SafeBreach Recognized as the

2021

Company of the Year

Global Breach and
Attack Simulation Market

Excellence in Best Practices

FROST & SULLIVAN

Strategic Imperatives

Frost & Sullivan identifies three key strategic imperatives that impact the cybersecurity industry: innovative business models, disruptive technologies, and transformative Mega Trends. Every company that is competing in the cybersecurity space is obligated to address these imperatives proactively; failing to do so will almost certainly lead to stagnation or decline. Successful companies overcome the challenges posed by these imperatives and leverage them to drive innovation and growth. Frost & Sullivan's recognition of SafeBreach is a reflection of how well it is performing against the backdrop of these imperatives.

THE IMPACT OF THE STRATEGIC IMPERATIVE 8™ ON THE CYBERSECURITY INDUSTRY

The following 3 strategic imperatives will ensure growth in the cybersecurity industry.

SI8	INNOVATIVE BUSINESS MODELS	DISRUPTIVE TECHNOLOGIES	TRANSFORMATIVE MEGA TRENDS
Why	• In an ever-changing threat landscape, end users want scalability and flexibility in their cybersecurity strategy. • Service providers have started to transition to cybersecurity-as-a-service models to integrate pricing flexibility. • A service-based approach to cybersecurity has given rise to new models such as assessment-as-a-service, and cybersecurity as a separate core functional area.	• Continuous authentication and encryption, data de-identification services, blockchain, and biometrics are being used for threat prevention. • Social media platforms are leveraging artificial intelligence (AI) and machine learning (ML) algorithms to automatically detect, isolate, and warn subscribers to prevent data breaches and misinformation. • Deepfake technology, quantum computing, 5G, and the IoT will drive strong growth opportunities but also host numerous vulnerabilities.	• The use of IoT-connected devices poses vulnerabilities for enterprises and customers. • With the rising IoT threat landscape and evolving cyber regulations, cybersecurity will emerge as an organization-wide approach with active involvement from the board, rather than merely an IT function. • Core cybersecurity responsibilities are becoming more prominent across businesses, with expertise in the roles of chief information officer, chief information security officer, chief technology officer, and chief cybersecurity officer.
When	• Service providers will focus on lowering the overall cost of ownership and reducing complexity through cybersecurity-as-a-service approaches. • End users will prefer tailored cybersecurity services that allow for periodic realignment to suit company needs and threat possibilities. • With additional opportunities in data monetization, individuals will seek data anonymization and de-identification services in the next 3 to 5 years.	• Revenue from ICT cyber benefits are expected to reach $180 trillion by 2030. Growth will be driven by the IoT, AI, Big Data analytics, and the sophistication of cyberattacks. • User behavior analytics, encryption, cloud, and deep learning will play significant roles in market growth for the next 5 to 10 years.	• Demand for cybersecurity services will be driven by the significant increase in the number of smart/connected devices and users. • By 2030, Asia-Pacific is expected to have the highest market revenue growth for cybersecurity solutions. • Security solutions will be a priority for private financial and banking services and for critical healthcare and aerospace and defense services.

Source: Frost & Sullivan

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each of the nominated companies. SafeBreach excels in many of the criteria in the Global Breach and Attack Simulation (BAS) space.

A Platform to Address Customer Pain Points

System vulnerabilities, ransomware, and advanced persistent threats (APTs) were the most prominent cybersecurity concerns identified by a recent Frost & Sullivan survey of 881 IT and security professionals. These statistics confirm that cyber adversaries are relentless in gaining access to enterprise networks and rapidly morph their tactics.

Chief Information Security Officers (CISOs) commonly invest in multiple security technologies to identify or address the latest security vulnerabilities. Such a disparate and siloed approach to security seldom provides a holistic view of an organization's security posture. Thus, a state of anxiety prevails in the security operations center (SOC), despite the significant time, money, and resources invested in security technologies.

Despite having an extensive security stack that addresses the latest vulnerabilities, many organizations experience a data breach or ransomware attack at some point. Cyber adversaries exploit misconfigurations and gaps in security controls to gain access and move laterally inside the network. Consequently, holistic visibility into the integrated impact of security controls across an organization is a top priority.

Maintaining a constant vigil with regards to an enterprise's network security readiness is an essential first step toward strengthening defenses. Enterprises use multiple mechanisms such as penetration testing, vulnerability scanning, and red teaming to assess their security readiness. Breach and attack simulation (BAS) is a recent entrant to the pool of security assessment mechanisms that aims to offset its predecessors' deficiencies. BAS tools take the cyber adversary's position, offering organizations a contextualized view of critical security risks.

"With 20,000+ breach and attack methods, SafeBreach provides comprehensive attack coverage. The company offers a feature-rich portfolio that includes remediation capabilities and integration with downstream applications. This, in turn, helps boost its annual recurring revenue from a loyal customer base."

- Swetha R K, Industry Analyst, Cybersecurity Practice

SafeBreach, founded in 2014, is one of the pioneers of the breach and attack simulation (BAS) market. The company is headquartered in Sunnyvale, California, and has its research and development Centre in Tel Aviv, Israel.

SafeBreach aims to transform the way that the industry approaches security operations. The company envisions a situation where security leaders will use their security technologies to the fullest instead of buying new tools every year and not using them to their full extent. With SafeBreach, security leaders are able to report, in real-time, on the organization's security posture with a prioritized list of action points and will be able to drive risk down based on where the greatest impact to the business is.

SafeBreach's feature-rich platform helps companies to validate their security controls, improve security posture and drive risk down on a continuous basis. The platform triggers security controls by running thousands of known threat indicators and attacking behaviors safely and continuously. In addition to a library of 20,000+ attack methods and tactics and growing every day, techniques, and procedures (TTP), customers can also build custom attack methods to test their defenses. The platform includes an extensive and flexible Hackers Playbook™ from which the SOC team can select the most relevant APT groups and run simulations with the click of a button.

The United States Computer Emergency Readiness Team (US-CERT) periodically publishes alerts on emerging threats, malware types, and attack methods. Within 24 hours, SafeBreach adds these attack methods into its playbook. Customers can run attack methods and send a full report to the board very quickly.

SafeBreach does not stop at running the attacks and generating a report. The company recognizes that running thousands of attack methods of various threat actors and malware types will generate vast data volumes. The SOC team can visualize the results from the simulations to understand multiple exposures. The platform provides the customers with the flexibility to visualize the data in different ways:

- A heat map of the enterprise security posture mapped to each of the TTPs of the MITRE ATT&CK framework
- Risk scoring across the enterprise that shows any configuration changes that may expose the organization to different risks
- Explorer view of the kill chain that shows the cyber adversary's perspective of how many different ways an adversary can move inside the network and steal data
- Flexible dashboarding which allows the organisation to generate both executive and operational reports in a way which aligns with their business goals and KPIs.

SafeBreach helps customers reduce the risk and maximize the value gained from the security stack within a business context. Customers can quantify risk based on business impact, set goals for reducing risk, identify and build a data-driven strategy to reach the goals, and track progress. Such features help companies make investment decisions in a business context and identify risk-to-revenue benefits based on a business units' security posture. Further, security teams can communicate clear KPIs to the board to show security program effectiveness in reducing risk systematically and justify spending based on outcome-driven metrics.

SafeBreach supports five different use cases within the breach and attack simulation product space:

Security control validation – This use case includes attack methods that validate controls across environments such as SIEM, endpoint, cloud, container, network, web, and email. The customer can also evaluate a new tool such as an endpoint solution or firewall in a controlled environment to understand the return on investment of their security stack.

Mergers and acquisitions – In this use case, customer planning for an M&A deal can drop simulations in the other company's IT environment to understand its cyber risk posture and potential security liability and thus support the right business decisions.

Risk-based vulnerability management – SafeBreach enables its customers to expand the capability of existing vulnerability assessment tools. It correlates the vulnerability scans with validating security controls to gain insight into which vulnerabilities are actually exploitable in their environment and prioritize patching and remediation.

Threat assessment – This use case helps customers to understand the organization's security posture against a threat of interest. This can be visualized from the perspective of the MITRE ATT&CK framework, threat phases and scenarios, and the explorer view of the kill chain.

Cloud Native Security - This use case helps customers validate cloud and container security by executing attacks that test their cloud control (CSPM) and data (CWPP) planes to ensure the security of their critical cloud operators.

A Robust Innovation Pipeline to Sustain Growth

SafeBreach Labs, with its dedicated team of researchers and cybersecurity experts, continuously expands the playbook with new emerging threats and attack methods. In 2020, the team expanded the attack playbook with 10,000+ additional attack methods covering even cloud and container environments.

In addition, SafeBreach makes a significant contribution to the TTP of the MITRE ATT&CK framework. Itzik Kotler, SafeBreach's Co-founder and CTO, has contributed to four techniques published in the MITRE ATT&CK framework. SafeBreach's platform can help the customer test its security posture against the framework's complete layout of tactics, techniques, and sub techniques.

SafeBreach has leveraged strategic partnerships to expand its customer base and improve product capabilities. For instance, key strategic partners leveraging tight integrations with SafeBreach are IBM, Microsoft, and Palo Alto Networks.

- **IBM** for training exercises at IBM's innovative Security Command Center XFORCE. The company partnered with IBM for training exercises at IBM's innovative Security Command Center X-FORCE. Operated by IBM's elite X-Force security training and incident response team, the Cyber Range is a state-of-the-art simulation and training center run by IBM Security. Their Cyber Range strives to immerse customers in simulated cyber attacks to train them on how to prepare for, respond to, and manage a broad range of real-world information security risk scenarios.
- **Microsoft** uses SafeBreach to execute attack techniques for users to effectively validate the security efficacy against Microsoft Defender for Endpoint in the Microsoft Evaluation Lab.
- **Palo Alto Networks**: SafeBreach is the only BAS vendor that was chosen for the Palo Alto Network Cortex XSOAR Marketplace launch of ecosystem experts that rapidly address new automation use cases. The integration enables full automation of IOCs and orchestrates the BIOCs (behavioral indicators of compromise) that SafeBreach has safely validated breached the organization.

The SafeBreach platform also integrates with the customer's existing vulnerability management tools to identify exploitable vulnerabilities. A detailed priority list based on what is exploitable helps customers to identify prioritized action points. The prioritized list helps companies correlate all of the data to visualize the value of making a specific change in the environment. Depending on the requirement, the customer can choose from various vulnerability prioritization levels such as attack surface, external access, exposure, critical segments, or critical segments access. SafeBreach provides the SOC team with action items that enable the creation of a prioritized list of vulnerabilities based on business impact.

SafeBreach takes a multi-pronged approach to provide the best customer experience. For instance, as part of its customer success program, the company assigns a dedicated customer success manager for the contract's entire duration. The program's goal is to help customers to realize the full potential and value of SafeBreach’s solution and provide deployment assistance, strategy consultations, and technical support.

In turn, the customer success program helps SafeBreach to receive periodic product feedback directly from different user profiles in the customer organization. The customer success team organizes Quarterly Business Reviews (QBRs), which helps to obtain high-level feedback, resulting in a targeted tracking list of every customer's features. The company then registers the input into its ticket management system and incorporates it in the product development process.

SafeBreach's customer support portal has a well-structured case ticket registration and management workflow for all customers and partners for break-fix and other product issues. The support portal has direct integration with the R&D bug tracking system to provide statistics on the defects of different platform modules, which are reviewed by the R&D team every day. The company offers precise resolution times and commitments to the customer for each request.

Market Leadership through Aggressive Expansion

In April 2020, SafeBreach secured $19 million in Series C funding to accelerate product development and expand sales channel partnership growth. The company has partnered with a leading MSSP to demonstrate the effectiveness of the MSSP's offerings using SafeBreach's platform. In addition, SafeBreach has partnerships with value-added resellers across the world to expand its customer base.

Feature-rich platform capabilities, comprehensive use-case coverage, and aggressive expansion efforts have helped SafeBreach to exhibit strong financial performance in 2020. Based on Frost & Sullivan's analysis, the company holds a market-leading 18.9% share of the global BAS market in 2020. SafeBreach has a strong revenue growth pipeline, thanks to its aggressive efforts to establish its presence in multiple verticals and regions. The company derives at least two-third of its revenue from these new opportunities.

Conclusion

With the ever-increasing volume of threats and digitized IT landscape, businesses deal with an overwhelming number of security controls. Often, security leaders suffer from a lack of visibility with regards to how different security controls work together to mitigate risk. Consequently, security leaders need to generate a focused, contextualized, and business-driven view of the organization's top risks and threats, coupled with a clear and prioritized mitigation plan in order to systematically drive risk down.

SafeBreach's platform creates synergy between disparate security solutions to reveal an organization's actual risk and promote cross-functional mitigation efficiency. A combination of research-backed product development, an aggressive new market expansion strategy, and superior customer experience focus has helped the company to expand its market share and strengthen its position

For its strong overall performance, SafeBreach has earned Frost & Sullivan’s 2021 Company of the Year Award.

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

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

Best Practices Award Analysis

For the Company of the Year Award, 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 by a robust solution development process

Visionary Scenarios Through Mega Trends: Long-range, macro-level scenarios are incorporated into the innovation strategy through the use of Mega Trends, thereby enabling first to market solutions and new growth opportunities

Leadership Focus: Company focuses on building a leadership position in core markets and on creating stiff barriers to entry for new competitors

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

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

Customer Impact

Price/Performance Value: Products or services provide the best value for the price compared to similar market offerings

Customer Purchase Experience: Quality of the purchase experience assures customers that they are buying the optimal solution for addressing their unique needs and constraints

Customer Ownership Experience: Customers proudly 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 high quality

Brand Equity: Customers perceive the brand positively and exhibit high brand loyalty

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 Engine™

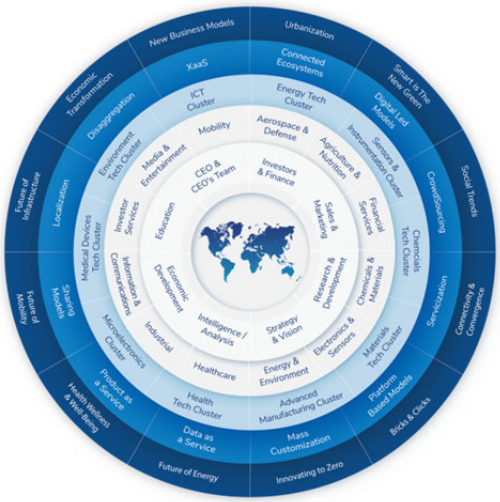
Frost & Sullivan's proprietary model to systematically create on-going growth opportunities and strategies for our clients is fuelled by the Innovation Generator™. Learn more.

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 six 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:

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