NULLVECTOR

The NullVector Unified Security Platform: Delivering Enterprise-Grade, AI-Native Cybersecurity for the Managed Service Provider

A Technical and Strategic Overview for Securing Small and Mid-Sized Businesses at Scale

Published by: NullVector
Classification: Public
Version: 1.0 — March 2026

Executive Summary

The small and mid-sized business (SMB) sector, the backbone of the global economy, is facing an existential threat. Cyber adversaries, once focused on large enterprises, now view SMBs as lucrative, soft targets. What we are tasked with defending these organizations are caught in a difficult position, burdened by fragmented security tooling, overwhelming alert volumes, and intense margin pressure. This operational reality demands a new model for security delivery — one that is unified, intelligent, and scalable.

The NullVector Unified Security Platform is the definitive answer to this market imperative. Purpose-built for the modern SMBs, the platform consolidates a comprehensive, enterprise-grade security stack into a single, AI-native, multi-tenant environment. It moves beyond simple product aggregation to provide a unified data and control plane that covers the most critical attack vectors, from identity and endpoints to email and cloud infrastructure. By integrating AI-powered Managed Detection and Response (MDR) with a sophisticated correlation and response capabilities, the platform provides the strategic infrastructure for SMBs to transform their business. It enables them to evolve from reactive IT support providers into proactive, high-value security partners, delivering consistent, profitable, and enterprise-grade cybersecurity at scale.

1. The Market Imperative: A New Model for SMB Security

The cybersecurity landscape for small and mid-sized businesses has fundamentally changed. No longer afforded security through obscurity, SMBs are now squarely in the crosshairs of sophisticated threat actors. According to a 2025 cybersecurity report, nearly half of all U.S. small businesses have already experienced a cyberattack [1]. Adversaries are leveraging advanced techniques like ransomware-as-a-service (RaaS), AI-powered phishing, and complex identity-based attacks that were previously reserved for targeting large corporations.

The consequences for SMBs are devastating, often leading to significant financial loss, reputational damage, and operational disruption.

This escalating threat environment has created an unsustainable operational challenge for the SMBs on the front lines. To provide adequate protection, SMBs have been forced to assemble a patchwork of disparate point solutions — one for endpoint protection, another for email security, a third for security awareness training, and so on. This vendor sprawl leads to a host of compounding problems: a lack of integration between tools, an overwhelming volume of uncoordinated alerts, high licensing and training costs, and an inability to gain a holistic view of a client's true security posture. MSPs are spending more time managing their tools than they are proactively defending their clients, all while facing downward pressure on pricing.

The market is signaling a clear and urgent need for a strategic shift. The old model of bolting on security products is no longer viable. The future of SMB-delivered security lies in a unified, platform-centric approach that provides a comprehensive security stack, operational efficiency, and the intelligence to not just respond to threats, but to anticipate them.

2. The NullVector Unified Security Platform: Architecture & Philosophy

The NullVector Unified Security Platform is engineered from the ground up to address the specific challenges of the modern SMB. It is not a bundle of products, but a cohesive, integrated platform built on a set of core architectural principles designed for security, scalability, and operational excellence.

Multi-Tenancy by Design: The platform was built with a true multi-tenant architecture at its core. This ensures strict data isolation between clients at the database and API layers, allowing us to manage entire client portfolios from a single dashboard without risk of data co-mingling. This is a fundamental requirement for delivering managed security services at scale.

AI-Native Operations: The platform leverages artificial intelligence and machine learning throughout the security stack. From the agentic AI that powers the Managed Detection and Response (MDR) service to the generative AI used in phishing simulations and report generation, the platform uses AI to automate tasks, identify anomalies, and provide intelligent insights, enabling SMBs to do more with less.

Unified Data & Control Plane: The platform's greatest strength is its unified nature. It consolidates the telemetry from eight distinct security layers into a single data lake. This allows the platform to correlate signals across different attack vectors — for example, linking a suspicious login event from the ITDR module with a malware detection on an endpoint and a malicious email click — to identify complex, multi-stage attacks that would be missed by siloed tools.

As part of the broader NullVector ecosystem, the Unified Security Platform serves as the core protective, monitoring, and response layer. It provides the real-time security posture data that informs the strategic guidance of the NullVector vCISO Platform and can be used to validate the effectiveness of security controls assessed by the NullVector xRiskS penetration testing platform.

3. Platform Capabilities: The Unified Security Stack

The NullVector Unified Security Platform integrates eight core security controls into a single, cohesive offering. This consolidation eliminates security gaps, reduces administrative overhead, and provides a comprehensive defense-in-depth strategy for every client.

Security Control	Description
Identity Threat Detection & Response (ITDR)	Monitors user behavior and cloud directory configurations in M365 and Google Workspace to detect and respond to identity-based attacks like account takeover and token theft.
Endpoint Security	Provides robust protection against malware, ransomware, and advanced threats at the device level, with options for both managed antivirus and full AI-native Endpoint Detection and Response (EDR) powered by SentinelOne.
Email Security	Leverages the power of Check Point Harmony Email to provide best-in-class, API-based protection against phishing, business email compromise (BEC), and malicious attachments without requiring MX record changes.
Cloud Data Protection	Secures sensitive data within cloud collaboration environments, preventing unauthorized access and data leaks without the need for complex policy configuration.
Security Awareness Training	Transforms employees from a security risk into a line of defense through pre-scheduled, engaging training modules that measurably improve security hygiene.
Automated Phishing Simulations	Uses generative AI to create and automate realistic phishing simulations, allowing MSPs to test employee resilience and reinforce training concepts.
External Footprint Monitoring	Continuously scans a client's public-facing digital footprint — including domains, IP addresses, and cloud assets — to identify and remediate exposures before they can be exploited.
Dark Web Monitoring	Proactively monitors the dark web for compromised client credentials and other sensitive data, providing early warning of potential breaches.

These are not simply eight different products in one portal. The true power of the platform comes from their integration. The **Identity Threat Detection & Response (ITDR)** capability, for example, is the new frontline of defense, focusing on the #1 attack vector: compromised credentials. By baselining normal user behavior, it can spot anomalies that

indicate an account takeover or session hijacking in progress and enable a one-click response to suspend the account. The **Endpoint Security** layer, with its **integrated SentinelOne**

EDR, provides the deep forensic visibility needed to understand what an attacker does after gaining initial access. The **Email Security** module, powered by Check Point, stops the primary initial access vector for many of these attacks before they ever reach an employee's inbox. Together, these integrated layers provide a level of protection that is far greater than the sum of its parts.

4. AI-Native Managed Detection & Response (MDR)

For MSPs looking to provide the highest level of security without the significant investment of building and staffing a 24/7 Security Operations Center (SOC), the NullVector Unified Security Platform offers an integrated, AI-native Managed Detection and Response (MDR) service. This service elevates the platform from a collection of security tools to a fully managed security solution.

The MDR service operates on a hybrid AI + Human model. The platform's agentic AI acts as the first line of defense, continuously monitoring the unified data stream from all security controls. It automatically triages alerts, filters out false positives, and enriches real threats with contextual data. When a high-fidelity threat is detected, it is escalated to the NullVector threat hunting team. These elite security analysts investigate the threat, provide detailed analysis, and deliver actionable response guidance directly through the platform.

This service covers the full scope of the platform, including advanced threats detected by the SentinelOne EDR and complex identity-based attacks identified by the ITDR module. It provides MSPs with the peace of mind that comes from knowing their clients are protected around the clock by a team of world-class security experts, all delivered through the same unified platform they use for their daily operations.

5. Conclusion: The Future of All-in-One Security

The NullVector Unified Security Platform fundamentally resolves the dual challenges that have constrained the MSP market for years: how to effectively protect SMB clients from an onslaught of advanced cyber threats, and how to do so profitably and at scale. By consolidating a comprehensive security stack, automating response, and providing a powerful business operations engine, the platform empowers SMBs to move up the value chain.

It is the essential infrastructure for any SMB looking to mature their security posture, differentiate their services in a crowded market, and transition from being a simple IT provider to an indispensable strategic security partner to their clients. The future of security is not about selling more products; it is about delivering better outcomes. The NullVector Unified Security Platform is the engine that makes those outcomes possible.

NULLVECTOR