2018 North American Authentication Solutions Technology Leadership Award
Contents
Background and Company Performance ................................................................. 3

   Industry Challenges.......................................................................................... 3

   Technology Leverage and Business Impact of Symantec .............................. 4

   Conclusion........................................................................................................ 5

Significance of Technology Leadership ............................................................. 7

Understanding Technology Leadership ............................................................. 7

   Key Benchmarking Criteria ........................................................................... 8


The Intersection between 360-Degree Research and Best Practices Awards .......... 10

   Research Methodology .................................................................................. 10

About Frost & Sullivan ....................................................................................... 10
Background and Company Performance

Industry Challenges

The Internet of Things (IoT) and ubiquitous connectivity deliver a myriad of benefits for organizations, such as increased productivity and revenue, but they also bring security challenges that put them at a higher risk for breaches and cyberattacks. As a growing number of enterprises deploy bring-your-own-device strategies and authorize employees to work remotely, so does the introduction of new vulnerabilities that cybercriminals exploit through their ever-evolving hacker modalities. Inadequate cybersecurity solutions leave businesses at risk for significant losses, including but not limited to, C-level jobs, customers’ trust and loyalty, intellectual property (e.g., trade secrets and customers’ data), and hefty fines. Many cybersecurity technologies verify a person’s identity via a single sign-on (SSO) credential, such as a personal identification number (PIN) or a password, which cybercriminals can hack or steal easily. Such rudimentary verification methods allow employees and hackers to access devices, networks, or applications (apps) effortlessly, leaving an enterprise vulnerable to countless malicious attacks. Two-factor authentication (2FA) and multi-factor authentication (MFA) solutions provide organizations with a more resilient cybersecurity protection solution than traditional firewall or perimeter defenses, particularly with technologies that monitor the behavior of a user throughout their session.

Furthermore, organizations need to meet company- and industry-specific standards, regulations, and policies while defending their ecosystem with a robust, comprehensive cybersecurity solution. In some cases, non-compliance and inadequate cybersecurity protection can lead to severe consequences, such as lost revenues, the financial cost to mend a company’s tarnished reputation, or the loss of life. For instance, healthcare organizations can be held accountable for violating the Healthcare Insurance Portability and Accountability Act and face significant fines or lawsuits from patients or their families. Moreover, a financial institution’s data breach can result in confidential customer information ending up in the hands of a hacker, and the organization may encounter fines for violating security and privacy compliance standards if they are not sufficiently securing and providing adequate protection for a customer’s personal information. Finally, a government agency’s infrastructure breach is a matter of national security and can have grim safety and security implications for an entire country.

Chief concerns among C-level executives regarding new solution implementation and configuration include the initial cost, return on investment (ROI), and operational downtime; thus, many organizations avoid rip-and-replace technologies. Vendors providing solutions that encompass these requirements often do not offer a comprehensive cybersecurity product line. Therefore, businesses need to piecemeal technologies from various companies, which do not guarantee compatibility and could cause delays or disruptions to business operations.
**Technology Leverage and Business Impact of Symantec**

Founded in 1982, California-headquartered Symantec™ is a global leader in the cybersecurity market. The company gives its users strong security through its identity and verification management service, Symantec™ VIP (Validation and ID Protection), regarded as the first cloud-based authentication solution on the market globally. Symantec provides a myriad of user-friendly authentication and access methods to apps and networks for on-premise, cloud, and hybrid-cloud environments via a secure and intelligent platform. Notably, the cloud and hybrid cloud options remove an organization’s need for on-premise hardware and the real estate to house such hardware, while decreasing the need for in-house information technology (IT) support staff; thus, lowering operational expenditures.

**Industry-leading Validation and ID Protection Service**

Symantec’s VIP authentication service enables clients to verify a user’s identity—employee or consumer—with its secure, reliable, and scalable solution, while providing the end user with a stress-free, effortless, and positive experience. The company’s authentication technology empowers organizations to secure their apps and networks via a customer-tailored verification process. For example, businesses can select from several authentication methods: one-touch push verification, mobile or workstation one-time password (OTP), security token or card OTP, risk-based authentication, biometrics (e.g., fingerprint, facial, or voice), text OTP, device ID, or voice call OTP. Furthermore, enterprises can require end users to provide one credential or 2FA, as well as behavioral authentication. For instance, when users logs in to their bank app on their smartphone, they usually check the usual areas—e.g., account balance. However, if a user logs-in and begins clicking and viewing areas they have never clicked before, Symantec™ VIP may prompt them for authentication again to verify the user’s identity further.

Furthermore, VIP offers a robust device hygiene and threat intelligence that allow organizations to go beyond just a second factor or step-up authentication. While the user may have verified their identity with a strong multi-factor authentication method such as one-touch push verification or voice biometric, there is no way an organization can verify that the user’s device or web application is not compromised. For example, while the user may be legitimate, their laptop or phone that they are using to log into their bank account may have been hacked by a malicious outsider who is waiting for the unassuming user to log into their sensitive accounts. Once the user logs into their account, the attacker has access to the victim’s bank account and therefore bypass the multi-factor authentication process altogether. VIP can detect a wide range of risk factors such as out-of-date devices, rooted or jail-broken phones, malicious WiFi networks, malware or ransomware, debuggers, and much more. In fact, VIP leverages the world’s largest civilian threat intelligence network to identify advanced threats such as malicious URLs and applications to protect users from the most recent web or mobile attacks. In a world where it is difficult to manage BYO devices or cloud applications, these advanced device hygiene and threat intelligence capabilities give added security for every single authentication attempt to verify not just the users but their devices and applications.
Symantec™ VIP integrates seamlessly with common virtual private networks, webmail, SSO apps, and user directories. The company ensures its services and products meet National Institute of Standards and Technology, North American Electric Reliability Corporation Critical Infrastructure Protection, and Federal Risk and Authorization Management Program compliance standards and regulations. Notably, Symantec prepared for and deployed General Data Protection Regulation compliant solutions well before it was a necessity, equipping customers to meet requirements in a timely manner.

**Exceptional Customer Service that Empowers Clients**

Symantec ensures it meets customer, end user, and industry needs by keeping the line of communication open and collaborating with its partners. Introduced over 10 years ago, VIP has many long-term clients, and Frost & Sullivan asserts this serves as a testament to Symantec’s ability and willingness to develop and evolve the technology to meet the needs of its customers. Furthermore, the high level of security ingrained in the solution gains and maintains the trust of clients and end users around the world. As a trusted, world-renowned cybersecurity vendor, Symantec understands the value of retaining the customer’s trust through industry-leading technologies that secure networks, apps, and devices, and the benefits of listening to clients' and end users' feedback and then implementing those suggestions to create an innovative service.

The company has experienced substantial growth in the last four years due to organizations’ desire to move away from static passwords towards 2FA and MFA credentials. Moreover, clients want to shift from on-premise only solutions to hybrid or entirely cloud environments. The company works closely with enterprises during these transitions to ensure clients understand the features available to them and how to use the technology to receive the most benefits and value. Also, Symantec offers consulting services, premium support options, technical training, and cybersecurity services to ensure clients receive the assistance they need to achieve a resilient and mature cybersecurity ecosystem.
**Conclusion**

As the BYO devices, cloud applications, and connectivity proliferate, organizations are met with countless benefits; however, it also creates challenges as it opens various avenues for malicious attacks via fraudulent or stolen credentials. Businesses can no longer rely on basic authentication methods—e.g., password or personal identification number. Therefore, they must turn to two-factor authentication (2FA) or multi-factor authentication (MFA), and behavior monitoring to protect their networks, devices, and applications. Additionally, many organizations must meet industry-compliance standards to prevent harsh consequences, such as substantial fines and the loss of C-level jobs.

Symantec offers its industry-leading technology solution, Symantec™ VIP (Validation and ID Protection), a secure identity and authentication service that provides customers with a myriad of benefits and value. Offered as an on-premise, hybrid, or entirely cloud solution, VIP enables end users to verify their identity via a spectrum of authentication methods—e.g., biometrics, push notification, and security token/card—as a one-time password, 2FA, or MFA. With its future-facing technology, superior security capabilities, customer-focused innovation, and strong overall performance, Symantec earns Frost & Sullivan’s 2018 North America Technology Leadership Award for its authentication solution, Symantec™ VIP.
Significance of Technology Leadership

Technology-rich companies with strong commercialization strategies benefit from the increased demand for high-quality, technologically-innovative products. Those products help shape the brand, leading to a strong, differentiated market position.

Understanding Technology Leadership

Technology Leadership recognizes companies that lead the development and successful introduction of high-tech solutions to customers’ most pressing needs, altering the industry or business landscape in the process. These companies shape the future of technology and its uses. Ultimately, success is measured by the degree to which a technology is leveraged and the impact that technology has on growing the business.
Key Benchmarking Criteria

For the Technology Leadership Award, Frost & Sullivan analysts independently evaluated two key factors—Technology Leverage and Business Impact—according to the criteria identified below.

Technology Leverage
- Criterion 1: Commitment to Innovation
- Criterion 2: Commitment to Creativity
- Criterion 3: Technology Incubation
- Criterion 4: Commercialization Success
- Criterion 5: Application Diversity

Business Impact
- Criterion 1: Financial Performance
- Criterion 2: Customer Acquisition
- Criterion 3: Operational Efficiency
- Criterion 4: Growth Potential
- Criterion 5: Human Capital
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.

<table>
<thead>
<tr>
<th>STEP</th>
<th>OBJECTIVE</th>
<th>KEY ACTIVITIES</th>
<th>OUTPUT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Monitor, target, and screen</td>
<td>Identify Award recipient candidates from around the globe</td>
<td>Conduct in-depth industry research, Identify emerging sectors, Scan multiple geographies</td>
</tr>
<tr>
<td>2</td>
<td>Perform 360-degree research</td>
<td>Perform comprehensive, 360-degree research on all candidates in the pipeline</td>
<td>Interview thought leaders and industry practitioners, Assess candidates’ fit with best-practice criteria, Rank all candidates</td>
</tr>
<tr>
<td>3</td>
<td>Invite thought leadership in best practices</td>
<td>Perform in-depth examination of all candidates</td>
<td>Confirm best-practice criteria, Examine eligibility of all candidates, Identify any information gaps</td>
</tr>
<tr>
<td>4</td>
<td>Initiate research director review</td>
<td>Conduct an unbiased evaluation of all candidate profiles</td>
<td>Brainstorm ranking options, Invite multiple perspectives on candidates’ performance, Update candidate profiles</td>
</tr>
<tr>
<td>5</td>
<td>Assemble panel of industry experts</td>
<td>Present findings to an expert panel of industry thought leaders</td>
<td>Share findings, Strengthen cases for candidate eligibility, Prioritize candidates</td>
</tr>
<tr>
<td>6</td>
<td>Conduct global industry review</td>
<td>Build consensus on Award candidates’ eligibility</td>
<td>Hold global team meeting to review all candidates, Pressure-test fit with criteria, Confirm inclusion of all eligible candidates</td>
</tr>
<tr>
<td>7</td>
<td>Perform quality check</td>
<td>Develop official Award consideration materials</td>
<td>Perform final performance benchmarking activities, Write nominations, Perform quality review</td>
</tr>
<tr>
<td>8</td>
<td>Reconnect with panel of industry experts</td>
<td>Finalize the selection of the best-practice Award recipient</td>
<td>Review analysis with panel, Build consensus, Select recipient</td>
</tr>
<tr>
<td>9</td>
<td>Communicate recognition</td>
<td>Inform Award recipient of Award recognition</td>
<td>Present Award to the CEO, Inspire the organization for continued success, Celebrate the recipient’s performance</td>
</tr>
<tr>
<td>10</td>
<td>Take strategic action</td>
<td>Upon licensing, company is able to share Award news with stakeholders and customers</td>
<td>Coordinate media outreach, Design a marketing plan, Assess Award’s role in future strategic planning</td>
</tr>
</tbody>
</table>
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.

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 more than 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.