Network Management Protocol (SNMP) or Windows Management Instrumentation (WMI). From a visibility and discovery standpoint, these protocols are fine. However, the NAC will let the device onto the network before authentication takes place. If at a later time, the device is determined to be rogue (or perhaps does not meet endpoint

[1] The majority of Cisco ISE deployments use the 802.1X protocol. For devices that don't support 802.1X, Cisco Catalyst switches can be configured to attempt WebAuth or MAB to place endpoints on the network using ISE guest, BYOD, or secure IoT access on-boarding and management applications. After a device and/or user have been authenticated, ISE pushes the appropriate access control list (ACL), VLAN or security group tag (SGT) to the switch. A change of authorization command is issued via RADIUS to provide access to the endpoint. In total, Cisco ISE supports attributes across six different probes (HTTP, SNMP, DHCP/DNS, NMAP, NetFlow, as well as RADIUS) for endpoint discovery, profile feed, and continuous monitoring.

compliance criterion), the NAC will have to kick the device off of the network post-connection.

Cisco ISE includes a TrustSec software-defined segmentation work center. TrustSec allows the IT administrator/security team to create granular policies to define access control and allowed protocols between security groups in a policy grid. These policies are defined in software and communicated to relevant network devices to enforce the segmentation and access control policies regardless of the point of access, topology, or existing VLANs.

Access control and endpoint enforcement policy can be labor-intensive processes. Secure device/end user on-boarding is problematic. Listed below are a few techniques facilitated by Cisco ISE, TrustSec, and AnyConnect technologies to make admissions and access control easier for the IT/security teams:

- **Network segmentation.** In ISE, endpoints are segmented either by VLANs, ACLS or TrustSec software-defined segmentation. However, network segmentation can be a fluid event. A change in the profile of a device or endpoint posture assessment, a security incident detected by a third-party platform, or an endpoint falling out of compliance, can prompt a change to the access privileges assigned to the endpoint.

- **Business Policy Enforcement.** Business policy enforcement provides a direct connection between a network entity (user, endpoint, or IoT thing) and their business role through a rule-based, attribute-driven policy model.

- **Directory services for managed devices.** ISE can connect directly to Microsoft Active Directory, Novell e-Directory, Open Lightweight Directory Access Protocol (LDAP), Sun LDAP, and RSA directory services natively. For other identity stores that follow standards-based LDAP, ISE can provide a customizable connector. Cisco ISE supports up to 50 independent non-trusted Active Directory forests with selection criteria to deal with username ambiguity.

- **Location-based access controls.** As eluded to briefly in the Network segmentation bullet point, network segmentation is a fluid event. Cisco Location Containment and Visibility with Mobility Service Engine (MSE) uses the physical location of the device as a factor in determining the type of access a device should have on a network.

In ISE, Cisco makes a concerted effort to balance the needs of security, endpoint policy and enforcement, network segmentation, and on-boarding a significant amount of end users with minimum effort.

Technology Leverage

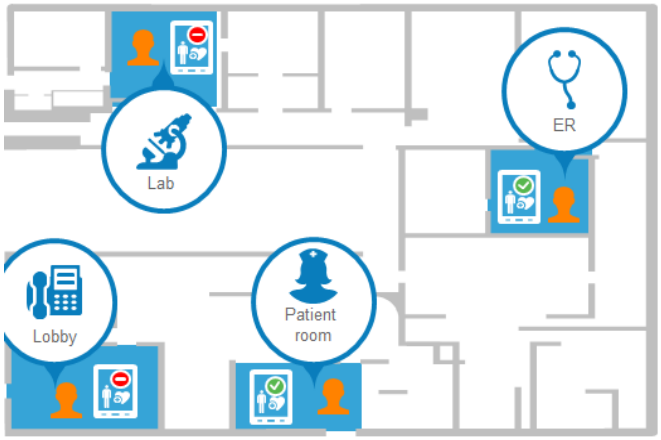
The difference between the NAC of a decade ago and next generation NAC is like the difference between black-and-white and color TV (or more apropos to our time perhaps the difference between standard-definition and high-definition TV).

The older NAC was an on-premises tool that enforced only rules-based endpoint compliance. The decision was almost literally black-and-white as endpoints were denied access to the company's main network (VPN/VLAN/data center). What has happened is next generation NAC uses analytics to determine contextual awareness. In gathering information about the endpoint, the NAC can factor in vulnerability, network mapping, policy compliance, behavioral patterns, physical location of an endpoint, and historical activities and connections, as well as information from third-party security platforms like firewalls or VM to determine risk, and, in turn use the risk assessment to determine network access.

Cisco ISE can be used to determine more than access conditions. Bidirectional communication with security platforms can make both Cisco ISE and the connected security appliance better. For instance, in communications with a firewall, if Cisco ISE quarantines an endpoint for lack of compliance, it can tell the firewall to look for similar traffic patterns and block the traffic from entering the network. As mentioned earlier, the next generation NAC can be used to investigate security incidents or to initiate more formal forensics investigations. Cisco uses Terminal Access Controller Access Control System (TACACS+). Cisco ISE can leverage the TACACS+ security protocol to control and audit the configuration of network devices. In investigations, network devices are configured to query ISE for authentication and authorization of device administrator actions, and send accounting messages for ISE to log the actions. Cisco ISE can also be the central administration point to push patches and security agents to endpoints.

The combination of integrations, risk-based analytics on Cisco ISE, and contextual awareness creates an innumerable amount of capabilities facilitating IT, security, and operational networking needs. One really interesting application is Cisco Location Containment and Visibility with Mobility Service Engine (MSE).

While Cisco ISE includes native location services, it also integrates with Cisco MSE to introduce more precise physical location-based authorization. Cisco ISE uses information from MSE to provide differentiated network access based on the actual location of the user, as reported by MSE.



Source: Used with Permission from Cisco Systems, Analyst Deck

To determine the location of a device, the MSE measures the signal strength (think of it as the radius of the circle that surrounds the AP, the endpoint is located on the edge of the circle). Since the MSE knows where the APs are located, it can triangulate the number of readings to tell where the device is. Location-based access can be determined within 1–2 meters of the device's physical location.

In the illustration, a schematic of a hospital is shown. Within a matter of meters, the access conditions for a

surgeon or physician can change.

By accepting data from the Cisco MSE, Cisco ISE can begin to enforce endpoint policies:

- The MSE location attributes are used for to authorize policies
- The MSE periodically checks for location changes
- The ISE now adjusts for granular policy control based upon the user, and enhanced policy enforcement.
- ISE reauthorizes authorization/access based on new location.
- Simplifies network management by configuring authorization with ISE management tools.

Cisco Location Containment and Visibility with MSE is emblematic of what Cisco ISE can do. Cisco's next generation NAC can combine multiple factors into a single value to determine access decisions and permissions and then initiate a response that gives Cisco ISE power.

Customer Ownership

The inputting of end users/devices onto a NAC can be onerous. Cisco ISE has native technologies that help IT/security teams set up and subsequently monitor their networks.

In many networking environments, IT administrators cannot always register devices onto a network. ISE offers a simple and automated on-board process. Out-of-the-box, Cisco ISE generates workflows that walk users through the on-boarding process and provides end users with their own self-service portals to add and manage their devices. ISE provides automatic supplicant provisioning and certificate enrollment for standard PC and mobile computing platforms. Lastly, for mobile devices, ISE can direct the user to the MDM or enterprise mobility management system to connect the registration flow with the overall mobile device. (Note, toward successful on-boarding, ISE along with Cisco Wireless Controllers have several mechanisms built in to ensure the solution gracefully handles high volumes of authentications. The advantages are not just in software).

Writing rules and establishing roles for each individual device coming onto a network would inundate an IT/security team. The Cisco Device Profile Feed associates a device with the type of policies that should be enforced. After an IP address or MAC address is entered onto a network, a proper profile of the devices needs to be built. Toward building the profile, ISE supports attributes across six different probes (HTTP, SNMP, DHCP/DNS, NMAP, NetFlow, RADIUS). ISE provides the ability for the system to call an update server nightly to gather the latest profiling definitions. The collection of attributes is then correlated and becomes a part of its device profiling capability. Currently, ISE has 544 device profiles out-of-the-box.

ISE supports a certificate authority service option. Cisco next generation NAC can check the certificate status of a device using the standards-based Online Certificate Status Protocol (OCSP). If a device is stolen, ISE can then provide automatic certificate revocation. It is anticipated that the Internet of Things (IoT) may consist of between 15—20 billion devices by 2020. To enroll IoT devices, Cisco ISE has a certificate provisioning portal to help with the manual creation of bulk or single certificates and key pairs, so that these devices can be connected to the network with a high degree of security.

Of real significance to an IT team, a next generation NAC should be extensible. The ISE architecture is scalable. ISE uses scalable protocols that allow Network Access Devices (switches, wireless LAN controllers, VPN concentrators and such) to focus on delivering network access and deal less with enforcing policies. Cisco next generation NAC platform can be scaled to facilitate up to 1,000,000 total endpoints and 250,000 concurrent endpoints. (Note: Cisco anticipates its next version of Cisco next generation NAC will support 1,500,000/and 500,000 endpoints respectively).

Next generation NAC traverses network requirements for IT, operations, and security. Next generation NACs also need to enforce policies for managed and mobile devices. Cisco ISE and related technologies largely reduce the friction experienced by IT/security teams, and ensure these processes transparently to the end user.

Conclusion

In 2015, the global NAC market for appliances and related services was $592.5 million. Cisco Systems is lauded here for its Market Leadership—it should be noted that each NAC deployment is different in terms of deployments needs (security, agent/agentless approach, quick on-boarding, and integration and orchestration with other IT and network security platforms, etc.).

While each NAC platform has its own distinct approach to NAC, there are compelling reasons to work with Cisco ISE. In the recent Frost & Sullivan Market Engineering study (Network Access Control (NAC) Global Market: Comprehending the Endpoint and Network Orchestration)[2], Cisco Systems is cited as having four Points of Competitive Differentiation:

- Security Features in a NAC
- Best Access Controls
- Best Innovation Initiated in 2015
- Rapid Threat Containment

[2] From the Frost & Sullivan Market Engineering Study, *Network Access Control (NAC) Global Market: Comprehending the Endpoint and Network Orchestration*, May 2016, Report#K001-74.

Cisco has taken a long view of what should happen on the NAC to protect the local network. However, Cisco ISE is further extensible with ways to connect with other network security platforms as well to connect other networks and security appliances to PxGrid to crowdsource external threat platforms in hopes of preventing malware on a global scale.

Cisco Systems has achieved a leadership position in the NAC market, with a market share of 39.3%.Because of this strong performance, Frost & Sullivan recognizes Cisco Systems with the 2016 Market Leadership Award.

Significance of Market Leadership

Ultimately, growth in any organization depends upon customers purchasing from your company, and then making the decision to return time and again. Loyal customers become brand advocates; brand advocates recruit new customers; the company grows; and then it attains market leadership. To achieve and maintain market leadership, an organization must strive to be best-in-class in three key areas: understanding demand, nurturing the brand, differentiating from the competition. This three-fold approach to delivering market leadership is explored further below.

Understanding Market Leadership

As discussed on the previous page, driving demand, strengthening the brand, and competitive differentiation all play a critical role in a company's path to market leadership. This three-fold focus, however, is only the beginning of the journey and must be complemented by an equally rigorous focus on the customer experience. Best-practice organizations therefore commit to the customer at each stage of the buying cycle and continue to nurture the relationship once the customer has made a purchase. In this way, they build a loyal, ever-growing customer base and methodically add to their market share over time.

Key Performance Criteria

For the Market Leadership Award, we focused on specific criteria to determine the areas of performance excellence that led to the company's leadership position. The criteria we considered include (although not limited to) the following:

Criterion	Requirement
Brand Strength	The possession of a brand that is respected, recognized, and remembered
Implementation Excellence	Processes support the efficient and consistent implementation of tactics designed to support the strategy
Growth Strategy	Demonstrated ability to consistently identify, prioritize, and pursue emerging growth opportunities
Product Quality	The product or service receives high marks for performance, functionality and reliability at every stage of the life cycle
Product Differentiation	The product or service has carved out a market niche, whether based on price, quality, uniqueness of offering (or some combination of the three) that another company cannot easily duplicate
Technology Leverage	Demonstrated commitment to incorporating leading edge technologies into product offerings, for greater product performance and value
Price/Performance Value	Products or services offer the best value for the price, compared to similar offerings in the market
Customer Purchase Experience	Customers feel like they are buying the most optimal solution that addresses both their unique needs and their unique constraints
Customer Ownership Experience	Customers are proud to own the company's product or service, and have a positive experience throughout the life of the product or service
Customer Service Experience	Customer service is accessible, fast, stress-free, and of high quality

The Intersection between 360-Degree Research and Best Practices Awards

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 to 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 over 50 years of experience in partnering with Global 1000 companies, emerging businesses and the investment community from 45 offices on six continents. To join our Growth Partnership, please visit http://www.frost.com.