

*Powering clients to a future shaped by growth*

A Frost & Sullivan White Paper

# Continuous Security Validation with Highly Innovative Breach & Attack Simulation Technology

Swetha Krishnamoorthi  
Industry Analyst, Cybersecurity

In Partnership with




## Table of Contents

---

<b>3</b>	Know Your Enemy with Breach and Attack Simulation
<b>4</b>	Breach & Attack Simulation: Why is it Necessary?
<b>5</b>	Executive-Level and Operational-Level Business Challenges
<b>9</b>	Navigating the Threat Landscape Using Security Control Validation
<b>12</b>	Cymulate: Company Philosophy
<b>14</b>	The Final Word
<b>15</b>	Endnotes

## Know Your Enemy with Breach and Attack Simulation



“To know your  
enemy, you  
must become  
your enemy.”

—The Art of War,  
Sun Tzu

Today, chief information security officers (CISOs) realize the significance of Sun Tzu's strategy in the wake of heightened cyberattack levels. Cyber adversaries are relentless in identifying the smallest vulnerability to gain access to enterprise networks. As a consequence, defensive security is no longer sufficient. It is critical to think from the cyber adversary's perspective to proactively defend the organization from an attack.

Breach and attack simulation (BAS) tools have recently gained popularity because they can help enterprises test their security resiliency by running simulations of cyberattacks on their IT infrastructure. Frost & Sullivan research on the global BAS market shows the technology is gaining acceptance.

The competitive landscape of an emerging market such as BAS presents exciting dynamics. Frost & Sullivan expects adoption to improve further and forecasts a compound annual growth rate of 35% between 2020 and 2024.

Cymulate, a leader in innovation and a noteworthy vendor, has strengthened its BAS market position within just four years of operation. The company received the highest score on the Frost Radar innovation index, a competitive benchmarking tool.<sup>1</sup> Understanding the customer's pain points around managing an organization's security infrastructure and posture has led Cymulate to develop a continuous security validation platform with significant BAS features. As a result, the company achieved a high growth rate to become one of the top global BAS market leaders. Following an in-depth analysis of the BAS market, Frost & Sullivan also recognized Cymulate with the 2021 Best Practices Product Leadership Award.

## Breach & Attack Simulation: Why is it Necessary?

One of the key factors driving the demand for continuous security assessment and validation is the rapid evolution of the threat landscape. The SolarWinds attack that also impacted FireEye in December 2020<sup>2</sup> shows that security vendors and large organizations with robust security controls and policies can fall victim to cyber adversaries.

For many organizations, the goal for the first half of 2020 was to digitally transform their business operations or risk going out of business. Frost & Sullivan's 2020 Cloud User Survey found that multi-cloud adoption increased by 54%.<sup>3</sup> As employees and consumers connect with companies through multiple touchpoints, the attack surface expands. With various devices and applications connecting and disconnecting from the IT infrastructure, enterprise networks are in a constant state of change. Such dynamic network infrastructure calls for security controls and policy updates in real-time.

Yet, most enterprises find it hard to pinpoint security vulnerabilities in real-time. The lack of skilled security professionals is a significant factor limiting the capabilities of enterprise security teams. An estimated 4 million unfilled cybersecurity positions were available globally, according to a report<sup>4</sup> by (ISC)<sup>2</sup>.

The skills shortage has led many organizations to increase cybersecurity spending on technologies that claim to be the silver bullet for specific security challenges.<sup>5</sup> Unfortunately, this has led to disjointed security architecture in many enterprises, resulting in a deluge of data and alerts for security analysts, which prompts them to divert their attention without sufficient context or a holistic perspective of the organization's security posture.

“It is challenging to see the big picture in a multi-layered security environment and simultaneously gauge each tool's effectiveness. Despite the increase in security spending, CISOs and security teams are frequently unable to comprehensively understand and measure an organization's security readiness in real-time.”

BAS tools provide organizations an automated, continuous, simple, and effective methodology to assess security posture drift in real-time, enabling security teams to defend infrastructure from exploits proactively. BAS tools are an alternative to traditional security posture assessment mechanisms such as penetration testing, red team exercises, security audits, and vulnerability assessment. BAS tools can act like an actual attacker while avoiding collateral damage to business systems.

## Executive-Level and Operational-Level Business Challenges

The role of the CISO has evolved beyond just securing an organization's IT infrastructure. In addition to protecting the enterprise from the rapidly changing threat landscape, the CISO plays a vital role as a business enabler.

Transition to cloud-based services, mobility, and connected devices is necessary for businesses today, as witnessed by the large-scale digital transformation projects C-Suite executives (CXOs) undertook in the wake of the COVID-19 pandemic. At the same time, business transformation without addressing the security risks can cost the companies dearly.

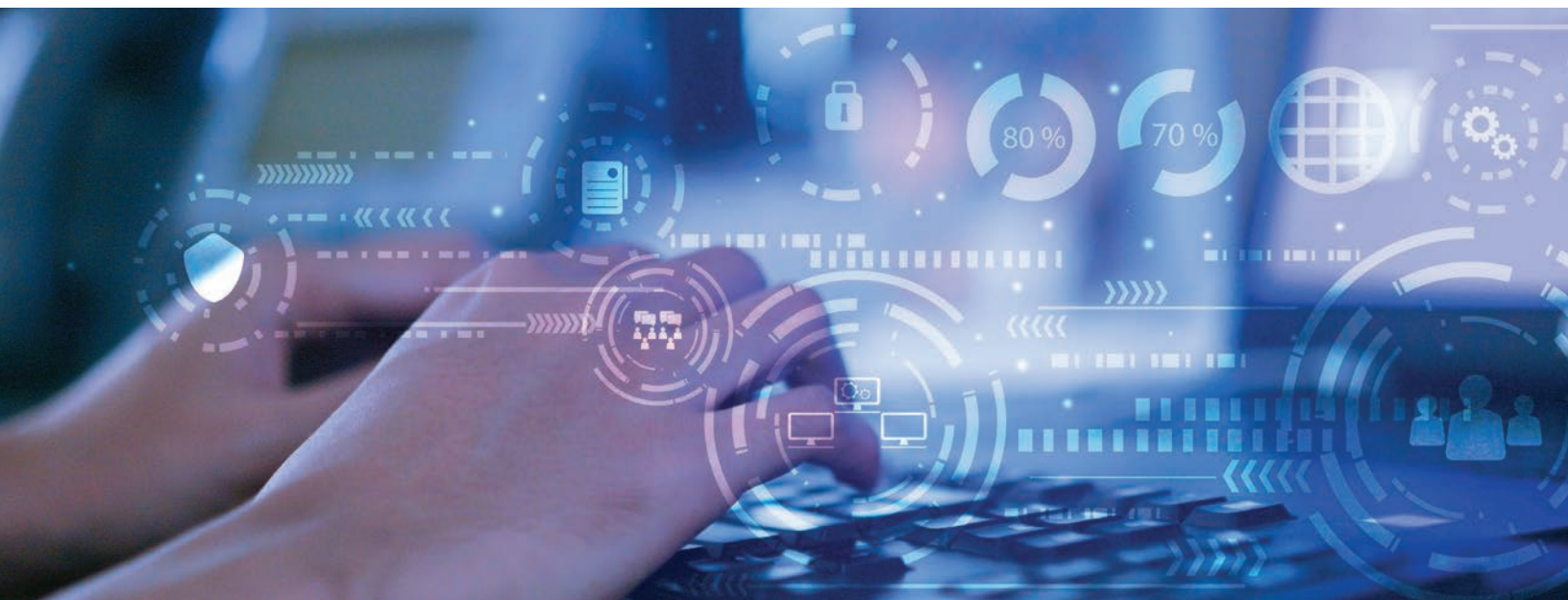
For instance, data breaches are the second-highest cause of brand reputation loss, behind poor customer service, according to a Frost & Sullivan survey of IT professionals. Even business executives acknowledge a strong negative impact on business results after public disclosure of a data breach.

Although board members demand regular updates on the company's security posture, security leaders are challenged to provide quantitative measures of the risk levels across the organization.

Similarly, a business's cyber risk level is a crucial factor influencing merger and acquisition (M&A) deals between companies. Therefore, business leaders require holistic and real-time visibility of companies' security readiness to understand the strengths and weaknesses of each organization.

Security leaders need to establish clear key performance indicators (KPIs) to quantify security performance like any other business department. A holistic view of risk exposure and security readiness level across the organization is a must-have for organizations of all sizes.

However, this is not an easy feat to achieve. Security teams need to address multiple challenges to satisfy the business requirements of all stakeholders.





## The Problem of Plenty

System vulnerabilities, ransomware, and advanced persistent threats (APTs) were the most prominent cybersecurity concerns identified by a Frost & Sullivan survey of 881 IT and security professionals. Cyber adversaries use sophisticated tools and are relentless in their pursuit of sensitive data from organizations.

The security architecture of most large enterprises includes an average of 130 different security tools. The result is that enterprises have numerous tools addressing similar challenges with overlapping capabilities. Instead of enriching the organization's defense and response capabilities, patchwork security architecture presents its own set of challenges.

Unlike security teams in organizations with fragmented security architectures, cyber adversaries are not limited by siloed technology teams and lines of business. While workflows and data move freely between applications, security controls protecting them seldom talk to each other. The lack of integrated security controls and holistic visibility across the network leads to security blind spots.

Cyber adversaries identify vulnerabilities and leverage multiple attack paths to access specific enterprise network assets. In most cases, cyber adversaries burrow deep into the network, hide their presence, and move laterally across the environment to access critical assets. A fractured infrastructure allows cyber adversaries to hide their presence in the gaps between control systems to evade detection.



“The result is that organizations’ security spending increases without a significant measurable impact on risk readiness levels. Meanwhile, security teams struggle to identify and eliminate tools that are no longer fit for purpose. A lack of contextual understanding of cyber risk levels provides opportunities for cyber adversaries in all organizations.”

## Growing Volume of Threats

Organizations face a combination of threats and attack pathways so large that it has become a daunting task for security professionals to assess an organization's risk level with confidence. As new threats are discovered almost daily, accurate risk assessments are challenging, time-consuming and expensive.

Manual security assessment techniques such as penetration (pen) testing or red team exercises lack the scale and thoroughness required by organizations. Further, manual verification of risk against a known library of threats is time-intensive, so identifying exploitable and relevant vulnerabilities becomes a combination of luck and skill that lacks consistency.

## Scalability of Assessments and Scarcity of Resources

A cyber adversary's ability to attack or access business-critical assets is directly related to the security posture of an enterprise network. However, the high volume of user activity across numerous endpoints intensifies the challenge of identifying issues that could unintentionally increase the organization's cyber risk and allow cyber adversaries to slip by undetected.








Most security teams are resource-constrained and juggling multiple responsibilities, so scheduling pen testing exercises depends on internal analysts' availability, ultimately limiting the frequency to once or twice a year.

Moreover, a large network with diverse applications, devices, and systems requires more time for a manual penetration testing team, which means higher internal and external costs. A single penetration testing exercise can cost between \$10,000 and \$100,000, depending on the scope. Therefore, manual penetration testing procedures only focus on a specific asset or segment of the organizational network at a particular point in time.

Sometimes, penetration testing is limited to specific attack scenarios, which forces an enterprise to pay more to test for additional scenarios. Thus, budgetary constraints provide security teams with narrow and frozen snapshots in time from a subset of a much larger IT infrastructure.

Following the risk assessment, the process of identifying and patching vulnerabilities for a large organization is a huge task. Even with a dedicated team to fix vulnerabilities, there is a high probability that the organization will struggle to address everything. As a result, security teams often focus on issues they perceive will have a higher impact on cyber risk reduction.

Understaffed security teams monitoring several security tools is common but generates dangerous levels of alert fatigue. While manual testing procedures can identify exploitable vulnerabilities, they add to an already overwhelmed security team's workload. Remediation of the identified vulnerabilities can take weeks or months, rendering the penetration testing exercise less effective.

	BAS	PENETRATION TESTING
 <b>NETWORK COVERAGE</b>	Can run attack simulations across the entire network simultaneously.	Can run attack simulations for a small part of the network or specific asset groups.
 <b>ASSESSMENT FREQUENCY</b>	Can be performed 24x7x365.	Typically implemented two or three times a year and gives a point-in-time snapshot of the security posture.
 <b>DEGREE OF AUTOMATION</b>	Most tools run fully automated simulations with minimal human involvement.	It relies entirely on the capabilities of human pen testers with assistance from hacking toolsets.
 <b>THREAT/ ATTACK COVERAGE</b>	BAS vendors have threat intelligence researchers and expert penetration testers who design and update out-of-the-box attack simulations that reduce cost and time for customers.	Attack scenarios simulated are limited to the pen tester's expertise; analysis and results can vary.
 <b>MITIGATION SPEED</b>	Most BAS tools provide remediation guidance and can be integrated with SIEM or SOAR to facilitate mitigation steps.	Security teams need to read through pen test reports and validate the findings; hence, it takes longer to initiate mitigation steps.
 <b>SAFETY</b>	Safety is non-disruptive to the production environment.	The probability of disruption or damage is high; it could leave a trail for attackers to exploit.
 <b>COST</b>	An annual subscription of BAS can cost at least 2.5 times less than a bi-annual penetration testing exercise for a large enterprise and at least 4X less expensive for an SME. BAS gives continuous and real-time security assessments.	Despite the higher spend, the pen test can only offer a point-in-time view of the enterprise's security posture, which becomes ineffective in the face of a dynamic IT and business environment.



## Navigating the Threat Landscape Using Security Control Validation

---

Businesses increasingly demand automated and continuous security testing techniques to reduce cyber risk. Breach and attack simulation (BAS) tools take the cyber adversary's perspective and run multiple attack scenarios across a network. Continuous BAS allows CISOs and security teams to keep their finger on the organization's security pulse in real-time without compromising critical production environments. Advanced BAS tools include a visual map of exposed endpoints, servers, or systems for the security team to quickly understand all vulnerable paths. This allows security teams to pinpoint choke points and fix vulnerabilities as they arise to maintain a higher security hygiene level than was previously possible.

The power and versatility of BAS tools help organizations use them for multiple use cases in addition to its broader intended application—risk assessment. Some of the popular use cases of BAS tools are described below.

### Intelligent Investigation

Security analysts require contextual intelligence that sheds light on how likely a threat would impact an organization, the attack pathways that can be exploited, and the effectiveness of protective measures in place. The ability to quantify risk exposure to threats in real-time helps security teams effectively optimize resource utilization.

Leveraging threat intelligence platforms is a smarter approach to risk assessments. Organizations can check their infrastructure against an extensive database of threats updated daily. Threat intelligence-led assessments enable security analysts to correlate threats with operational activity data to take the guesswork out of their analysis. This approach allows organizations to decide to consolidate, replace, or optimize existing security controls.

BAS tools typically leverage a commercial threat intelligence platform or integrate with the customer's internal threat intelligence feeds. Organizations can test their security controls by running simulations of new and emerging threats. Some BAS vendors, such as Cymulate, can run automated assessments against new threats as soon as they are identified in the wild.

Moreover, integrating BAS tools with vulnerability management tools allows organizations to triage based on the criticality of assets, potential impact, and effectiveness of compensating controls. Security teams get a comprehensive report that lists indicators of compromise (IoCs) and prioritizes them by risk level and recommended countermeasures.

With an advanced BAS solution, the dashboard will recommend subsequent remediation actions and integrate with security information and event management (SIEM) or security orchestration and response (SOAR) platforms.

## Simplified Security Stack

CISOs have limited security budgets, so they need to identify the indispensable tools that give holistic protection and optimize their security spending. BAS tools are used to gauge the efficacy of security tools against a specific threat or attack pathway so a CISO can make informed product investment decisions.

BAS tools leverage automation to reduce the time a security analyst takes to manage, monitor, and analyze data. By testing all attack pathways and producing a comprehensive and prioritized report of vulnerabilities and action items, security analysts can rapidly and efficiently improve an organizations' security posture.

BAS tools also play a role in M&A due diligence assessments of the cyber risk of companies being acquired. Running a BAS assessment on a companies' security architecture will reveal security gaps and highlight its risk readiness level, which is a crucial factor influencing M&A decisions. Post-M&A, the automated BAS risk assessment report will help the company identify and remediate security gaps quickly.



## Red/Purple Team Automation

Organizations need security assessment procedures that can provide consistent results and a holistic and integrated security infrastructure perspective. Effective security assessment procedures must also have automated remediation capabilities to ease the team workload.

BAS tools run exhaustive scenarios, checking every possible attack pathway via automated attack campaigns that safely test against hacking tools and techniques within the production environment to expose attack vectors and compromised assets without disruption.

With BAS tools, organizations no longer need to hire penetration testers or skilled red team professionals. Security teams can launch attack campaigns with minimal expertise and effort. Organizations with an in-house red team can scale up their capabilities by leveraging BAS technology. Blue teams with minimal adversarial skills can also use BAS to design and launch attack flows using the customizable templates provided with most BAS tools.

BAS helps enterprises scale up security posture assessments, regardless of the size or complexity of the network. They can also conduct continuous security risk assessments across the entire network infrastructure. Accomplishing the same task with manual penetration testing requires a multi-million dollar budget.

“BAS leverages a framework of attack scenarios; the most commonly used is the MITRE ATT&CK framework, which includes an extensive database of tactics, techniques, and procedures (TTP). The MITRE ATT&CK framework includes 14 different tactics that span the entire kill chain and is continuously updated.”

Cymulate, a leading BAS vendor, offers a purple team automation module that aligns with the MITRE ATT&CK framework to craft and run risk assessments. The module allows red teams to operationalize the framework in the context of an organization's security architecture, using specific and custom attack scenarios. Besides providing visibility on security posture, the purple team automation module enables automated assessments as well as monitors security drift to help ensure compliance requirements are met. Security teams can leverage out-of-the-box scenarios and attack templates to simulate attacks from APT groups or specific security improvement scenarios.

## Cymulate: Company Philosophy

Cymulate, founded in 2016, has rapidly grown its presence in the global BAS market, gaining hundreds of customers across North America, Europe, the Middle East, Latin America and Asia-Pacific. The company says it sets the industry standard for BAS. Its vision is to make continuous security validation accessible and achievable for every business and to be the largest and most comprehensive consultant-free security validation company. Its three-dimensional product design and development strategy reflects its vision in several ways:

### 1 Simplicity

- a. Armed with a Software-as-a-Service platform, Cymulate customers need to deploy just one lightweight agent per environment (Windows, Mac, and Linux). The agent launches simulations within the infrastructure while external attacks and external attack surface analyses are performed from the cloud.
- b. The organization can deploy Cymulate within an hour, enabling security teams to quickly schedule simulations and get results within minutes.
- c. Cymulate provides out-of-the-box assessments that do not require penetration testing skills. These assessments are helpful for small teams that do not have a qualified pen tester. Similarly, large enterprises can automate assessments to scale up red team and security operations.












### 2 Coverage

- a. Cymulate provides end-to-end coverage of the MITRE ATT&CK framework. The platform maps the organizational cyber resiliency to all types of TTPs in the framework.
- b. It also applies a consistent scoring methodology based on the National Institute of Standards and Technology (NIST) and Common Vulnerability Scoring System (CVSS) 3.0 frameworks to assess an attack's likelihood and impact. A standard scoring methodology across all attack vectors ensures that risk levels are comparable across the organization. Organizations can, therefore, prioritize activities, remediation efforts, investments, and projects consistently.
- c. Full kill chain simulations are used that apply various dynamics of the threat to understand attack pathways. With a rich library of assessments, Cymulate's platform evaluates a company's security against different APT groups relevant to an organization's industry.

### 3 Customizability

- a. Cymulate allows customers to choose from a rich library of continuously updated assessment templates or create their own assessments. The customizable templates allow security teams to focus on different types of attacks that leverage specific attack vectors.
- b. The platform allows security teams to sequence different types of atomic executions to create a complex assessment scenario.
- c. Organizations can scale red team capabilities by automating everyday activities of a security operations center (SOC), integrating with SIEM and SOAR tools to manage and fine-tune detection capabilities. The SOC can schedule purple team activities on a daily, weekly, or monthly frequency.

Cymulate provides a comprehensive list of use cases for customers, enabling an end-to-end security assessment and remediation workflow.

USE CASE	DESCRIPTION
 <b>THREAT INTELLIGENCE-LED ASSESSMENT</b>	With its Immediate Threats Intelligence module, Cymulate automates threat intelligence-led testing.
 <b>SECURITY POSTURE MANAGEMENT</b>	Cymulate leverages the MITRE ATT&CK framework to operationalize myriad TTPs used by attackers.
 <b>SECURITY CONTROL EFFICACY/OPTIMIZATION</b>	Expert and threat intelligence-led, out-of-the-box assessments make it simple for security professionals across skill levels to challenge, assess and optimize the current effectiveness of security controls in place.
 <b>ATTACK SURFACE MANAGEMENT</b>	Cymulate performs continuous discovery and quantitative technical analysis of public-facing digital assets of organizations.
 <b>RED/PURPLE TEAM AUTOMATION</b>	The platform makes purple team exercises accessible and achievable to security teams with minimal adversarial skills by leveraging out-of-the-box attack scenarios.
 <b>RISK-BASED VULNERABILITY MANAGEMENT</b>	Cymulate assessments identify exploited and exploitable vulnerabilities through integration with vulnerability management systems and evaluate the adequacy of compensating security controls.
 <b>SECURITY ASSURANCE AUTOMATION</b>	Cymulate enables security teams to automate many of the tasks associated with frequent, typically daily activities that provide ongoing assurance of an organization's security architecture and policy.
 <b>SOC/SIEM VALIDATION &amp; AUTOMATION</b>	Using the MITRE ATT&CK framework as a reference, Cymulate enables companies to validate their SOC's performance through integrations with endpoint detection and response (EDR), extended detection and response (XDR), and SIEM systems.
 <b>SECURITY VISIBILITY</b>	Companies can perform rapid and consistent risk assessments for cybersecurity due diligence by performing a full kill-chain security validation assessment to enable organizations to optimize resource allocation and security spend. Quantitative KPIs enable security teams to communicate security posture effectiveness, gaps and future requirements effectively.
 <b>RISK ASSESSMENT FOR M&amp;A AND THIRD-PARTY INTEGRATION</b>	Cymulate helps organizations perform accurate assessments for due diligence of a company before an M&A deal or third-party integration. Post-M&A, companies can expedite IT integration after clearly identifying security gaps and remediating them.
 <b>VALIDATION FOR REMOTE WORKING</b>	Continuous security validation enables organizations to emulate a remote worker's endpoint and validate its defenses' effectiveness, including cloud-based and endpoint security controls.
 <b>COMPLIANCE ENABLEMENT</b>	Cymulate lets organizations comply with GDPR, PCI, HIPAA, and all other federal or industry regulations that require regular testing of security controls.



## The Final Word

The threat landscape is in a state of rapid evolution, and businesses must stay ahead of cyber adversaries. Simultaneously, investing in multiple security tools increases budgetary expenditure and can become too labor-intensive for SOC analysts to handle. In addition, security posture visibility in real-time is necessary to address the rapidly changing digital landscape.

Enterprises use multiple mechanisms, including penetration testing, vulnerability scanning, and red teaming, to assess security readiness. BAS is a much-needed evolution of security assessment mechanisms that offsets its predecessors' deficiencies. BAS tools enable continuous security improvement by taking the cyber adversary's position, providing organizations a real-time, contextualized view of critical security risks.





## Endnotes

---

- 1 <https://www.frost.com/research/frost-radar/>
- 2 FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State - The New York Times ([nytimes.com](https://www.nytimes.com))
- 3 The State of the Cloud ([frost.com](https://www.frost.com))
- 4 (ISC)<sup>2</sup> Finds the Cybersecurity Workforce Needs to Grow 145% to Close Skills Gap and Better Defend Organizations Worldwide ([isc2.org](https://www.isc2.org))
- 5 Frost & Sullivan statistical research across multiple nations reflects that 47% of enterprises had plans to increase cybersecurity spending in 2020 before the pandemic and subsequent work-from-home initiatives.



Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

The contents of these pages are copyright ©2021 Frost & Sullivan.