FROST & SULLIVAN

Hybrid MDR: A Holistic Security Solution for SMBs

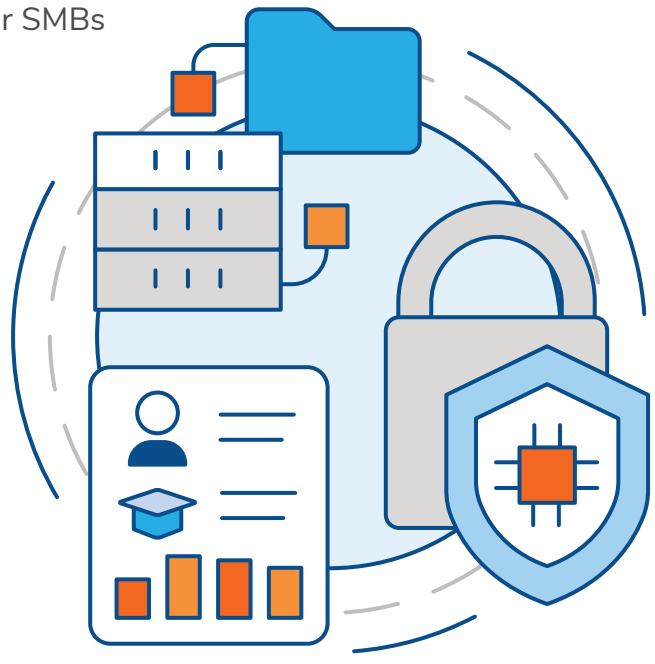
Challenges and Solutions for Protecting Organizations

Authored by Sarah Pavlak
Industry Principal, Security

FROST & SULLIVAN VISUAL WHITEPAPER

The contents of these pages are copyright © Frost & Sullivan. All rights reserved.

CONTENTS



All rights reserved ©2023 Frost & Sullivan | www.frost.com

Industry Challenges for Small and Midsize Businesses

According to Frost & Sullivan research, businesses use an average of 11 different products for their security needs. This highlights the importance of holistic security solutions and partnering with vendors that can provide such solutions.

- The move to a remote/hybrid workforce expanded the cyberattack surface for most organizations leading to difficulties in finding security vendors that provide solutions for everything from endpoints to new cloud environments.
- Cyber attackers are automating and scaling attacks on small and midsize businesses (SMBs).

There is a common misperception of a lack of competent cybersecurity providers/partners capable of supporting their security needs.

- The insufficient number and expense of cybersecurity specialists is a usual obstacle to organizations' security.

All rights reserved ©2023 Frost & Sullivan | www.frost.com

- The same threats affecting large enterprises also affect SMBs, heightening the importance of vendor solutions that provide leading-edge machine learning-enabled capabilities.
- The SMB market is significantly underserved, and most organizations cannot afford to purchase or deploy enterprise-grade technologies nor use sub-par security solutions to face pervasive and persistent cyber threats.
- Some security solutions are so complex that they are unusable for SMBs in-house expertise, so the organization cannot take direct measures to increase its security posture.
- Flexible pricing model offerings are essential for the success of SMBs. Most SMBs allocate security budgets in yearly or three year plans for services.

Some vendor partner engagement models that can help SMBs achieve their security goals include:

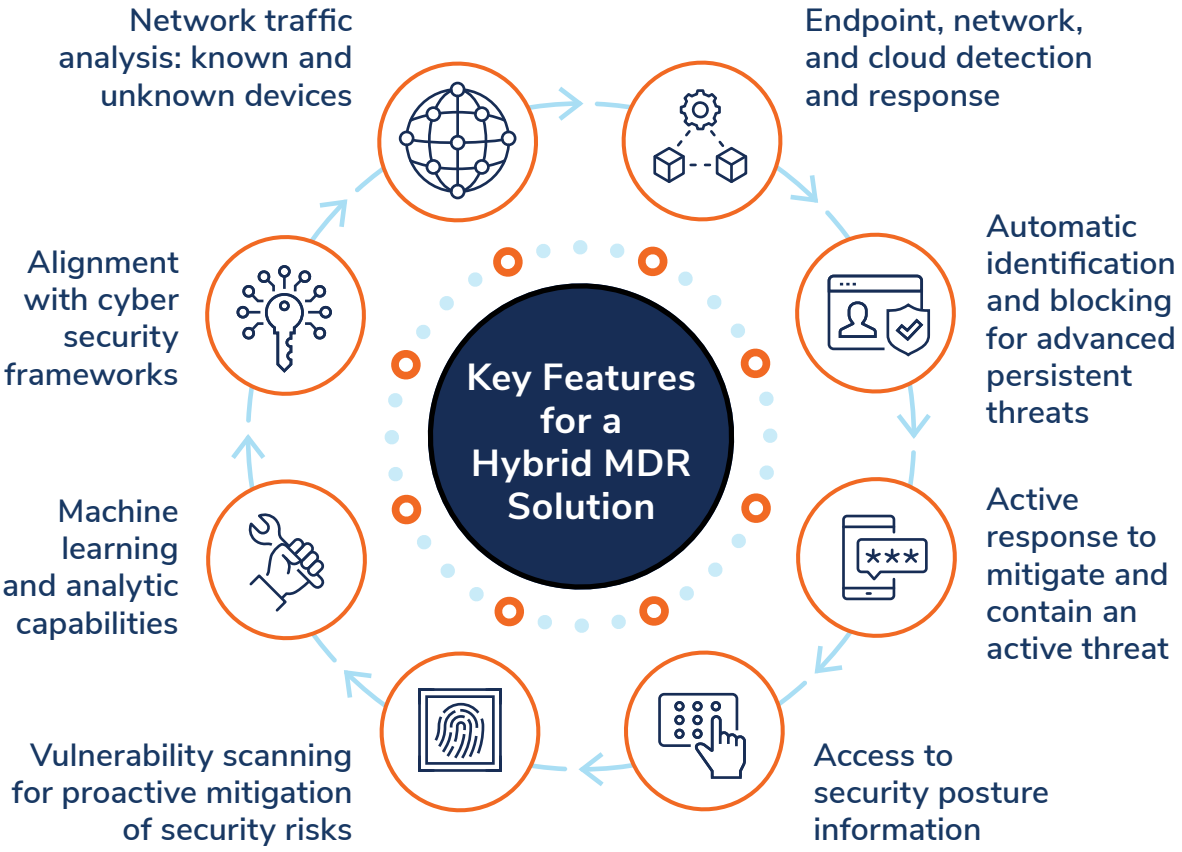
- Scalability and on-demand expertise
- High product effectiveness for security efficacy and positive business outcomes
- A strong partnership to help SMBs secure their operations and drive greater efficiency.

All rights reserved ©2023 Frost & Sullivan | www.frost.com

Hybrid Managed Detection and Response (MDR) as a Holistic Approach

- Real-time threat monitoring, detection, and blocking solution within a single platform
- End-to-end visibility across the entire threat surface along with endpoint protection in one platform for threat detection, analysis, and response
- Automation capabilities utilizing machine learning algorithms and advanced analytics
- Hybrid MDR natively integrating endpoint, network, cloud, document/file/email/email attachment scanning, and external surface scanning components to provide unified protection across all areas of an organization

Focus on attackers' objectives and techniques rather than only the result of their activity.



All rights reserved ©2023 Frost & Sullivan | www.frost.com

End-to-End Holistic Solution Components for Protecting Organizations

ENDPOINT MONITORING

- Prevention of ransomware, advanced persistent threats, and malware in real-time.
- Normal behavior determined, with response adapted accordingly.
- Comprehensive visibility of all activity on the operating systems through user- and kernel-mode capability.
- Observation of privileged access to identify attack or exploitation.
- Intelligent detection and analysis with focus on attacker tactics and techniques to effectively detect unknown threats.
- Continuous review of threat data to improve detection policies and analysis capabilities.
- Proactive scanning to identify new threats and vulnerabilities.

NETWORK MONITORING

- Observation of network traffic such that it is unalterable by threat actors, providing a vantage point to apply security practices to identify threats and vulnerabilities across the network.
- Extraction of information from network traffic to support security monitoring, with evaluation of network signatures to alert about known malicious activity.
- Collection and analysis of network telemetry to report on threat surface risks and respond to threat detections.
- High-res real-time inspection and analysis Son all IPv4 and IPv6 network traffic.

CLOUD MONITORING

- Analysis of data across various cloud services to identify anomalous events.
- Cross-analysis of potential cloud-based security events with data from both the network and associated endpoints.
- Detection of and alerting on cloud account risks and threats including phishing attempts, abnormal activity or behavior, and insecure configuration.
- Detection of and alerting on data loss which may indicate compromise.
- Monitoring of cloud data including audit and event log analysis, cloud provider security logs, and information relating to users, accounts, and groups.

All rights reserved ©2023 Frost & Sullivan | www.frost.com

Human Intelligence Must Be Incorporated into Automated Security Solutions

Automated cyber security solutions must balance **technology** and **human intelligence**—by incorporating machine learning ***and*** advanced analytics designed, maintained, and updated by experienced security analysts.

- Security analytics blended with machine learning using both supervised and unsupervised approaches
- Powerful and reliable solution with automation to scale the human element
- Humans can never be eliminated in a proper security solution
  - This human expertise must be provided by the cybersecurity vendors—this burden cannot be on the SMB
  - The combination of humans + machine learning + analytics ensures fewer and more reliable alerts, and provide alerts fidelity for customers and an efficient workflow for IT professionals
  - Experienced cybersecurity analysts employ machine learning algorithms and analytics to identify, investigate, and respond quickly to potential security incidents

A high efficacy of alerts—with a reduction in the volume of alerts and false positives—gives SMBs confidence to focus on their business, not cybersecurity challenges

All rights reserved ©2023 Frost & Sullivan | www.frost.com

Leveraging Active Response for Next-level Protection

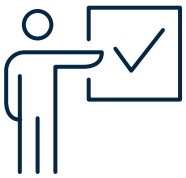
- Respond actively and in real time.
- Provide insights gained from advanced threat detection analysis designed to be easy to understand—straightforward and concise—and actionable without security expertise.
- Recognize the necessary response and action needed to secure an organization.
- Reduce the alert fatigue experienced by most cyber security customers and offer clear explanations for critical alerts.
- Unify data analysis workflow combining alerts from the endpoint, network, and cloud for increased visibility.

What is an ARO?

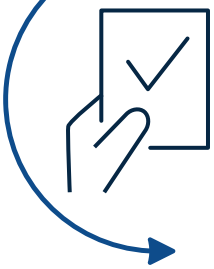
ACTIONS

Required Actions

Immediate for an active or imminent threat that could compromise the network or endpoint devices.



RECOMMENDATIONS



Suggested Changes

Specific vulnerabilities or possible threats that warrant changes in network configuration, software, or technology.

OBSERVATIONS

Early Indicators

Events with a security context that may be deliberate and expected, or could be an indication of malicious activity.

> **“The AROs approach is unique. Other monitoring solutions will aggregate the event logs and provide the information, but nothing is distilled for us, requiring more time to evaluate the data and determine the best course of action.”**
>
> —From WW Works Case Study

All rights reserved ©2023 Frost & Sullivan | www.frost.com

Why the Hybrid MDR Approach is Ideal for SMBs

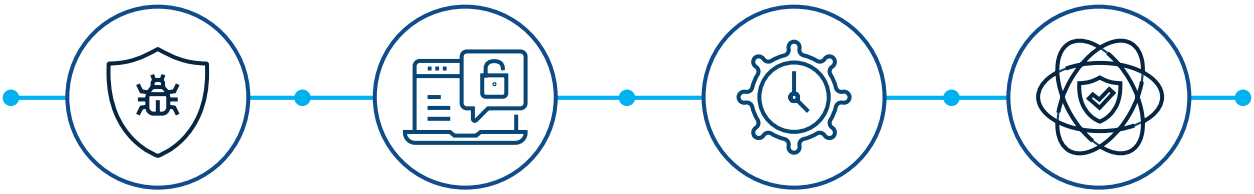
SMBs are looking for a one-stop shop for their cybersecurity needs—hybrid MDR covering endpoint, cloud, and network security can offer such a solution. Hybrid MDR can ensure concrete business outcomes and strong ROI.

- Hybrid MDR provides a new way of transmitting threat and risk information to SMBs with simplicity and a lowered technological and cybersecurity burden for the end-user.
- Continuous view of potential cyber risks and malicious activity, enriched by cyber experts, prevents cyber threats and eliminates security vulnerabilities.
- Hybrid MDR as a managed service provides an ideal solution to the lack of experienced security professionals, the need to address sophisticated threats, and the high volume of alerts caused by the changing security perimeter.
- A hybrid MDR approach can cover a broad range of use cases. This is essential as organizations move away from on-premises solutions and toward hybrid environments becoming the norm.
- SMBs are looking for a one-stop shop for their cybersecurity needs—hybrid MDR covering endpoint, cloud, and network security can offer such a solution. Hybrid MDR can ensure concrete business outcomes and strong ROI.
- A single dashboard delivering straightforward, easy-to-consume information designed for the SMB, allowing for constant awareness and direct control over security posture.

> Our goal was finding a security service built for small businesses and not just a bunch of additional products to manage."
>
> —From WW Works Case Study

All rights reserved ©2023 Frost & Sullivan | www.frost.com

Real-time Active Protection from Threats and Attacks



Threats are blocked or contained across networks, endpoints, and cloud services.

Activity can be blocked or stopped based on the organization's response policy.

Timely, meaningful and actionable feedback alerts are vital factors.

Clear, relevant threat and risk alerts lead to fewer false positives and less alert fatigue.

Response actions include:

- **NETWORKS**
  Preventing or stopping remote communications through DNS firewall and dynamic block lists to provide a broad defense against threats that hinder external communications and prevent threat actor command and control.
- **ENDPOINTS**
  Blocking malicious activity and isolating a host/endpoint from external communications.
- **CLOUD**
  Locking cloud accounts and revoking active sessions upon discovering malicious activity.

> Some customers may not want the hassle of using new services, like two-factor authentication for their applications and devices, but when they see our ARO reports, they change their minds."
>
> —From WW Works Case Study

All rights reserved ©2023 Frost & Sullivan | www.frost.com

Looking Ahead to Growth and Expansion

Growth figures will rise for regions with high-security maturity and technology adoption, like:

Frost & Sullivan research shows that the **security challenges** facing organizations, especially SMBs, have led to **a preference for managed services**.

- MSPs offering a portfolio of comprehensive and tightly integrated security solutions will lead as **the focus shifts to next-generation solutions**. In addition, strong customer support capabilities able to meet the needs of global organizations of various industries are necessary.
- **Holistic cybersecurity solutions are critical to protecting organizations of all sizes and budgets**. SMBs need to partner with a security vendor that offers a one-stop shop for their cybersecurity needs. A wide variety of security services and solutions integrated into a single platform is critical for success.
- **Automated security solutions** incorporating human intelligence factors must be included in holistic security solution portfolios.
- As an essential component of cybersecurity, **the importance of managed services will grow**. Frost & Sullivan research shows these services offer the fastest growth rates and the most significant ROI for channel organizations.
- With a constantly evolving threat landscape, **comprehensive and well-integrated security solution portfolios are critical**. These solutions provide SMBs with the tools necessary for preventing and mitigating security incidents with ease of management and lower costs.

All rights reserved ©2023 Frost & Sullivan | www.frost.com

THE GROWTH PIPELINE COMPANY

For over six decades, Frost & Sullivan has provided actionable insights to corporations, governments and investors, resulting in a stream of innovative growth opportunities that allow them to maximize their economic potential, navigate emerging Mega Trends and shape a future based on sustainable growth.

Contact us: Start the discussion

FROST & SULLIVAN