FROST & SULLIVAN

Navigating the Modern Threat Landscape with Limited Resources

By Martin Naydenov, Senior Cybersecurity Analyst, Frost & Sullivan

FROST & SULLIVAN VIRTUAL THINK TANK

Introduction

In today's complex cybersecurity threat landscape, organizations face a growing number of alarming dangers from multiple attack vectors simultaneously. These include internal threats, like malicious insiders, and external threats, like malware, phishing, and network attacks. To make matters worse, global digitalization efforts (such as cloud migration, remote work, and IoT adoption) have exponentially increased organizations' attack surfaces and IT complexity. This has left many organizations struggling with information overload and alert fatigue, all while dealing with an increasing talent shortage. In short, organizations are struggling with more dangers, too much information, and not enough resources.

It comes as no surprise that an increasing number of organizations are turning to external support to fortify their security efforts.

> As per the recent Frost & Sullivan Global Voice of the Enterprise Customer survey, almost 70% of organizations have outsourced their cybersecurity operations partially or entirely. In this hostile cyber environment, where a single misguided click can have devastating consequences, it is crucial to implement a comprehensive security approach that fully utilizes both in-house and outsourced security services to protect an organization's entire digital footprint.

For example, managed detection and response (MDR) service providers offer the support of experienced professional teams dedicated to threat detection and response. Adopting MDR services empowers organizations to reallocate in-house resources toward value-added tasks and strategic initiatives.

But what does an ideal hybrid security model that seamlessly integrates internal and external resources look like? The benefits and effectiveness of a hybrid security program highly depend on the company's security maturity, industry vertical, culture, technology, security operations, people, and risk profile. While every company has its own set of unique challenges, it is important to recognize the common obstacles and make informed decisions regarding the allocation of security functions, distinguishing between those suitable for outsourcing and those better kept in-house. This understanding helps organizations make a balanced choice that aligns with their overarching business strategy and thrive in an ever-evolving threat landscape.

Filling the Void: A Race Against the Dark Forces

The security professional shortage remains a pressing concern, but even if organizations successfully recruit a sufficient number of security analysts, retaining the talent is also a significant hurdle.

> Matt Standard, Global Head of Cybersecurity Operations at Novartis, shared his insights with Frost & Sullivan: "To retain cybersecurity professionals, we work with each individual on a custom career path and encourage them to explore cross-functional duties."

Unfortunately, many businesses lack the organizational structure and resources to provide individualized career paths for their security professionals. In many cases, security departments are characterized by horizontal integration and limited opportunities for career advancement. This stagnant work environment quickly becomes mundane, prompting security professionals to seek better opportunities that offer improved compensation, benefits, and a work culture that fosters more engaging experiences. This, in turn, creates a vicious cycle for organizations, involving the continuous training and onboarding of new personnel over extended periods, only to witness them leave for another company, repeating the cycle over and over again.

With the number of threat actors far exceeding the number of available security professionals, organizations must increasingly rely on managed services to keep up with emerging threats and protect digital assets. MDR providers fill this talent void by delivering comprehensive incident response teams, proactive threat-hunting capabilities, MITRE ATT&CK mapping features, and end-to-end visibility over an organization's existing security stacks and workflows.

The Duality of AI

Generative AI is a powerful technology that, like a double-edged sword, can be wielded by organizations seeking to improve their security posture and by malicious threat actors. Chris Brosnan, a cybersecurity executive at DeepSeas, echoed this sentiment: "At DeepSeas, we are watching to see how AI can/will be used for malicious purposes. We frequently encounter clients who are inquiring about the implications of AI and the potential impact on their digital footprint."

The main risk with AI is that anybody can become a threat actor nowadays; technical experience is no longer a prerequisite. Any wannabe hacker can ask their generative AI tool for step-by-step instructions on infiltrating an organization network, identifying vulnerabilities, writing exploits, and launching sophisticated phishing attacks at scale.

On the flip side, Matt Standard expressed his optimistic outlook: "The ditch of gloom may obscure our path, but it's within this challenging environment that we can forge AI solutions uniquely suited to our specific challenges." MDR providers deeply understand the threat landscape and know how hackers utilize AI. This knowledge equips them to guide and educate organizations and their security teams on emerging tactics, techniques, and procedures (TTPs), resulting in significant time and resource savings. Through the powerful combination of MDR and AI, organizations can proactively patch any vulnerabilities in their source code, automate and streamline workflows, contextualize their threat intelligence, augment their threat detection and response, and bridge the cybersecurity talent gap.

Dealing with a Phishing Epidemic in Deceptive Waters

With more personal and business interactions shifting to the virtual realm, the risk of customers and employees falling for a phishing attack that impersonates a company or executive has increased significantly.

> Paul Garrin, Chief Information Officer at Urban Health Plan, expressed his concern: "In the healthcare industry, we deal with many phishing campaigns, which is becoming our number one priority."

A successful phishing attack can have devastating consequences, including brand erosion, business disruption, and considerable financial loss. Yet, tackling this inherently human problem requires more than reliance on technology and point solutions. Paul emphasized the importance of awareness and education: "We have to provide constant anti-phishing training because all it takes is only one wrong choice." Proactively mitigating socially engineered attacks remains a challenge, however, as most organizations do not have the time and resources to train their staff on the latest phishing trends—especially as attacks are increasing in number and becoming more sophisticated with the help of AI. MDR providers can offer a solution to this by virtue of their abundant resources, expertise, and powerful network effect generated by serving thousands of customers. This positions them to proactively identify and train staff in new phishing techniques while implementing the right security measures.

Security Is Only as Strong as the Weakest Link

Regardless of size or industry, most organizations rely on third parties for various operational aspects, including access to systems, applications, and data. Vulnerabilities embedded in source code, API misconfigurations, the presence of shadow IT, data leakage, and poor privacy practices are just a few examples of what hackers can use to breach organizations both upstream and downstream in the supply chain.

> As Ebu Mbaye, Deputy CISO at Capital One, pointed out, "Our biggest challenge when it comes to cyber is securing software. Most organizations are still not there yet and lack critical security frameworks and tracking capabilities for internal and external applications."

An ongoing business constraint is allocating adequate resources to comprehensively evaluate and monitor an extensive partner network and accurately assess every organization's risk profile. MDR providers can work closely with organizations to develop customized security strategies that address the specific challenges and risks associated with their supply chain and third-party relationships. By providing robust oversight, guidance, and a holistic framework for comprehensive risk management, MDR providers augment and enable security teams to monitor their digital assets inside and outside their network perimeter.

Securing Endpoint and IoT Devices: Like Catching Water with a Net

Increased remote work, bring your own device (BOYD), and IoT device adoption have drastically expanded the average attack surface of an organization. This surge in endpoints and IoT devices introduced numerous business challenges ranging from reduced visibility and control to information overload. As Paul Garrin rightfully fears: "What keeps me up at night is the proliferation of IoT devices in the healthcare industry. Many healthcare device manufacturers have not convincingly demonstrated robust security measures. Handling the influx of IoT devices, especially operated outside of your immediate site, poses one of the most formidable challenges we face today."

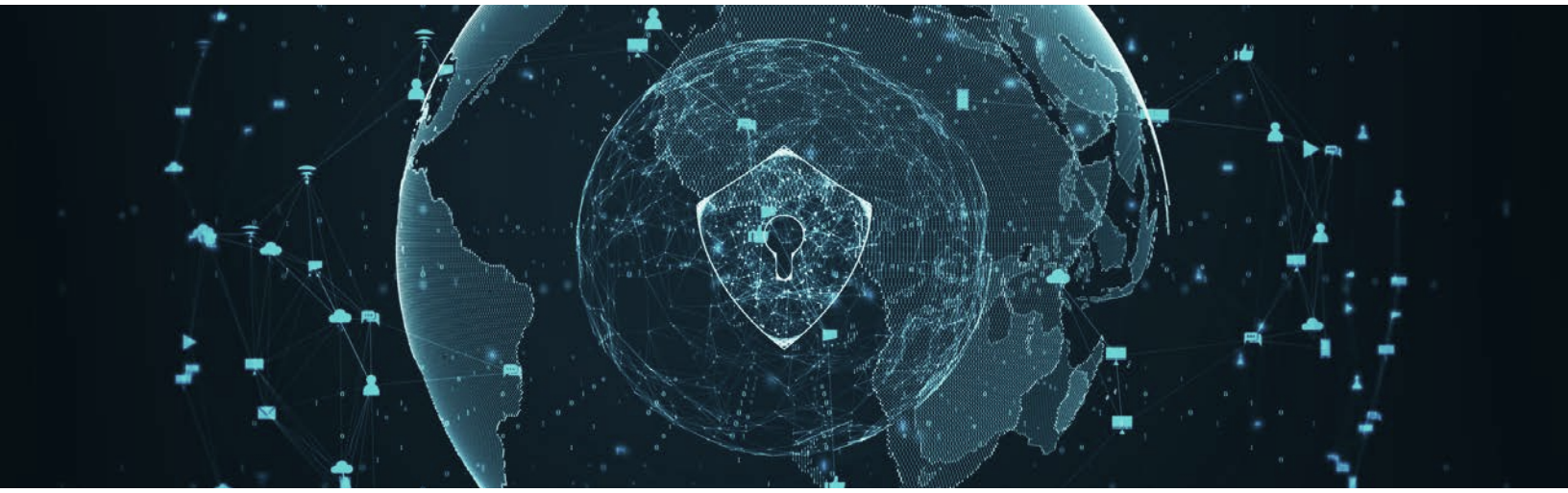
Threat detection and response becomes almost impossible when security teams monitor thousands of endpoint devices with different operating systems and controls, all while dealing with distinct data sets and workflows. MDR offers a compelling solution that

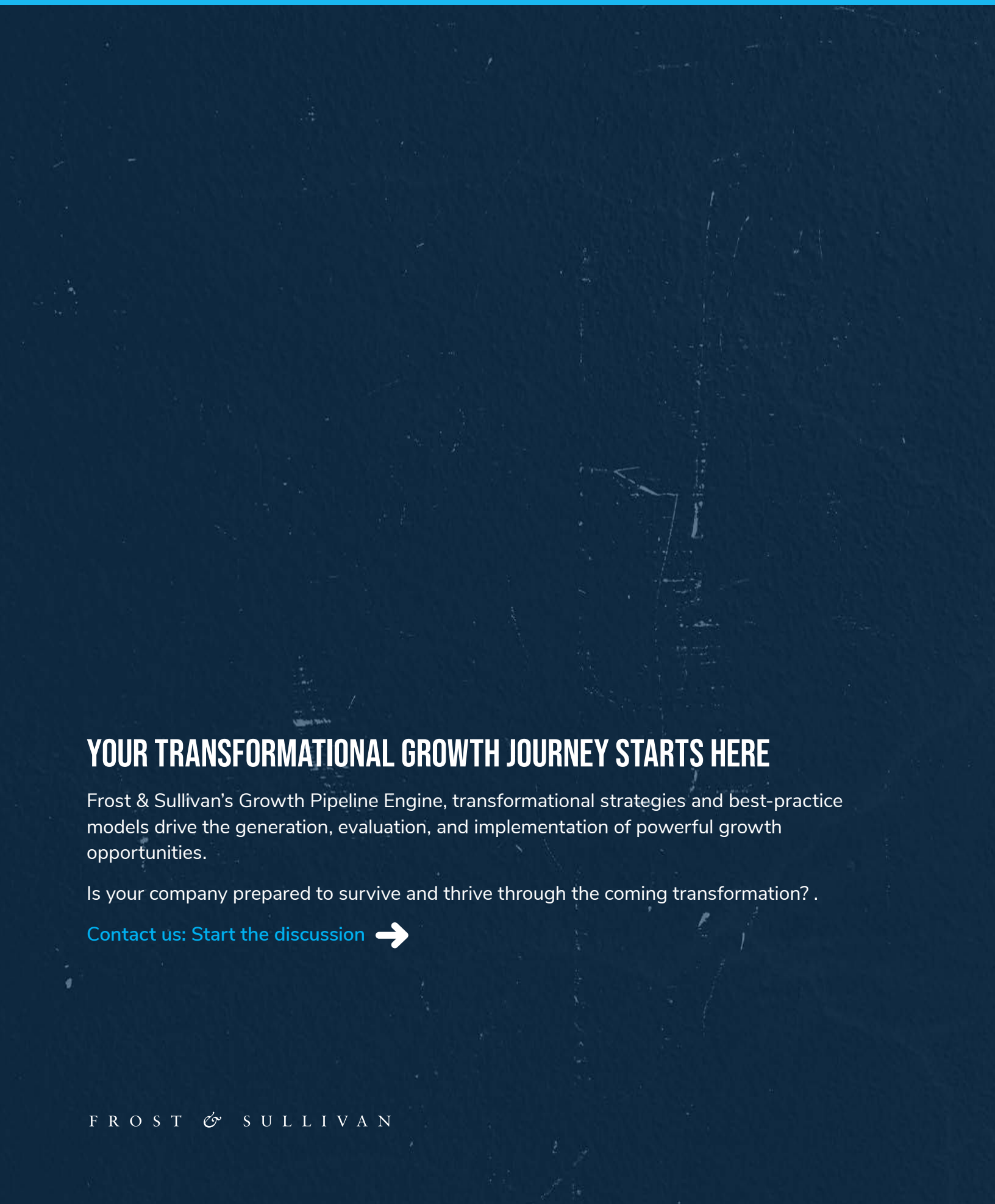
harnesses the power of a centralized ecosystem and a global team of designated security analysts. Aggregated threat data from various sources, such as endpoints, cloud servers, email systems, and IoT devices, equips MDR vendors with end-to-end and real-time visibility of an organization's IT environment, enabling around-the-clock threat response.

Reimagining Cybersecurity

As highlighted, organizations face a wide range of challenges but often lack the resources to address these problems themselves. Wade Alt, Chief Operating Officer at DeepSeas, shared some of his insights and pain points many customers face: "Virtually any industry faces a similar battle between granting (perceived) freedom to their employees and securing the environment. Cyber operations become even more challenging with the expansion into new attack surfaces, such as manufacturing, IoT, and mobility."

Outsourcing cybersecurity operations can tremendously benefit organizations with improved security posture and significant time and cost savings. MDR providers have economies of scale, deep industry knowledge, and advanced tools to mitigate threats in real time by harnessing the power of a centralized network of thousands of customers. The main advantage of managed security services is that they empower organizations to focus on the thing that matters—THEIR BUSINESS. By leveraging external support from MDR providers, organizations effectively bridge the security talent gap and free up valuable resources to focus on more important strategic imperatives—such as proactive security measures to reduce supply chain risks and successful phishing attacks. As accurately observed by Ebu Mbaye: "Everyone is grappling with different challenges, which underscores the fact that there is no one-size-fits-all hybrid security model." Regardless of the extent to which organizations choose to outsource their security operations, MDR can provide the visibility and resources to tackle the most challenging aspects of cybersecurity.





YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation? .

Contact us: Start the discussion

FROST & SULLIVAN