FROST & SULLIVAN

BEST PRACTICES



2026 GLOBAL EMAIL SECURITY CUSTOMER VALUE LEADERSHIP

knowbe4

Table of Contents

Best Practices Criteria for World-Class Performance 3

The Transformation of the Email Security Industry 3

More Protection, Fewer Tools, Better Value 4

Driving Customer Value Through Simplicity and Integration 5

Conclusion 7

What You Need to Know about the Customer Value Leadership Recognition 8

Best Practices Recognition Analysis 8

Business Impact 8

Customer Impact 8

Best Practices Recognition Analytics Methodology 9

Inspire the World to Support True Leaders 9

About Frost & Sullivan 10

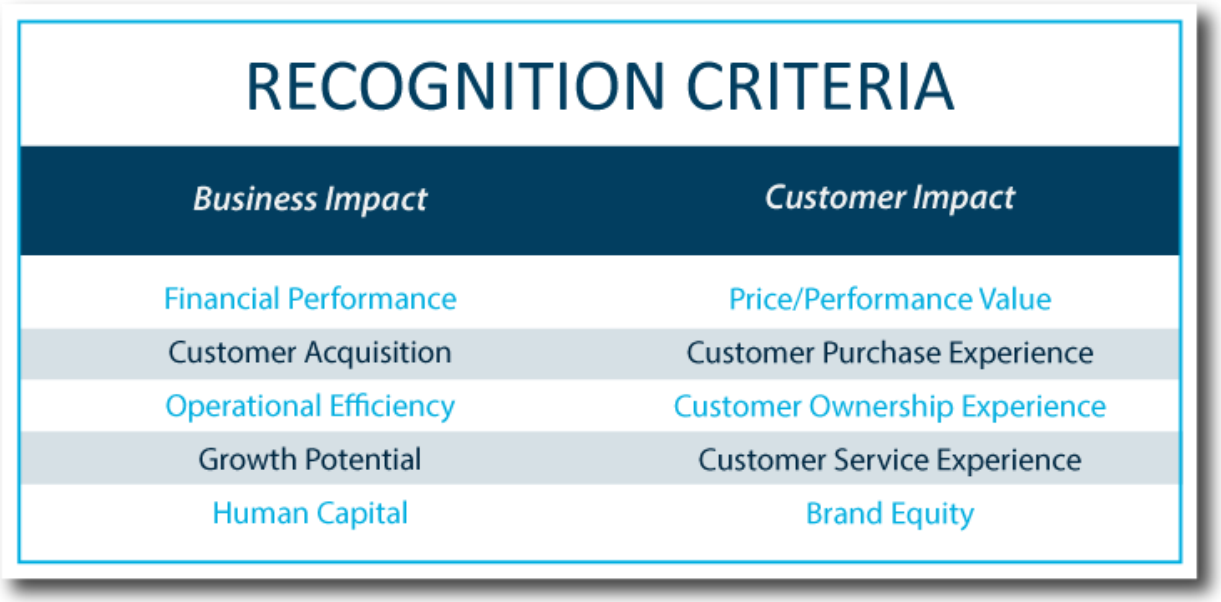
The Growth Pipeline Generator™ 10

The Innovation Generator™ 10

© Frost & Sullivan 2026

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. KnowBe4 excels in many of the criteria in the Email Security space.



The Transformation of the Email Security Industry

Email remains the most prevalent initial attack vector in modern cyber incidents. Phishing, business email compromise (BEC), credential harvesting, and accidental data exposure continue to exploit the human element of cybersecurity, making email security a critical control point for organizations worldwide. At the same time, the evolving threat landscape, characterized by AI-generated phishing campaigns, impersonation attacks, and compromised legitimate accounts, demands solutions that move beyond static detection models and signature-based approaches.

KnowBe4 has established itself as a global leader in addressing this challenge through its KnowBe4 Platform, which provides attack simulation and training, collaboration security, and agent security. The company has extended its longstanding expertise in security awareness and behavioral risk management into a comprehensive email protection framework that integrates inbound threat detection, outbound data protection, incident response automation, and real-time user coaching.–The core of the KnowBe4 platform is AIDA (Artificial Intelligence Defense Agents), the company's AI-powered security controls. Combining technical protection mechanisms with behavioral intelligence, KnowBe4 delivers a holistic approach to reducing human-driven cyber risk.

© Frost & Sullivan 2026

The company's email security portfolio—comprising Inbound Email Security, Outbound Email Security, Messaging Security, Incident Response (for PhishER)—operates as an integrated ecosystem rather than a set of standalone tools. Telemetry generated across these modules feeds dynamic risk scoring and adaptive training mechanisms, enabling organizations to identify vulnerabilities, respond to threats rapidly, and reinforce secure user behavior. This architecture reflects a broader shift in cybersecurity strategy: protecting the organization not only by blocking malicious activity but also by influencing user behavior at the moment risk occurs.

More Protection, Fewer Tools, Better Value

A Unified Platform to Secure the Digital Workforce

KnowBe4 differentiates itself in the email security market by tightly integrating technical protection with behavioral risk management. Rather than treating email filtering, user training, and incident response as separate security disciplines, the company combines them within a single HRM+ platform that continuously correlates user activity, threat intelligence, and policy enforcement.

The platform's core modules—Inbound Email Security, Outbound Email Security, Messaging Security, Incident Response (for PhishER)—share telemetry and contextual intelligence. This unified architecture enables organizations to identify threats more effectively and respond faster, while reinforcing secure user behavior through contextual guidance and adaptive training.

KnowBe4's integrated approach improves value for customers by reducing the need for multiple overlapping tools. Organizations can manage inbound phishing detection, outbound data protection, and security awareness workflows through a consolidated environment, simplifying security operations while improving protection against increasingly sophisticated attacks.

Advanced AI-Driven Detection Capabilities

At the core of KnowBe4's email security technology is its Agentic Detection Engine, which leverages natural language understanding, contextual machine learning, and social graph analysis to evaluate email messages as complete artifacts rather than isolated components. This approach allows the platform to detect subtle indicators of deception, impersonation, and emotional manipulation that traditional filtering techniques may overlook.

The system analyzes communication patterns, linguistic cues, and behavioral anomalies to identify suspicious messages, even when they originate from compromised legitimate accounts. By incorporating large-scale phishing data and adversarial AI testing, the platform continuously refines detection models to keep pace with emerging attack techniques.

Through this advanced detection capability, KnowBe4 delivers strong price–performance value by reducing false positives while maintaining high detection accuracy. Organizations benefit from reliable protection against phishing and social engineering attacks without overwhelming users or security teams with excessive alerts.

Real-Time Behavioral Intervention and User Guidance

Another key differentiator is KnowBe4's use of contextual prompts and behavioral nudges to influence user decisions during risky interactions. When a suspicious email is detected, the platform surfaces risk indicators directly to the user through contextual banners that explain the nature of the threat in clear language.

Similarly, outbound controls notify users when they attempt to send sensitive information to unusual recipients or external domains. These real-time interventions help prevent accidental data exposure and reinforce security awareness at the moment risk occurs.

This human-centric approach improves long-term security outcomes by transforming every detection event into an opportunity for user education. Over time, organizations see measurable improvements in phishing reporting rates, data-handling practices, and overall employee security awareness.

Driving Customer Value Through Simplicity and Integration

Seamless Integration with Existing Security Ecosystems

KnowBe4 has designed its email security platform to integrate seamlessly with widely adopted enterprise environments, particularly Microsoft 365. As a launch partner with Microsoft's Integrated Cloud Email Security (ICES) program, KnowBe4 manages post-delivery remediation directly within Microsoft's unified quarantine framework.

> *"KnowBe4 has designed its email security platform to integrate seamlessly with widely adopted enterprise environments, particularly Microsoft 365. Participation in Microsoft's Integrated Cloud Email Security (ICES) program enables KnowBe4 to manage post-delivery remediation directly within Microsoft's unified quarantine framework."*
>
> ***- Claudio Stahnke,***
> ***Senior Industry Analyst***

This integration allows security teams to remediate threats quickly while maintaining a consistent user experience within the Microsoft environment. Organizations can enhance the capabilities of native Microsoft security controls without replacing them, enabling a layered defense strategy that is both practical and efficient.

By aligning closely with existing productivity platforms, KnowBe4 minimizes deployment complexity and accelerates time to value for customers.

Simplified Procurement and Platform Consolidation

Another important contributor to customer value is KnowBe4's platform consolidation strategy. Many organizations face operational challenges caused by fragmented security toolsets that require separate procurement processes, integrations, and management workflows.

KnowBe4 addresses this challenge by unifying multiple human risk management capabilities within a single vendor ecosystem. Customers can deploy email protection, phishing response automation, security awareness training, and behavioral analytics through one integrated platform.

This consolidation reduces operational overhead, simplifies vendor management, and ensures that security teams have a consistent view of human risk across their organizations.

Strong Customer Support and Ownership Experience

> *"KnowBe4 continues to invest in innovation to address emerging cybersecurity challenges. Future platform enhancements focus on expanding protection beyond email into collaboration platforms and messaging environments where phishing and impersonation attacks increasingly originate."*
>
> ***- Claudio Stahnke, Senior Industry Analyst***

KnowBe4 complements its technology with a strong customer success model designed to ensure organizations achieve maximum value from the platform. The company provides extensive onboarding resources, ongoing training, and responsive technical support to help customers deploy and operate its solutions effectively.

These services contribute to a positive ownership experience, enabling organizations to adapt the platform to their specific security requirements while maintaining consistent operational performance.

Innovation That Keeps the Growth Engine Running

Expanding Global Adoption Across Key Industries

KnowBe4 has experienced strong growth in the email security market by leveraging its extensive customer base in security awareness training. The company now serves tens of thousands of organizations worldwide, spanning industries such as government, healthcare, financial services, education, and technology. These sectors are particularly vulnerable to social engineering attacks and data exposure risks, making the integration of technical protection and behavioral intelligence especially valuable.

By addressing both technical and human vulnerabilities, KnowBe4 delivers a differentiated solution that resonates with organizations seeking comprehensive protection against phishing and insider threats.

Strategic Platform Expansion Following the Egress Acquisition

A key milestone in KnowBe4's growth strategy was the acquisition of Egress, which accelerated the company's entry into the email security market. The integration of Egress technology has enabled KnowBe4 to deliver a mature cloud email security solution while preserving the company's focus on human risk management.

Customers benefited from a smooth transition following the acquisition, with continued service quality and platform usability throughout the integration process. This stability reinforced customer confidence and strengthened KnowBe4's reputation as a reliable cybersecurity partner.

Continuous Innovation and Future Growth Potential

KnowBe4 continues to invest in innovation to address emerging cybersecurity challenges. Future platform enhancements focus on expanding protection beyond email into collaboration platforms and messaging environments where phishing and impersonation attacks increasingly originate.

This multi-channel protection strategy will extend KnowBe4's behavioral risk management approach to additional communication channels, enabling organizations to address human-driven threats wherever they occur.

By maintaining a strong focus on customer outcomes, platform cohesion, and technological innovation, KnowBe4 is well-positioned to sustain its growth trajectory in the global email security market.

Conclusion

KnowBe4 has demonstrated exceptional performance in delivering customer value through its innovative approach to email security. By combining advanced AI-driven threat detection with behavioral intelligence and real-time user guidance, the company addresses one of the most persistent challenges in cybersecurity: the human element.

The integration of inbound threat protection, outbound data loss prevention, encryption, and incident response automation within a unified platform enables organizations to simplify security operations while improving protection against phishing and social engineering attacks. At the same time, KnowBe4's strong ecosystem integrations, customer-focused support model, and commitment to continuous innovation ensure that customers can deploy and operate its solutions efficiently.

Through its Human Risk Management platform and expanding email security capabilities, KnowBe4 has successfully bridged the gap between technical defense and behavioral security. This holistic approach not only strengthens organizations' ability to detect and respond to threats but also fosters lasting improvements in user awareness and security culture.

KnowBe4 earns Frost & Sullivan's 2026 Global Customer Value Leadership Recognition for its strong overall performance in the Email Security industry.

© Frost & Sullivan 2026

What You Need to Know about the Customer Value Leadership Recognition

Frost & Sullivan's Customer Value Leadership Recognition identifies the company that offers products or services customers find superior for the overall price, performance, and quality.

Best Practices Recognition Analysis

For the Customer Value Leadership Recognition, Frost & Sullivan analysts independently evaluated the criteria listed below.

Business Impact

Financial Performance: Strong overall business performance is achieved in terms of revenue, revenue growth, operating margin, and other key financial metrics

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Leveraging innovative technology characterizes the company culture, which enhances employee morale and retention

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®

© Frost & Sullivan 2026

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

© Frost & Sullivan 2026

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 fueled 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)

