FROST & SULLIVAN

BEST PRACTICES AWARDS

OneSpan

Be bold. Be secure.

2020 GLOBAL DIGITAL IDENTITY AND RISK-BASED AUTHENTICATION PLATFORM COMPANY OF THE YEAR AWARD

Contents

Background and Company Performance

Industry Challenges

As organizations and consumers recognize the benefits of conducting transactions through mobile and web-based platforms, fraud has shifted from in-person to remote interventions, perpetrated in the online, mobile, and voice-based self-serve environments. High-profile data breaches in recent years have exposed millions of consumers' sensitive personally identifiable information (PII), which is increasingly being used by cybercriminals to create new, digital-only identities for application fraud and account takeover (ATO) fraud, fraudulent tax return filing, and other misdeeds. By analyzing various data sources to identify unusual behavior or high-risk transactions through rule- and analytics-based methodologies, fraud prevention solutions represent the core intelligence essential to helping organizations address fraud and security challenges.

Moreover, traditional identity verification credentials—e.g., a password or personal identification number (PIN)—are no longer effective options alone to authenticate an end user as imposters use various tactics to gain confidential data. To overcome issues regarding traditional credentials, vendors deployed multi-factor authentication (MFA) credentials as an additional security measure, such as a security question or a one-time password sent via email, text, or phone call. However, cybercriminals can obtain security answers on social media platforms or access other information—including passwords and PINs—through screen-scraping or key-logging via passive malware.

To combat this new set of challenges, technology companies have integrated biometric identity and authentication capabilities so hackers cannot steal biometric modalities—e.g., facial, fingerprint, iris, or voice. However, malicious actors can hack the biometric template information—while they are technically more secure, methods have arisen to make them as easily hackable as traditional credentials—while authentication processes transmit the data back and forth as most companies do not secure this information sufficiently while such transfers occur. Hackers can then use the biometric template data to trick a system into accepting the data as a valid and verified identity credential. Once a cybercriminal compromises an account, they can access proprietary or confidential data with the chances of detection being low because many platforms do not verify a user's identity beyond the initial sign-in process. Organizations must implement more robust security technologies that detect threats in real time and throughout a user session to prevent hackers from gaining access to accounts and systems or from harvesting sensitive data from an accountholder if hackers do bypass a traditional sign-on method.

In response to hackers continuously enhancing their tactics, technology companies developed abnormal behavior detection capabilities—i.e., behavioral biometrics—to provide organizations with real-time continuous monitoring of a user's sessions, which can trigger identity verification unique to a consumer's interactions through adaptive authentication—i.e., risk-based authentication capabilities. Adaptive authentication technologies passively—and sometimes, actively—challenge the user to secure a session better through a precise level of security for each unique user interaction based on their risk score. Adaptive authentication solutions typically generate a risk score for users based

on real-time analysis of vast amounts of user, device, and transaction data. An individual's risk score triggers automated security workflows that apply the exact security measures required to secure the user's session and account. Behavioral biometrics observes a user's activities, such as how they interact with their mobile device and touch the screen (e.g., swipe curvature, length, and velocity and the pressure applied)—while adaptive authentication capabilities analyze and compare that data to the account owner's previous typical actions during a session.

Moreover, Frost & Sullivan's research indicates that fraud prevention solutions focused primarily on static data and rule-based analytics to address transaction fraud are inadequate for preventing the sophisticated mechanisms employed by hackers. There is a clear need for behavioral analytics-based fraud management solutions that can leverage the power of machine learning (ML) and artificial intelligence (AI) to identify threats and assist with timely decision-making for fraud prevention. The ability to collect, create, and augment data from across verticals, industries, companies of various sizes, locations, and types of products to find patterns and behaviors that would otherwise be hidden if the data were only in a single network or location is imperative. Ultimately, it is not just the amount of data that is collected: what the provider does with the data is what matters for successful fraud prevention.

Finally, due to various liabilities and government fines for non-compliance with industry standards, organizations must meet strict mandates that protect access to information stored, gathered, or accessed. Increased awareness and concern for data security and privacy matters—as evidenced by the General Data Protection Regulation (GDPR) from the European Union and heightened security concerns globally—rapidly accelerate an organization's need to protect access to digital data from nefarious individuals.

Visionary Innovation & Performance and Customer Impact of OneSpan

Founded in 1991 and headquartered in Chicago, Illinois in the United States (US), OneSpan develops and delivers revolutionary digital identity and anti-fraud solutions that protect companies and users through risk-based analytics and advanced fraud detection. The company serves clients globally in the banking and financial services, government, healthcare, and insurance industries. Frost & Sullivan recognized OneSpan as the 2019 Global Customer Value Leader in the risk-based authentication market and continues to be impressed by the company's on-going innovation and security-focused design.

Game-changing Digital Identity and Risk-based Authentication Technology

OneSpan's cloud-based, software-as-a-service solutions are powered by their Trusted Identity Platform and consist of digital identity and anti-fraud solutions that secure a consumer's PII through various capabilities. These include e-signatures, fraud analysis, identity verification, mobile app security, and risk-based authentication. The Trusted Identity Platform's application programming interface enables clients to integrate the solution with any third-party platforms, making it a future-proof identity authentication platform. This comprehensive solution portfolio prevents malicious individuals from breaching a client's ecosystem and harvesting consumers' confidential data. The

capability, in conjunction with OneSpan's behavioral biometrics feature, offers consumers a frictionless experience while securing their account by monitoring throughout the session to remove unnecessary identity verification steps—i.e., presenting credentials. The Intelligent Adaptive Authentication enables an authorized user to access and navigate their account without interruption while securing the account and associated digital information against unauthorized cybercriminals.

For example, if an end user usually logs into a banking application (app) to check their account balance, Intelligent Adaptive Authentication will require they provide additional credentials if they are using a different or jailbroken device, logging in from an unusual location or IP address, or attempt to enact a transaction in a larger than usual amount or to an unknown recipient. Such capabilities stop hackers as they do not know the typical actions of the account's owner. OneSpan's Intelligent Adaptive Authentication solution prompts the user for credentials. If such modalities are incorrect, the platform will activate other security credentials to prove a user's identity based on the level of risk associated with the transaction; these additional protocols may include additional biometrics, one-time passcodes, or potentially ending a session if the transaction is deemed too high of a risk and potentially fraudulent. For instance, an organization may allow a user three attempts to verify their identity, if the individual does not provide proper credentials, the platform boots and suspends them from the session for a pre-defined number of minutes or hours, depending on the client's pre-determined settings. Alternatively, Intelligent Adaptive Authentication requests a different set of credentials—e.g., fingerprint, one-time password or PIN, or voice—or requires the user to contact customer support to unlock the account, depending on the security level an organization needs to maintain.

Moreover, OneSpan equipped its Intelligent Adaptive Authentication solution with sophisticated ML capabilities that drastically reduce the number of false positives and false negatives as demonstrated by competing technologies. Subsequently, the solution decreases credential prompts for an authorized user's low-risk transactions and prevents account takeovers by deploying risk-based analytics to hinder hackers from accessing PII and committing fraud. Intelligent Adaptive Authentication detects, identifies, and prioritizes potential fraudulent transactions, freeing analysts to concentrate first on the more devastating incidents that could rapidly spawn further events, compromise consumers' data, or damage the organization's brand reputation. Moreover, the solution also detects unsecured endpoints, such as jailbroken and rooted devices. The company applies advanced proprietary encryption layers to protect all communications channels (i.e., email, text, and phone call) through OneSpan's Mobile Security Suite to prevent malicious individuals from eavesdropping, screen-scraping, key-logging, and stealing information and credentials (including biometric data templates).

> "*We selected OneSpan's innovative solutions because they provide a high level of security and usability. Traditionally, it's very difficult to combine the two—until now, it's always been a trade-off. We wanted to innovate and simplify the customer experience. With this project, we were able to do that*."
>
> —Alexander Kiesswetter, CIO at Raiffeisen Information System

The company's digital account opening solution, in conjunction with the capabilities above, allow OneSpan's clients to experience higher consumer self-onboarding rates by removing the frustrating and time-consuming process of visiting a physical location. Furthermore, customers achieve a lower consumer onboarding abandonment rate due to the seamless account opening feature and integrated Know Your Customer (KYC) compliance tool, ultimately increasing revenue and consumer loyalty. OneSpan's onboarding process enables consumers to complete account registration in minutes, significantly reducing abandonment rates. At the same time, the KYC compliance feature allows banks to ensure that remote applicants are who they say they are through real-time, accurate identity verification.

OneSpan integrates identity validation capabilities into its solutions to meet KYC mandates by requiring onboarding consumers to provide a photo of their driver's license or state/country identification card and take a selfie, allowing the technology to compare the two pictures for identity verification. Moreover, to ensure the selfie is a real-time image of the individual and not a photograph held in front of the camera, OneSpan's platform sends data from a short video surrounding the selfie capture to check for liveliness. Impressing Frost & Sullivan's research analysts, one of the top Canadian banks implemented OneSpan's Trusted Identity Platform and reduced account opening errors by 80% and achieved a 40% increase in process efficiency. Moreover, bank customers were able to open an account in less than eight minutes using the smartphone banking application.[1]

Impressive Partnerships and Customer-centric Design

OneSpan's integration and technology partner network consists of world-renowned companies, including Aware, BehavioSec, Cisco, Forgerock, IBM, Jumio, Microsoft, Nok Nok, Salesforce, and Validated ID. The company's close collaboration with its partners, combined with the Trusted Identity Platform's API, allows OneSpan to ensure its solutions remain compatible with third-party systems, platforms, and apps, creating a seamless deployment and integration process for clients. The company's customer base includes organizations such as Bank of Cyprus, HSBC, Investec, Mizuho, OneMain, P&V Insurance, Raiffeisen, the US Department of Agriculture, the US Department of Transportation, and Wells Fargo.

> "*We purchased [OneSpan Sign] for tracking and evidence of electronic document delivery. The benefits we've experienced are customer convenience, cost savings, and an improved loan process*."
>
> —Wells Fargo

OneSpan specifically designed its Trusted Identity Platform to secure digital banking and financial environments; it boasts more than 2,000 financial institutions amongst its client base of more than 10,000 organizations. Serving as a testament to the company's unmatched technology and market leadership, more than half of the top 100 banks and financial institutions globally are OneSpan customers. The company makes online banking

[1] https://www.onespan.com/solutions/account-opening-onboarding (OneSpan website, accessed March 2020)

processes efficient and secure by automating e-signature workflows integrated with industry-leading security layers—through OneSpan Sign solution—while meeting industry compliance mandates.

OneSpan equips its solutions with comprehensive industry compliance audit reporting that automatically generates compliance reports, which demonstrates to auditory agencies that the organization took the proper steps required to conduct transactions online—e.g., following KYC regulations. Furthermore, such audit reports are vital to an organization if a consumer disputes a transaction and enables the financial institution to research a dispute promptly with digital forensic evidence—which also protects the consumer in fraud and identity theft cases.

> "*For us, it was important to partner with a market leader that could demonstrate expertise in the financial sector*."
>
> —Mr. Nasar Siddiqui, Head of Digital Channels at National Bank of Fujairah

The company's solutions enable financial institutions to avoid ramifications due to non-compliance—e.g., failed industry compliance audits, costly fines, brand reputation damage, and the job loss of C-level executives. In addition to OneSpan's headquarters in the US, the company also has offices in Austria, Australia, Belgium, Canada, Beijing and Shanghai in China, France, Japan, Enschede and Rosmalen in the Netherlands, Singapore, Switzerland, the United Arab Emirates, the United Kingdom, and Massachusetts, US to enable it to serve its clients better, work with them more closely to fulfill their needs, and remain abreast to regional industry compliance standards. Such industry regulations include Fast ID Online, the Federal Financial Institutions Examination Council regulations, GDPR, the Payment Card Industry Data Security Standard, and the Payments Services Directive. The Trusted Identity Platform's MFA compatibility, combined with its automated industry compliance capabilities, allows clients to focus on their business rather than worrying about security and industry compliance and creates a seamless and secure experience for consumers.

Comprehensive Resources for Clients and Market Participants

Social engineering or the art of deceiving or tricking people into divulging login credentials or access through a wide variety of communication mediums, such as phone, email, and social media platforms make up 43% of total cybersecurity breaches. Malicious actors leverage social engineering strategies to target an individual's curiosity and fear while often creating a false sense of urgency or by promising money or fame. Such tactics prompt some end users into voluntarily divulging confidential data to cybercriminals, not knowing the individual's malicious intent.

Cybercriminals are even capitalizing on the novel coronavirus (COVID-19) pandemic by baiting people with malicious emails, causing individuals to download malware inadvertently. In response, OneSpan published a blog post warning organizations about COVID-19 phishing emails and how they can protect their business and consumers. Frost & Sullivan's research analysts note that phishing attacks are one of the leading causes of cybersecurity breaches and ATO fraud, and thus organizations must ensure their employees are well-informed and remain vigilant in combatting such attacks. Many

cybercriminals pose as a legitimate organization, such as the World Health Organization, the Centers for Disease Control and Prevention, or a supplier informing the business about a delivery delay. OneSpan's blog walks readers through the challenges, hackers' tactics, and how to combat such attacks. Moreover, the company provides a social engineering and phishing prevention feature as part of its Mobile Security Suite and offers it as part of its Enterprise Security solution, allowing organizations to protect their ecosystem—including company-approved, third-party, or personal devices—and to defend consumers' devices and accounts from such attacks.

In addition to its regularly posted blogs, OneSpan provides clients with e-books, webinars, whitepapers, and the OneSpan Community Portal—an online forum that allows administrators, developers, and end users to communicate with one another about industry trends, technologies, and overcoming challenges. The OneSpan Community Portal enables members to ask and respond to questions, helping them on the digital security journey. Moreover, the company provides videos on various topics, such as customer success stories and how to optimize OneSpan's solutions.

Conclusion

With the Internet of Things' rapid expansion, organizations' digital environments expose more surface areas to attack due to bring-your-own-device strategies and work-from-home policies. Cybercriminals continue to refine their methods of acquiring credentials and accessing consumers' private information to sell on the dark web for financial gain. OneSpan's Trusted Identity Platform provides digital identity verification and risk-based authentication solutions equipped with anti-fraud and e-signature capabilities to combat the ever-evolving hacker model through multi-factor credentialing, behavior monitoring, advanced adaptive authentication, and automatic industry compliance report generation. The company maintains a close relationship with its partners and clients, enabling it to develop technologies that customers need while filling key capability gaps in the market, such as liveliness detection through selfie photographs to validate an individual's identity.

For its unique technologies, commitment to customer-focused strategies, and strong overall performance, OneSpan earns Frost & Sullivan's 2020 Global Company of the Year Award in the digital identity and risk-based authentication platform market.

Significance of Company of the Year

To receive the Company of the Year Award (i.e., to be recognized as a leader not only in your industry, but among non-industry peers) requires a company to demonstrate excellence in growth, innovation, and leadership. This excellence typically translates into superior performance in three key areas—demand generation, brand development, and competitive positioning—that serve as the foundation of a company's future success and prepare it to deliver on the 2 factors that define the Company of the Year Award: Visionary Innovation and Performance, and Customer Impact).

Understanding Company of the Year

Driving demand, brand strength, and competitive differentiation all play critical roles in delivering unique value to customers. This three-fold focus, however, must ideally be complemented by an equally rigorous focus on Visionary Innovation and Performance to enhance Customer Impact.

Key Benchmarking Criteria

For the Company of the Year Award, Frost & Sullivan analysts independently evaluated each factor according to the criteria identified below.

Visionary Innovation & Performance

Criterion 1: Addressing Unmet Needs
Criterion 2: Visionary Scenarios through Mega Trends
Criterion 3: Implementation Best Practices
Criterion 4: Blue Ocean Strategy
Criterion 5: Financial Performance

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

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

Frost & Sullivan analysts 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 of 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	• 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 able to 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

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 participants and for identifying those performing at best-in-class levels.

360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS

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.