

2025 COMPANY OF THE YEAR

Driving impact across the customer value chain

RECOGNIZED FOR BEST PRACTICES IN THE NORTH AMERICAN SECURITY IN CUSTOMER EXPERIENCE MANAGEMENT INDUSTRY

FROST & SULLIVAN

Table of Contents

Best Practices Criteria for World-class Performance 3

The Strategic Imperative: 8 Factors Creating Pressure on Growth 2

Top Transformations Impacting Growth in the Security in Customer Experience Management Industry 4

TP: Innovating Cybersecurity with Automation and Fraud Analytics 5

A Holistic Approach to Security: Compliance, Training, and Intelligence Sharing 7

A Future-Proof Cybersecurity Framework 8

Conclusion 9

What You Need to Know about the Company of the Year Recognition 10

Best Practices Recognition Analysis 10

Visionary Innovation & Performance 10

Customer Impact 10

Best Practices Recognition Analytics Methodology 11

Inspire the World to Support True Leaders 11

The Growth Pipeline Generator™ 12

The Innovation Generator™ 12

Best Practices Criteria for World-class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each recognition category before determining the final recognition recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. TP excels in many of the criteria in the North American security in customer experience management space.

RECOGNITION CRITERIA	
Visionary Innovation & Performance	*Customer Impact*
Addressing Unmet Needs	Price/Performance Value
Visionary Scenarios Through Megatrends	Customer Purchase Experience
Leadership Focus	Customer Ownership Experience
Best Practices Implementation	Customer Service Experience
Financial Performance	Brand Equity

The Strategic Imperative: 8 Factors Creating Pressure on Growth



- **Innovative Business Models** - A new revenue model that defines how a company creates and capitalizes economic value, typically impacting its value proposition, product offering, operational strategies, and brand positioning
- **Compression of Value Chains** - Customer value chain compression as a result of advanced technologies, internet platforms, and other direct-to-consumer models that enables reduction in friction and the number of steps in customer journeys
- **Transformative Mega Trends** - Global forces that define the future world with their far-reaching impact on business, societies, economies, cultures, and personal lives
- **Disruptive Technologies -** The internal organizational behaviors that prevent a company from making required changes
- **Internal Challenges** - A new wave of competition from start-ups and digital business models that challenge the standing conventions of the past, compelling established industries to rethink their competitive stance

- **Competitive Intensity** - Chaos and disorder arising from political discord, natural calamities, pandemics, and social unrest that impact global trade, collaboration, and business security
- **Geopolitical Chaos** - New, disruptive technologies that are displacing the old, and significantly altering the way consumers, industries, or businesses operate
- **Industry Convergence** - Collaboration between previously disparate industries to deliver on whitespace cross industry growth opportunities

Top Transformations Impacting Growth in the Security in Customer Experience Management Industry

Rank	Strategic Imperative	Timeline	Impact (%)	Impact Curve
1	**Transformative Mega Trends** Rise of personalized AI assistants for customer service	2027 - 42	72	Polynomial
2	**Internal Challenges** Adapting to rapidly changing security regulations	2027 - 37	68	Exponential
3	**Transformative Mega Trends** Adoption of quantum computing for data encryption	2025 - 45	67	Exponential
4	**Geopolitical Chaos** Developing contingency plans for data centers in politically unstable regions	2025 - 45	66	Exponential
5	**Disruptive Technologies** Use of AR for immersive customer service experiences	2026 - 38	64	Exponential
6	**Industry Convergence** Collaboration with healthcare providers to integrate wellness data into customer service	2025 - 35	62	Exponential
7	**Compression of Value Chains** Automation of customer verification processes using AI	2025 - 37	61	Exponential
8	**Competitive Intensity** Strategic partnerships with tech giants for advanced R&D	2026 - 41	59	Polynomial
9	**Innovative Business Models** Launch of a subscription model for premium security services	2027 - 35	58	Linear
10	**Industry Convergence** Joint ventures with financial institutions to enhance payment security	2026 - 38	57	Linear

The Transformation of Security in Customer Experience Management Industry

Organizations across industries increasingly recognize customer experience (CX) as a fundamental driver of business success. As customer expectations continue to evolve, businesses face the challenge of delivering seamless, high-quality CX while addressing the growing complexities of service interactions. The demand for CX management (CXM) solutions is surging, fueled by technological advancements, shifts in consumer behavior, and an accelerated focus on digital transformation. The rise of artificial intelligence

(AI) and self-service automation streamlines customer interactions but also introduces new challenges. While AI-driven solutions improve efficiency, they make live customer engagements more complex, requiring businesses to invest in skilled human support alongside automated systems. Additionally, companies must balance cost efficiency with value creation, ensuring that CX investments enhance service quality without compromising operational effectiveness.

Security emerges as a critical pillar of CX, with increasing digitalization exposing organizations to heightened risks related to data breaches, identity theft, and cyberattacks. Regulatory frameworks such as the General Data Protection Regulation and the California Consumer Privacy Act reinforce the need for stringent compliance measures, particularly in highly regulated sectors like banking, financial services, insurance, and healthcare. Customers expect organizations to protect their data while demonstrating transparency and accountability in security practices. Additionally, trust and empathy influence customer relationships. Consumers prefer brands that prioritize their privacy, communicate openly, and take proactive steps to safeguard sensitive information. Organizations that embed security into their CX strategy differentiate themselves by fostering customer confidence and long-term loyalty.[1]

As businesses strive to integrate security into every touchpoint of the customer journey, the role of CXM providers is expanding. Companies seek partners that deliver exceptional service experience and robust security frameworks to safeguard customer interactions. Against this backdrop, industry leaders in CXM position themselves at the forefront of innovation, ensuring that their security and compliance capabilities evolve alongside customer needs.

TP: Innovating Cybersecurity with Automation and Fraud Analytics

Founded in 1978 and headquartered in Paris, France, TP emerges as a leader in secure CX, offering one of the most advanced cybersecurity programs in the CXM industry with its robust security infrastructure. The company's cybersecurity strategy prioritizes real-time monitoring, rapid response, and automation. Its system detects unauthorized changes within an average of two minutes and mitigates them in under 15 minutes. This level of responsiveness prevents service disruptions and ensures business continuity, a critical factor for clients relying on TP's secure environment. Its security system neutralizes 98% of cybersecurity incidents automatically before needing human intervention, demonstrating the efficiency of its automated threat detection framework.[2] The company maintains a resilient security posture while optimizing operational efficiency through automation and skilled cybersecurity personnel.

TP's cybersecurity framework includes a comprehensive fraud prevention program designed to address external and internal threats. The Security Risk Assessment process evaluates 220 various risk factors across five main areas:[3]

- **Caller Identification**: Evaluates the effectiveness of client authentication processes and determines whether agents can bypass security measures.
- **Agent Access**: Assesses whether agents have unrestricted access to client applications outside of active customer interactions.

[1] Security: The Key to Customer Experience Excellence (Frost & Sullivan, June 2024)

[2] Frost & Sullivan's Interview with TP (February 2025)

[3] Ibid.

- **Exposure of Sensitive Information**: Analyzes the extent of customer data visibility to agents and applies security measures such as tokenization to protect sensitive information.
- **Unauthorized Modifications**: Detects whether agents can alter customer data, such as payment details, without timely notifications to the customer.
- **Metric Manipulation**: Identifies risks related to agents tampering with key performance indicators such as customer satisfaction (CSAT) and average handling time to misrepresent service quality.

> *"The company's cybersecurity strategy prioritizes real-time monitoring, rapid response, and automation. Its system detects unauthorized changes within an average of two minutes and mitigates them in under 15 minutes. This level of responsiveness prevents service disruptions and ensures business continuity, a critical factor for clients relying on TP's secure environment."*
>
> ***- Sebastian Menutti***
> ***Research Director, Customer Experience***

This rigorous assessment enables the company to detect vulnerabilities and prevent exploitation, even in environments where client systems operate on legacy technology stacks with limited security capabilities. After identifying risks, TP categorizes them into three groups: TP-controlled risks, joint risks, and client-controlled risks.

TP mitigates these risks by deploying proprietary tools such as TP Protect, an advanced monitoring solution that detects unauthorized keystrokes, copy-pasting of sensitive information, and unapproved data modifications. TP Protect enhances monitoring, detection, and fraud prevention capabilities, particularly for high-risk sectors like retail and financial services. TP Protect integrates AI within a comprehensive security ecosystem, allowing the system to detect unauthorized behaviors and provide immediate alerts to supervisors and security teams. This capability enables proactive intervention before fraudulent activity occurs. Furthermore, it can be customized to meet specific client security requirements, offering an extra layer of protection against fraud and payment card data breaches.

Additionally, TP's Fraud Data Analytics program leverages AI and machine learning to detect anomalies and fraudulent behavior patterns using transaction reports from clients. Clustering techniques identify outliers, such as agents whose activity deviates from their peer group, enabling fraud detection within 24 hours, whereas other solutions take weeks or months. This proactive approach effectively eliminates repeated fraud offenders in higher-risk sectors, such as retail and financial services, reinforcing trust between the company and its clients. Fraud Data Analytics eliminates repeated fraud offenses in every environment. The heightened level of monitoring creates a significant deterrent effect, as agents recognize the increased oversight and are far less likely to engage in fraudulent behavior.

In addition to these internal security measures, TP takes a proactive stance against sophisticated cyber threats posed by external actors. The company has specifically strengthened its defenses against United States (US)-based cyber threat actors known for social engineering attacks. By enhancing identity verification protocols, improving agent security training, and implementing more robust access controls, the company mitigates potential vulnerabilities within its workforce effectively. TP's continuous improvement Project "Eagle Talon" was specifically launched to combat these threats, introducing FIDO2 keys for all privileged accounts. These keys prevent attackers from accessing administrator accounts, even

if a breach compromises the credentials. These countermeasures underscore the company's commitment to staying ahead of emerging threats and safeguarding client data from advanced cyber adversaries.

Frost & Sullivan recognizes TP's continuous leadership in security excellence for its multi-layered cybersecurity approach, which integrates automation, AI-driven fraud analytics, and proactive threat mitigation strategies. Its ability to adapt to evolving cyber threats while ensuring operational efficiency makes it a trusted partner for organizations requiring robust data protection solutions.

A Holistic Approach to Security: Compliance, Training, and Intelligence Sharing

TP integrates security compliance into its operational framework. The company holds the International Organization for Standardization 27001 and Payment Card Industry Data Security Standard certifications, which serve as baseline requirements for securing client data. Over the past year, TP underwent 654 security audits from clients, passing each without a single failure. These audits confirm adherence to industry regulations and contractual security obligations, which have become more stringent in recent years. This perfect track record underscores the company's commitment to maintaining the highest security standards in a rapidly evolving threat industry.

Recognizing that technology alone cannot secure an enterprise, TP emphasizes security awareness training. Its personnel undergo continuous education through phishing simulations, behavioral training, and specialized programs tailored to high-risk roles such as finance and software development. In 2024, the company conducted 1.2 million phishing tests, resulting in a low failure rate of 5.9%, significantly below industry averages.[4] Personnel who fall for simulated phishing attempts repeatedly receive targeted retraining, ensuring that security awareness remains a priority. By fostering a security-conscious culture, TP strengthens its human defenses against social engineering attacks, making its workforce an integral part of its security strategy.

Moreover, TP's commitment to security extends beyond its operations. The company collaborates actively with other business process outsourcing (BPO) providers to enhance industry-wide cybersecurity resilience. Through an informal Information Sharing and Analysis Center model, TP enables real-time cyber threat intelligence exchange, allowing BPO industry peers to respond proactively to emerging threats. Furthermore, the company leads client-focused security consortiums, where companies share best practices to strengthen their collective defenses. For example, TP facilitated a security consortium for a major healthcare client, uniting various BPO providers to optimize fraud prevention and intelligence sharing. The company's Cyber Threat Intelligence team aggregates security reports from all participating vendors, ensuring that when one provider detects a new attack vector, the entire consortium receives an alert.

Additionally, TP hosted a SIM swap fraud seminar in September 2024, bringing together nine major telecommunication clients and experts from the US Secret Service, Federal Communications Commission, Department of Justice, and CrowdStrike. With over 30 industry professionals in attendance, the seminar facilitated intelligence exchange and reinforced collaborative fraud prevention efforts. The company also provides continuous dark web monitoring for itself and its clients. A recent case demonstrated its

[4] Ibid.

effectiveness when TP's monitoring detected a phishing campaign against a major financial services client before attackers launched the attack. This early interception allowed the client to block access, preventing the phishing website from causing harm, reinforcing TP's reputation as a proactive security leader.

> *"TP continuously evolves its security strategy to stay ahead of emerging threats. The company's Project Eagle series enhances its security framework systematically by integrating cloud-based security monitoring, privileged access controls, and advanced fraud detection."*
>
> ***- Sebastian Menutti***
> ***Research Director, Customer Experience***

Client satisfaction metrics further validate the company's leadership in security. TP's CSAT score for compliance and security stands at 4.17 out of 5, surpassing many operational CSAT benchmarks.[5] This high rating reflects clients' confidence in the company's dedication to safeguarding their interactions and data.

Frost & Sullivan recognizes TP's dedication to security, driven by its commitment to operational excellence, compliance, security awareness, and industry collaboration. This commitment solidifies its reputation as a trusted partner in safeguarding customer interactions.

A Future-Proof Cybersecurity Framework

TP demonstrates its long-term commitment to security through sustained financial investment. Over the past five years, the company allocated over €50 million beyond standard security operating costs to advance its security infrastructure.[6] This investment represents 15.2% of total information technology (IT) expenditure, aligning with the budgets of major financial institutions.[7]

TP demonstrates its security effectiveness through its ability to maintain uninterrupted service delivery. The company has not experienced a single cybersecurity-related service disruption in the past year, a rare achievement in the industry. Even during large-scale cyber incidents, TP fully recovered within a matter of hours, while other organizations faced prolonged outages lasting weeks.[8] This remarkable recovery time highlights TP's highly automated and resilient IT infrastructure, which minimizes downtime and ensures continuous operations.

TP continuously evolves its security strategy to stay ahead of emerging threats. The company's Project Eagle series enhances its security framework systematically by integrating cloud-based security monitoring, privileged access controls, and advanced fraud detection. Early Eagle projects replaced outdated security platforms with a unified, cloud-based framework, allowing real-time threat detection across multiple IT environments. Project Eagle Eye strengthens security by focusing on protecting back-office applications such as Office 365, Salesforce, and Workday. The initiative includes activating improved security features, enforcing single sign-on and multi-factor authentication, and aggregating security logs into the global security operations center for anomaly detection.

[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid.

Moving forward, TP is preparing for the next wave of AI-driven security risks, including prompt injection attacks, model poisoning, and unauthorized AI usage. The company implements strict AI governance policies to counter these risks, blocking unauthorized generative AI tools while allowing secure internal AI deployments through Microsoft Copilot. By 2026, it plans to deploy Island. IO as the default secure enterprise browser for its nearly 490,000 employees, enhancing endpoint security and preventing unauthorized data access. TP maintains a state-of-the-art security infrastructure by aligning technology upgrades with a structured renewal cycle, ensuring continuous adaptation to cybersecurity advancements.

Conclusion

TP's commitment to fraud prevention and data protection positions it as a strong leader in cybersecurity. Through a combination of automation, AI-driven analytics, and proactive security strategies, the company creates a highly resilient framework capable of detecting and neutralizing threats before they escalate. Its investments in real-time monitoring and fraud prevention tools, such as TP Protect and Fraud Data Analytics, ensure swift detection and mitigation of internal and external threats. TP's collaborative approach, engaging with industry peers and regulatory bodies, further strengthens its security ecosystem and enhances collective defense against cyber threats. By integrating security compliance with employee training and intelligence-sharing initiatives, TP fosters a culture of vigilance that minimizes human risk factors. Its ability to recover from incidents rapidly and maintain uninterrupted service delivery underscores the effectiveness of its security infrastructure. As TP continues to innovate through projects such as Eagle Talon and Eagle Eye, it remains at the forefront of cybersecurity advancements.

With its strong overall performance, TP earns Frost & Sullivan's 2025 North American Company of the Year Recognition in the security in customer experience management industry.

What You Need to Know about the Company of the Year Recognition

Frost & Sullivan's Company of the Year Recognition is its top honor and recognizes the market participant that exemplifies visionary innovation, market-leading performance, and unmatched customer care.

Best Practices Recognition Analysis

For the Company of the Year Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Visionary Innovation & Performance

Addressing Unmet Needs: Customers' unmet or under-served needs are unearthed and addressed to create growth opportunities across the entire value chain

Visionary Scenarios Through Megatrends: Long-range scenarios are incorporated into the innovation strategy by leveraging mega trends and cutting-edge technologies, thereby accelerating the transformational growth journey

Leadership Focus: The company focuses on building a leadership position in core markets to create stiff barriers to entry for new competitors and enhance its future growth potential

Best Practices Implementation: Best-in-class implementation is characterized by processes, tools, or activities that generate consistent, repeatable, and scalable success

Financial Performance: Strong overall business performance is achieved by striking the optimal balance between investing in revenue growth and maximizing operating margin

Customer Impact

Price/Performance Value: Products or services offer the best ROI and superior value compared to similar market offerings

Customer Purchase Experience: Purchase experience with minimal friction and high transparency assures customers that they are buying the optimal solution to address both their needs and constraints

Customer Ownership Excellence: Products and solutions evolve continuously in sync with the customers' own growth journeys, engendering pride of ownership and enhanced customer experience

Customer Service Experience: Customer service is readily accessible and stress-free, and delivered with high quality, high availability, and fast response time

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty, which is regularly measured and confirmed through a high Net Promoter Score®

Best Practices Recognition Analytics Methodology

Inspire the World to Support True Leaders

This long-term process spans 12 months, beginning with the prioritization of the sector. It involves a rigorous approach that includes comprehensive scanning and analytics to identify key best practice trends. A dedicated team of analysts, advisors, coaches, and experts collaborates closely, ensuring thorough review and input. The goal is to maximize the company's long-term value by leveraging unique perspectives to support each Best Practice Recognition and identify meaningful transformation and impact.

		VALUE IMPACT	
STEP		WHAT	WHY
1	**Opportunity Universe**	Identify Sectors with the Greatest Impact on the Global Economy	Value to Economic Development
2	**Transformational Model**	Analyze Strategic Imperatives That Drive Transformation	Understand and Create a Winning Strategy
3	**Ecosystem**	Map Critical Value Chains	Comprehensive Community that Shapes the Sector
4	**Growth Generator**	Data Foundation That Provides Decision Support System	Spark Opportunities and Accelerate Decision-making
5	**Growth Opportunities**	Identify Opportunities Generated by Companies	Drive the Transformation of the Industry
6	**Frost Radar**	Benchmark Companies on Future Growth Potential	Identify Most Powerful Companies to Action
7	**Best Practices**	Identify Companies Achieving Best Practices in All Critical Perspectives	Inspire the World
8	**Companies to Action**	Tell Your Story to the World (BICEP*)	Ecosystem Community Supporting Future Success

*Board of Directors, Investors, Customers, Employees, Partners

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Generator™

Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.

Learn more.

Key Impacts:

- **Growth Pipeline:** *Continuous Flow of Growth Opportunities*
- **Growth Strategies:** *Proven Best Practices*
- **Innovation Culture:** *Optimized Customer Experience*
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** *Industry Leadership*



The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.

Analytical Perspectives:

- Megatrend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)

