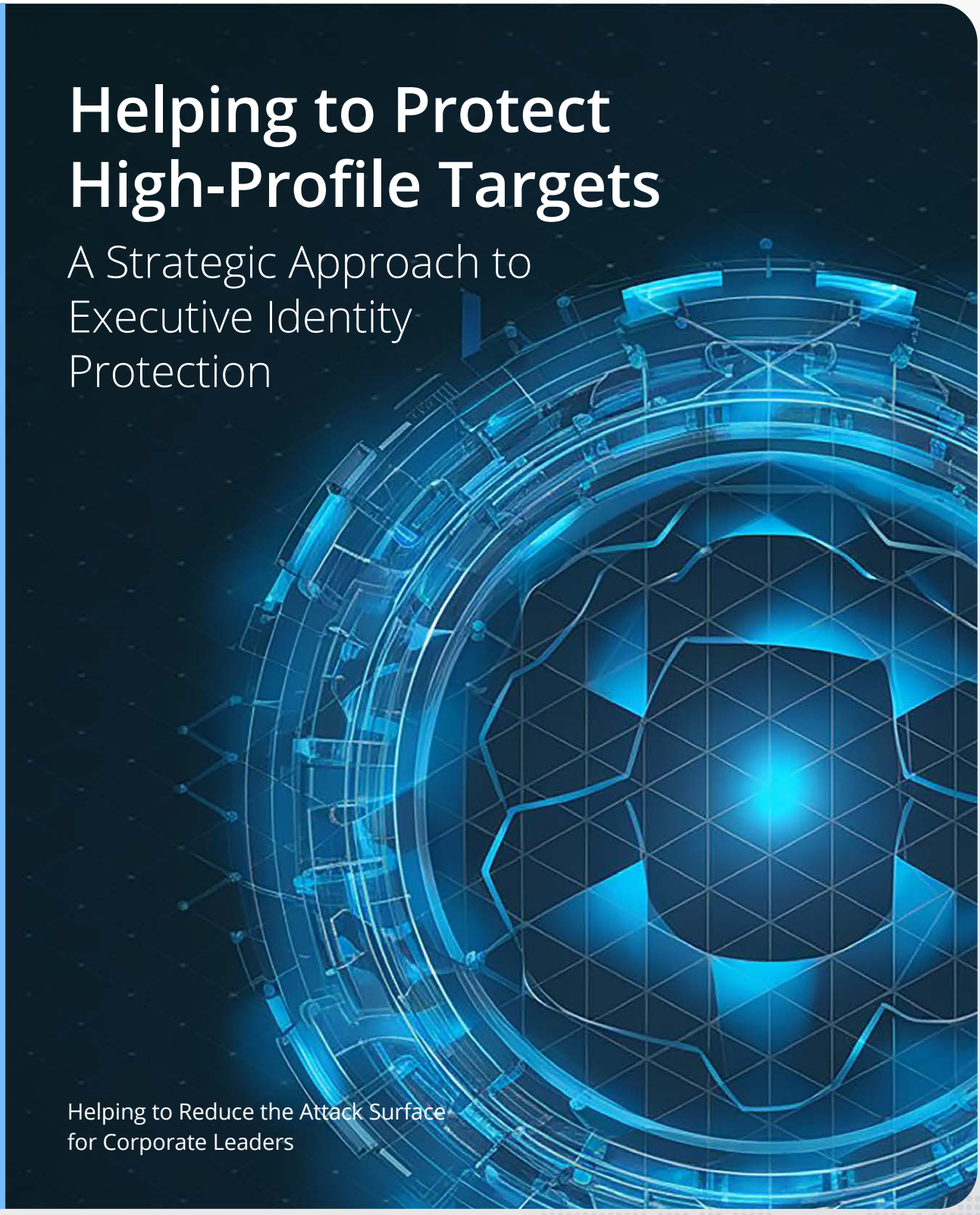
FROST & SULLIVAN

Helping to Protect High-Profile Targets

A Strategic Approach to Executive Identity Protection



Helping to Reduce the Attack Surface for Corporate Leaders

A Frost & Sullivan White Paper
Commissioned by Verizon

frost.com

verizon

Contents

Helping to Protect High-Profile Targets: A Strategic Approach to Executive Identity Protection

Executive summary

Executives can face growing risks as their personal and professional lives become more exposed online. Public data from social media, media coverage, and data brokers is increasingly exploited by attackers to launch identity-based threats like impersonation, fraud, and phishing. These risks can extend beyond digital harm, potentially exposing executives and their families to reputational and physical danger.

Despite strong enterprise security policies, there is often a disconnect between corporate protections and executive online exposure. Closing this gap requires a focused approach to executive identity protection. This paper outlines the evolving threat landscape and introduces a proactive solution from Verizon that can help reduce exposure, protect leadership, and safeguard enterprise integrity.

Despite strong enterprise security policies, there is often a disconnect between corporate protections and executive online exposure.

Growing online exposure is fueling targeted threats

Executives today can face a rapidly evolving threat landscape shaped by their expanding online presence. From media appearances and social media to real estate records and data broker listings, personal and professional information is exposed more than ever. This increased visibility has significantly widened their attack surface, making them prime targets for both digital and physical threats.

The notable 2024 fraud attack involving Mark Read, CEO of one of the world's largest advertising companies, WPP, underscores this growing risk. Fraudsters created a fake WhatsApp account using a publicly available image of the CEO, paired it with AI-generated voice cloning and YouTube footage, and invited a senior executive to a virtual meeting impersonating company leadership. The attackers attempted to use this deepfake setup to solicit sensitive information and financial transactions.

> Executive identity has become a strategic vulnerability that can lead to financial loss, reputational damage, and personal danger.
>
> Frost & Sullivan

While the scam was ultimately unsuccessful, it reflects a disturbing trend: bad actors are leveraging generative AI and publicly available data in an attempt to convincingly mimic executives and manipulate internal stakeholders. According to GetApp's 2024 Executive Cybersecurity Report, 72% of senior executives reported being targeted by cyberattacks within the past 18 months. These risks go far beyond cybersecurity; executive identity has become a strategic vulnerability that can lead to financial loss, reputational damage, and personal danger. As such, protecting identity must be a core element of a person's and organization's broader security strategy, one that safeguards not just the individual but the integrity of the family and entire enterprise.

Beyond cybersecurity: the real-world risks of executive exposure

Senior executives have often become prime targets

Executives have become prime targets for threat actors due to:

Access to sensitive information

Public visibility

Influence over key business decisions

With the expansion of digital platforms and social media, an executive's digital footprint can grow rapidly. This can make personal and professional information easier to access, which can enable attackers to craft convincing and targeted campaigns that can lead to financial fraud, data breaches, and reputational damage.

Both digital and physical threats

These digital threats do not always stay confined to cyberspace. Publicly available information can be used to track movements, identify family members, and escalate threats into the physical world, including harassment or personal safety incidents. Attackers commonly rely on tactics such as business email compromise, impersonation schemes, and phishing. These methods can often be successful because they use personal data to increase credibility and bypass suspicion.

As more executive information is collected in public records, leaked in data breaches, or shared voluntarily online, the line between professional and personal vulnerability can fade.

One of the big enablers of these threats is the data broker industry. Data brokers collect, aggregate, and resell volumes of personal information from various sources, such as: credit card transactions, online activity, public filings, social media, and other sources. These profiles can often include home addresses, phone numbers, known associates, political preferences, and even behavioral data.

While initially intended for advertisers, this data can now be readily exploited by cybercriminals to help them engineer realistic attacks. The availability of detailed and verified information can help threat actors impersonate executives convincingly or design attacks that appear legitimate to colleagues, partners, or service providers.

Despite these threats, many executives continue to underestimate their level of risk. This can create a gap between formal corporate cybersecurity frameworks and the informal digital habits of senior leaders. While organizations may deploy advanced technologies to secure enterprise systems, executives may still use unsecured personal devices, weak passwords, or fail to manage their online presence.

These behaviors can unintentionally weaken corporate defenses, making it no surprise that, based on Frost & Sullivan's 2023 Voice of the Customer (VOC) survey, identity theft and targeted phishing attacks are among organizations' top concerns (Figure 1).

Executive identity protection must be treated as a shared concern. It is not just about protecting one individual but about reducing a major point of exposure for the organization. Closing this gap requires not only technical safeguards but also a cultural shift in how executive risk is understood and addressed.

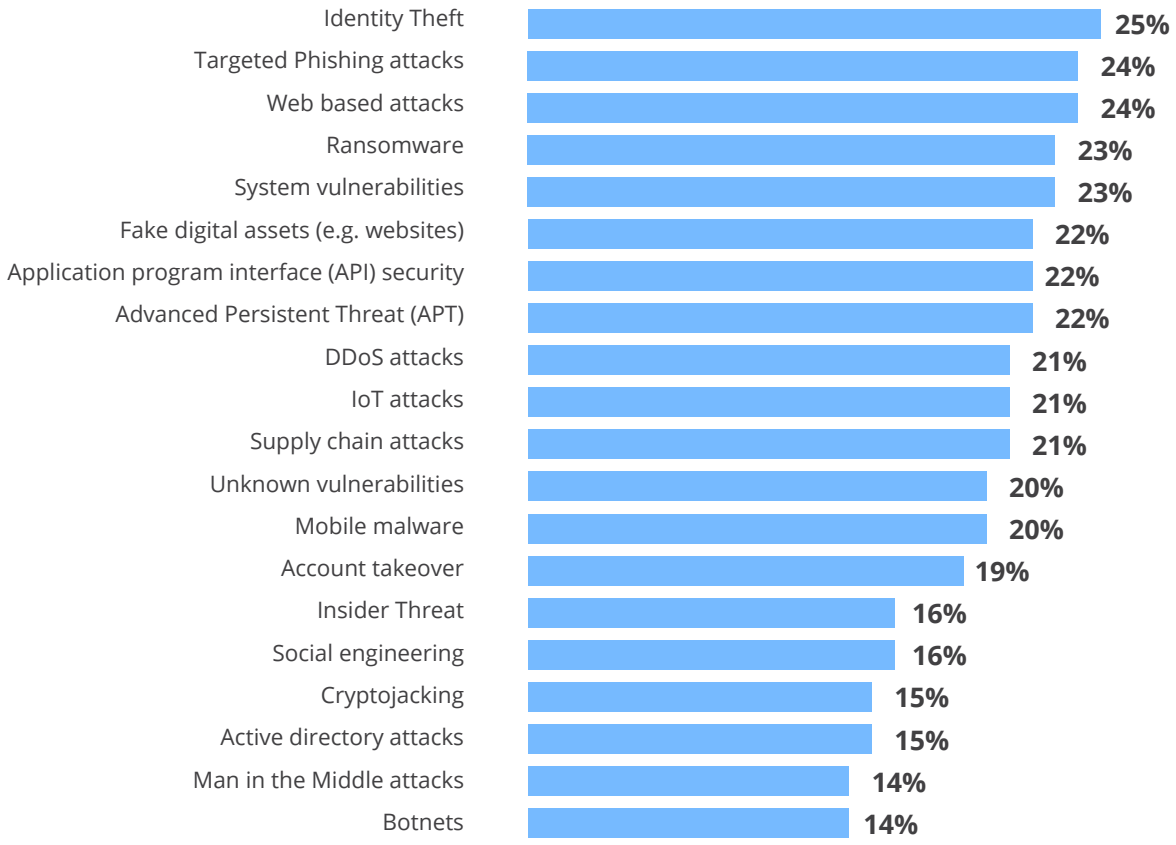
Global Perspective

N=2248

Identity theft, targeted phishing attacks and web-based attacks are the top cybersecurity concerns, but many of the other concerns cited by respondents are in a similar range.

Frost and Sullivan's Global VOC Survey, 2023

What are the main cybersecurity concerns for your organization?



Importance of executive identity protection

Executive identity protection is important for organizations extending beyond the traditional solutions utilized for cybersecurity. Based on Frost & Sullivan analysis, organizations must take the following steps to help holistically protect their executives:

Protect all types of identity, with additional emphasis on executive identity

Organizations need to consider securing various levels of identity. Cyber attackers now frequently use techniques mentioned earlier to target identity and infiltrate the organization through people. These forms of identity are typically protected by various physical and cybersecurity solutions:

- **Physical identity with keycards**, biometrics (fingerprint or facial recognition)
- **User identity** with Identity and Access Management (IAM) and Multi-Factor Authentication (MFA)
- **Customer identity** with Federated Identity Management (FIM)

However, additional care and protection should be given to executive identity, as executives typically hold escalated privileges and have access to sensitive corporate information.

Quantify the visible attack surface

Organizations need to fully understand the visible data attack surface. This data for the organization and executives could be from:

- **Open Source Intelligence (OSINT)**
- **Public data sources**
- **Public documents with signatures**
- **Data brokers**
- **Adult family members**
- **Young family members**

Investigate the hidden attack exposure

Organizations also need to delve into potential hidden exposure of data as well. These could include:

- **Dark web investigation**
- **Analysis for both executive and their family members**

Executive identity protection outcomes for organizations

Executive identity protection programs can assist the organization by helping to:

Reduce the cyber exposure for key executives in the organization

Work directly with the Do Not Call (DNC) registry to minimize contact footprint, followed by ongoing and proactive monitoring

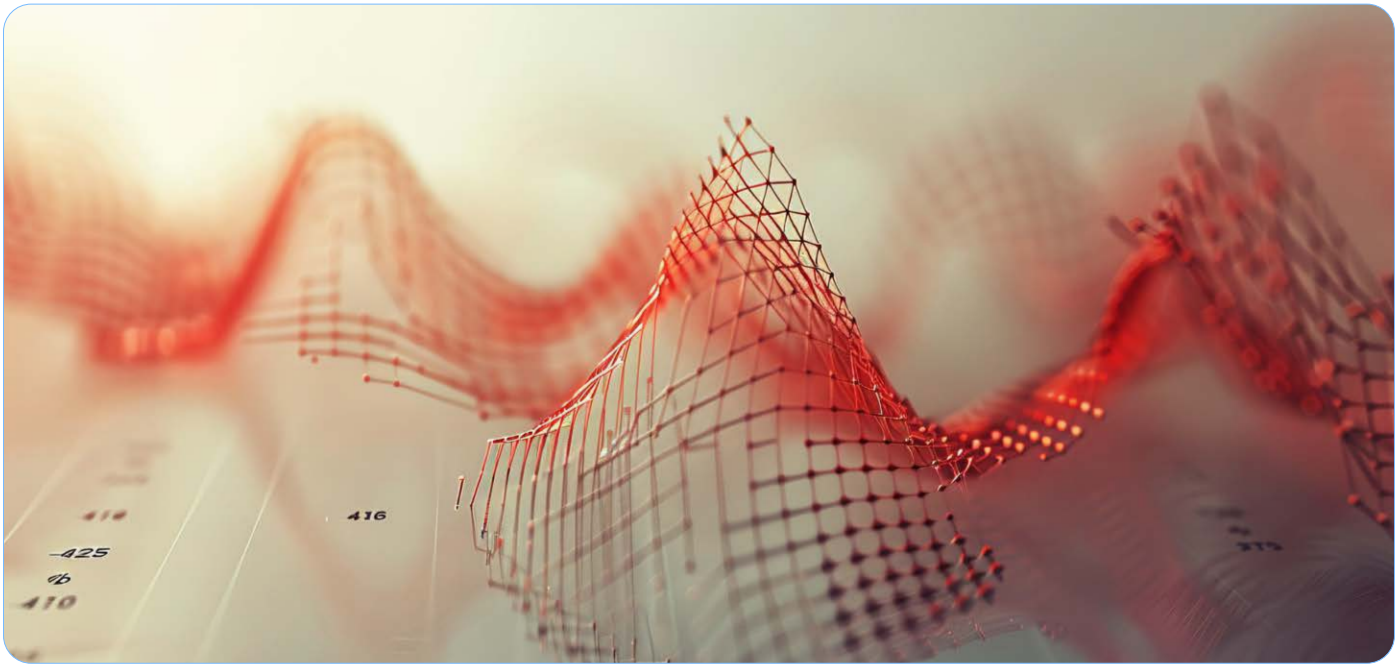
Limit data available for reconnaissance

Decrease both the executive's cyber risk and physical risk

Allow executives to focus on core business activities with reduced risk

Analysis of Verizon's Executive Identity Protection

Based on Frost & Sullivan’s analysis of the Verizon's Executive Identity Protection service, the service benefits



1

White-glove service: a robust service with a privacy specialist assigned to each customer
This service provides organizations with support of senior executives who require a high level of protection, offering a single point of contact.

2

Systematic phased approach
Verizon has developed a 3-phase approach from initial assessment to ongoing monitoring based on their experience supporting senior executives:

Vulnerability assessment phase, with initial identification and assessment

Removal request phase, with privacy specialists focused on removal requests

Ongoing monitoring, where privacy specialists continue monitoring to help proactively identify and request removal of new data inclusions

3

Holistic services
Verizon also offers an option to extend the service to spouses and adult children.

Case studies based on real-world executives

Below are three anonymized case studies illustrating how organizations have leveraged the service to address executive risk management challenges:

A recently promoted executive and proactive organizational response

Following the promotion of a senior executive, the organization identified new cybersecurity and physical security risks associated with the elevated role. To proactively manage these risks, the organization engaged Verizon's service to reduce the executive's and his family's data exposure.

Responding to a compromised digital footprint

An organization discovered that one of its executives had a compromised digital footprint that posed potential risks of exploitation by malicious actors. In response, the organization utilized Verizon's service to remediate the executive's online presence by removing outdated personal data and updating key contact information.

Mitigating physical safety risks stemming from digital exposure

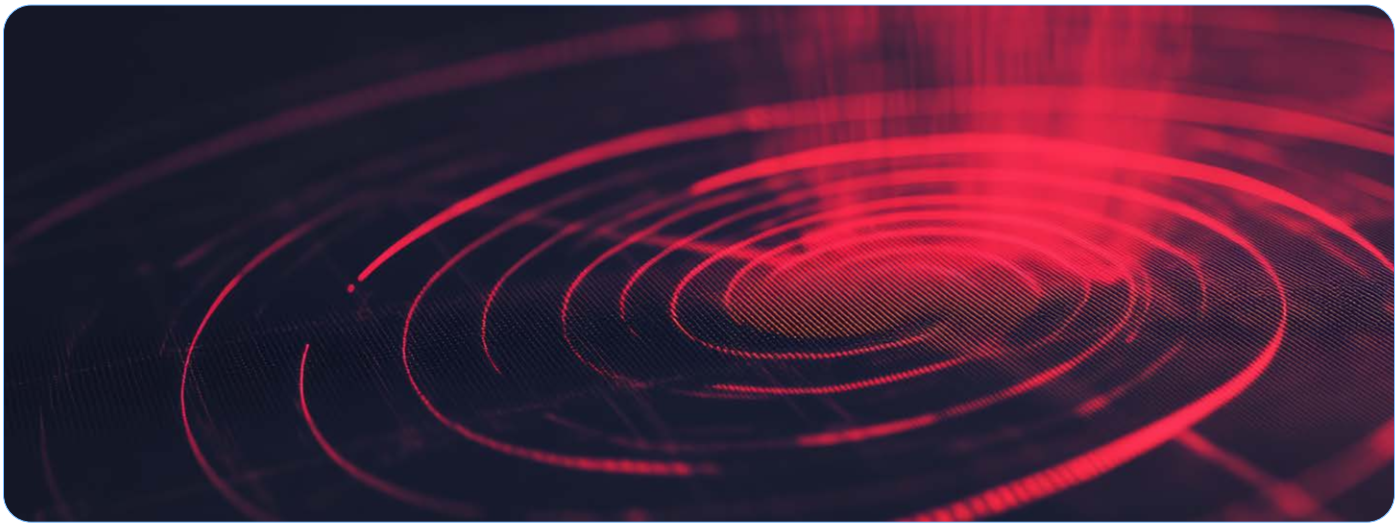
After uncovering that an executive's digital information had been compromised, an organization took additional steps to safeguard the executive's family. Concerned about how exposed digital data could translate into physical threats, the organization deployed Verizon's service to remove sensitive online information and help mitigate associated safety risks.

Strengthening executive security is vital through identity protection

The risks facing today's executives can go far beyond the digital realm, touching every part of their personal and professional lives. Their growing digital footprint has become a valuable target for attackers, and without intentional protection, this exposure can lead to financial loss, reputational harm, and even physical danger.

To build a truly holistic security posture, organizations must include executive identity protection as a strategic component. This means going beyond standard cybersecurity controls and addressing the unique vulnerabilities of leadership.

> By proactively protecting executive identities, organizations can reduce risk, strengthen resilience, and ensure their leaders are free to focus on driving the business forward.
>
> Frost & Sullivan



Services like Verizon's Executive Identity Protection, which offer white-glove support, continuous monitoring, and targeted data removal requests, are essential to helping protect the identities of those most critical to the business. By proactively helping to protect executive identities, organizations can help reduce risk, strengthen resilience, and allow their leaders to focus on driving the business forward.

Find out more about Verizon's Executive Identity Protection

Verizon Executive Identity Protection is a premium white-glove service designed for executives that need a high level of protection. Each customer is assigned a security specialist that pays close attention to the details of each removal request with the objective of securing successful removals, while also advising executives on how to minimize exposure moving forward.

We Accelerate Growth

WWW.FROST.COM

Auckland	Colombo	London	Paris	Singapore
Bahrain	Detroit	Manhattan	Pune	Sophia Antipolis
Bangkok	Dubai	Mexico City	Rockville Centre	Sydney
Beijing	Frankfurt	Miami	San Antonio	Taipei
Bengaluru	Iskandar, Johor Bahru	Milan	Sao Paulo	Tel Aviv
Bogota	Istanbul	Mumbai	Seoul	Tokyo
Buenos Aires	Jakarta	Moscow	Shanghai	Toronto
Cape Town	Kolkata	New Delhi	Shenzhen	Warsaw
Chennai	Kuala Lumpur	Oxford	Silicon Valley	Washington D.C.

ABOUT FROST & SULLIVAN

Frost & Sullivan is a growth partnership company focused on helping our clients achieve transformational growth as they are impacted by an economic environment dominated by accelerating change, driven by disruptive technologies, mega trends, and new business models. The research practice conducts monitoring and analyzing technical, economic, mega trends, competitive, customer, best practices and emerging markets research into one system which supports the entire "growth cycle", which enables clients to have a complete picture of their industry, as well as how all other industries are impacted by these factors.

Contact us: Start the discussion

To join our Growth Partnership, please visit www.frost.com