FROST & SULLIVAN

Customer Transformation Journeys

MSP-Enabled Microsoft 365 Security: Hornetsecurity by Proofpoint

How Hornetsecurity by Proofpoint Helps MSPs Consolidate Multiple Point Solutions into a More Integrated Microsoft 365 Security Model

Lead Analyst: Claudio Stahnke

M1O3-74 | August 2026

Contents

Summary

Hornetsecurity by Proofpoint helps managed service providers (MSPs) operationalize Microsoft 365 security through an integrated portfolio spanning email security, backup, permission management, and security awareness. This report is based primarily on Frost & Sullivan interviews with MSP and managed security service provider (MSSP) partners, supplemented by customer examples shared by those partners, rather than direct interviews with end customers. Across the interviews, partners highlighted Hornetsecurity's ability to simplify fragmented security stacks, streamline onboarding, improve reporting, and support more strategic customer conversations. Several MSPs also described downstream customer benefits, including stronger Microsoft 365 backup coverage, faster post-delivery email remediation, improved visibility into permissions risk, and more board-level engagement with security awareness metrics. These insights demonstrate how partner-delivered cybersecurity can help small and mid-market organizations improve resilience without adding operational complexity.

Overview

Organizations increasingly rely on Microsoft 365 as the operational backbone for email, collaboration, document sharing, and business communication. This dependency creates a broad security and resilience challenge. Email remains one of the primary entry points for phishing, fraud, credential theft, and malware. At the same time, Microsoft 365 environments often contain backup gaps, unmanaged sharing links, permission sprawl, and inconsistent user security behaviors. For SMB and mid-market organizations, these risks are particularly difficult to manage because internal IT teams are frequently resource-constrained and must balance security, productivity, compliance, and cost.

Traditional approaches based on disconnected point solutions are becoming less effective. Customers may have separate tools for email filtering, backup, security awareness, archiving, permission management, and reporting, but fragmented stacks can increase administrative burden and make it harder for MSPs to deliver consistent outcomes. This complexity also makes cybersecurity harder to explain to nontechnical stakeholders, who increasingly expect evidence of value, risk reduction, and ROI.

MSPs play a critical role in closing this gap. They translate cybersecurity capabilities into managed services, operational processes, reporting cadences, and business-level recommendations. For partner-led security delivery to scale, MSPs need platforms that are easy to deploy, simple to manage across multiple customers, commercially flexible, and capable of producing insights that customers can understand. Hornetsecurity addresses this need by combining Microsoft 365-focused security, backup, permissions, and awareness capabilities in a portfolio designed to support both partner operations and downstream customer resilience.

Hornetsecurity by Proofpoint

Hornetsecurity by Proofpoint is a global provider of cloud-based security, compliance, backup, and security awareness solutions, with a particular focus on protecting Microsoft 365 environments. Its portfolio brings together email security, backup and recovery, data protection, permission management, and human risk management delivered via a multitenant, all-in-one platform, giving organizations and MSPs a broader alternative to fragmented point-product deployments.

This integrated approach is especially relevant for service providers that need to deliver consistent protection across multiple customer environments. Centralized management, Microsoft 365 integration, and a portfolio spanning both technical and human risk controls help MSPs simplify service delivery, standardize onboarding, and reduce the operational complexity of managing separate security tools.

Beyond the technology itself, Hornetsecurity's channel proposition is strengthened by its partner engagement model. MSP interviewees highlighted responsive support, accessible account management, and a willingness to incorporate partner feedback into product development. These capabilities allow partners to package services more effectively, improve reporting, and support more strategic customer conversations around security posture, resilience, and compliance.

Note: *Following the completion of Proofpoint's acquisition of Hornetsecurity in December 2025, Hornetsecurity became Proofpoint's dedicated business unit focused on MSP and SMB cybersecurity solutions for Microsoft 365 environments: MSP Platform.*

Partner-Led Transformation Journeys

Frost & Sullivan interviewed Hornetsecurity MSP partners to assess how the company's portfolio supports partner-led customer transformation. The following journeys focus first on the MSPs' own operational and commercial transformation, then on partner-reported examples of downstream customer outcomes. Frost & Sullivan did not directly interview the end customers referenced in these examples unless otherwise stated.

LIMA: From Point-Solution Fragmentation to Strategic Microsoft 365 Security Partner

LIMA's relationship with Hornetsecurity began from an unusual starting point. The MSP had been using a backup solution that Hornetsecurity had acquired. Still, the initial perception was narrow: the technology was seen primarily as a backup product, and LIMA was considering offboarding it. The turning point came when Hornetsecurity demonstrated the platform's broader richness. LIMA realized that it could consolidate several separate tools and functionalities, repositioning Hornetsecurity as part of a broader Microsoft 365 security story. As LIMA explained, the shift was immediate: "This was an opportunity to consolidate email security, backup, permissions management, compliance, and security awareness services, that we had been positioning to customers as point solutions, into a more unified Microsoft 365 security proposition." Over roughly 18 months, the relationship evolved from a potential offboarding conversation to a more strategic partnership, with LIMA describing it as going from "zero to hero." The MSP also worked with Hornetsecurity on joint campaigns around Microsoft licensing, backup, and security. These activities helped initiate broader customer discussions around cyber resilience, Microsoft 365 governance, and long-term security strategy, supporting LIMA's advisory-led approach to customer engagement.

The transformation affected both LIMA's internal operations and its customer engagements. By reducing reliance on multiple point solutions, the MSP simplified both service delivery and the way it communicates Microsoft 365 security to customers. Rather than discussing individual products in isolation, LIMA was able to have broader conversations around security posture, resilience, backup strategy, governance, and risk management. The unified platform also supported more consistent reporting and enabled the MSP to position Microsoft 365 security as an ongoing business conversation rather than a series of standalone technologies. LIMA reported strong customer adoption following migration, with customers retaining and, in many cases, expanding their use of the Hornetsecurity portfolio.

One housing association initially questioned the value of the compliance module because it had not yet adopted some of the platform's newer capabilities. Working closely together, LIMA and Hornetsecurity reviewed the configuration and demonstrated additional functionality, helping the customer realize greater value from the solution.

Natpoint: Turning Security Data into Customer Conversations

Natpoint serves roughly 200 customers and has been migrating its customer base to Hornetsecurity over the past 18 months. The MSP had previously developed its own email security platform, but needed to replace and simplify its Microsoft 365 security stack. For Natpoint, a good product had to work reliably across a broad customer base, be manageable at scale, and come with a responsive vendor relationship. Hornetsecurity's partner model stood out because Natpoint could provide feedback, escalate issues quickly, and see suggestions incorporated into the product.

The most important operational change was the ability to generate meaningful customer-facing insight more quickly. Before deploying Hornetsecurity's 365 Total Protection, producing reports from Microsoft environments could take too long to support regular, high-value customer conversations. With Hornetsecurity, Natpoint could activate trials, show customers what was happening within their organizations, and use those findings to explain risk in a visual, commercially relevant way. As Natpoint stated, "It's enabled us to very quickly show high-value material to our customers, which beforehand we weren't doing because the time taken to get there was too long."

The downstream customer impact was broad. Natpoint reported that customers improved email security and Microsoft 365 backup coverage, including Teams, archive folders, and more complete Microsoft 365 stack protection. For customers using higher-tier products, Hornetsecurity's 365 Permission Manager gave Natpoint visibility into SharePoint and OneDrive risks, including anonymous links and long-running shares that had not been closed.

Natpoint also provided strong partner-reported evidence around Human Risk Management (HRM). In one charity with approximately 100 staff, the MSP observed that about 50% of employees initially clicked simulated phishing emails. Over the following year, the partner reported that users became "much, much more aware." More broadly, Hornetsecurity's reporting gave customer leadership teams clearer visibility into employee risk and training participation, turning security awareness into a measurable governance issue. In one case, the initial results prompted the board to make training mandatory and set a 100% compliance target. Other customers established 80% targets and began reporting progress regularly at board level.

veraTECH Solutions: Fast Deployment and Post-Delivery Remediation for Small Businesses

veraTECH Solutions focuses heavily on small businesses, particularly organizations with fewer than 50 seats, with a strong presence in healthcare and professional services. The MSP first adopted Hornetsecurity via backup technology and later expanded to include the email security suite. veraTECH had used a previous email security vendor, but felt the solution was not keeping pace with the threat landscape. The MSP was particularly attracted to Hornetsecurity's hybrid email security approach, combining gateway-level protection with direct Microsoft 365 access.

This integration filled an important security gap. veraTECH's previous solution operated only as a gateway and did not have API-level access into Microsoft 365 mailboxes. Hornetsecurity's connection to the tenant enabled mailbox-level actions after delivery, giving the MSP stronger remediation capabilities and better operational control. The MSP also highlighted usability, reduced technician effort, and fast support response as key differentiators.

Onboarding was another major improvement. veraTECH described Hornetsecurity's Microsoft 365 deployment as a "one-button" process that establishes the tenant connection, configures inbound and outbound transport rules, and pulls relevant Microsoft 365 user and mailbox information. Outside that workflow, the main remaining step is the MX record change, which the MSP characterized as simple.

The strongest downstream customer example involved post-delivery phishing remediation. veraTECH reported that when a phishing email slipped through and a user clicked it, the same message was also delivered to two other mailboxes. The MSP used Hornetsecurity to remove the message from those mailboxes before the other users opened it. As the partner explained, "within a matter of seconds," it could pull the phishing email out of every affected mailbox. This capability helped veraTECH provide better protection even when an initial email bypassed preventive controls.

Customers also noticed improvements in the email digest report. veraTECH reported that Hornetsecurity's customizable digest made it easier for users to manage quarantined messages, allow lists, and block lists without relying as heavily on MSP technicians. This improved the end-user experience while also saving technician time.

PORTFORMANCE: Long-Term Platform Expansion for Mid-Market Security Delivery

PORTFORMANCE has worked with Hornetsecurity since 2011, giving it a long-term view of the company's evolution from email filtering into a broader Microsoft 365 security portfolio. This MSSP focuses on organizations with their own IT departments, typically ranging from 100 to 5,000 employees. Its customers include logistics companies, hospitals, insurance organizations, and other mid-market businesses that need security expertise without necessarily outsourcing all IT operations.

For PORTFORMANCE, Hornetsecurity's value has expanded significantly as the portfolio has grown. The MSSP emphasized the benefits of having email security, backup, permission management, and other modules in a single all-in-one package. This integrated model reduces the need for customers to purchase and manage multiple products, while also helping PORTFORMANCE sell broader plans and build stronger long-term customer relationships.

Microsoft 365 integration is central to the operational story. PORTFORMANCE reported that onboarding has become easier, especially for larger customers. While changing a firewall can become a major project, the partner indicated that a typical Hornetsecurity customer can often be onboarded in 4 to 8 hours, depending on the plan, and email-security-only deployments can take around 1 hour. For larger environments, templates and established processes help the MSSP accelerate deployment.

PORTFORMANCE also provided strong partner-reported customer examples. One customer, preparing for a new investor, used 365 Permission Manager and discovered that former management still had access to company files via OneDrive. The tool surfaced the issue quickly, allowing the organization to address a previously invisible governance and access risk. In another case, a customer undergoing onboarding was hit by a large email attack involving approximately 100,000 highly malicious messages in an hour. Hornetsecurity blocked most of the attack even though the configuration was not fully complete.

Hornetsecurity enables MSPs to deliver a more integrated Microsoft 365 security model across email security, backup, permission management, and awareness. Several partners contrasted this approach with fragmented point-solution stacks that were harder to manage, explain, and commercialize.

Claudio Stahnke
Senior Industry Analyst

In HRM, PORTFORMANCE described a large automotive transportation customer that received an automated phishing simulation referencing an evacuation plan. Among the first 843 emails sent, 99% of users clicked, exposing a significant vulnerability to highly contextual phishing. Following the simulation, the customer continued with Hornetsecurity's ongoing automated training program, while its Employee Security Index reflected the initial decline and subsequent improvement in employee resilience. The case demonstrates how realistic simulations can uncover hidden behavioral risks and provide a measurable basis for continuous training, rather than relying on one-off annual awareness sessions.

Transformation Outcomes

Integrated Microsoft 365 Security Delivery Through MSPs

Hornetsecurity enables MSPs to deliver a more integrated Microsoft 365 security model across email security, backup, permission management, and awareness. Several partners contrasted this approach with fragmented point-solution stacks that were harder to manage, explain, and commercialize. LIMA's ability to consolidate several point solutions under one umbrella is the clearest example of this transformation. PORTFORMANCE similarly emphasized the value of a complete bundle, while Natpoint highlighted improved email security, broader Microsoft 365 backup coverage, and permission visibility across SharePoint and OneDrive.

This integration matters because Microsoft 365 risk is not limited to one control layer. Customers need email protection, backup and recovery, secure collaboration, permission governance, and user behavior improvement. MSPs are often responsible for converting these needs into manageable services. By giving partners a more cohesive portfolio via a central multitenant console, Hornetsecurity helps them reduce tool sprawl and deliver security in a way that customers can understand and adopt.

Greater Partner Efficiency and Faster Customer Onboarding

The MSP interviews show that Hornetsecurity can improve partner efficiency by reducing deployment friction, simplifying administration, and supporting repeatable service delivery. veraTECH described Microsoft 365 onboarding as a one-button deployment process, with MX record changes as the main additional step. PORTFORMANCE reported that a typical customer can often be onboarded in 4 to 8 hours, depending on the plan, or in about 1 hour for email-security-only deployments. Natpoint is migrating approximately 200 customers to Hornetsecurity, reinforcing the importance of manageability at scale.

Efficiency gains are not limited to deployment. Partners also highlighted responsive support, escalation paths, customer-facing reporting, and product feedback loops. Natpoint and LIMA both emphasized Hornetsecurity's willingness to listen to partner suggestions and collaborate on improvements. For MSPs, this matters because service delivery depends not only on product functionality but also on the vendor's ability to support the partner as customer requirements evolve.

From Security Data to Board-Level Customer Action

One of the strongest transformation patterns is using security data to improve customer conversations. MSPs repeatedly described the importance of translating technical telemetry into business-relevant insight. Natpoint used Hornetsecurity reporting to show customers what was happening inside their organizations and make cybersecurity understandable to nontechnical leaders. The partner also reported that HRM data, including training compliance and user risk patterns, became board-level material for several customers.

This is especially important in HRM and permission management. Security awareness results can prompt customers to set training-compliance targets, investigate performance changes, and reinforce a stronger security culture. Permission reports can reveal anonymous links, long-running shares, or inappropriate access by former employees. These insights help MSPs move beyond tool administration and act as strategic advisors. For customers, the value lies in making risk visible, measurable, and actionable before it becomes an incident.

Insights for CISOs

Security leaders evaluating MSP-delivered Microsoft 365 security should focus on operational evidence, governance visibility, and partner accountability.

Treat Microsoft 365 as an operating environment, not a control: Email, collaboration, identities, permissions, and backup require coordinated protection. CISOs should assess MSPs on cross-tenant visibility, post-delivery remediation, recovery coverage, and actionable Microsoft 365 security reporting for risk-led business decisions.

Use partner reporting to drive governance: Security data becomes valuable when translated into executive actions. Require recurring reviews that connect blocked threats, backup status, permission risks, awareness performance, and remediation priorities to business outcomes and accountability.

Prioritize automation without losing accountability: Automated onboarding, phishing simulations, digest reports, and mailbox remediation can reduce friction for MSPs. CISOs should still define escalation paths, response authority, service expectations, and ownership across every customer tenant.

Measure behavior, not completion alone: Training completion matters, but click patterns, reporting behavior, micro-learning engagement, and department-level risk reveal more. Use these insights to consistently target coaching, policy, communications, and investments with measurable follow-up actions.

Frost Perspective

MSP-delivered cybersecurity is becoming increasingly important as SMB and mid-market organizations depend more heavily on Microsoft 365 but lack the internal resources to manage security, backup, permissions, awareness, and reporting as separate disciplines. Hornetsecurity's partner-led value proposition is strongest where MSPs need to consolidate tools, simplify delivery, and convert technical security data into customer action.

The interviews show that the company's portfolio supports both operational efficiency for MSPs and downstream customer resilience. Partners can onboard customers more consistently, remediate email threats after delivery, improve Microsoft 365 backup coverage, identify permission risks, and use awareness metrics to elevate security discussions with executives. To maximize value, MSPs should package Hornetsecurity around measurable service outcomes, recurring business reviews, and maturity expansion rather than positioning it as a set of disconnected modules.

Looking forward, Frost & Sullivan expects MSP-focused security platforms to become more integrated, automated, and insight-driven. Vendors that help partners reduce complexity while strengthening customer governance will be best positioned to scale through the channel.

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied to us by manufacturers or users. Quantitative market information is based primarily on interviews and is therefore subject to fluctuation. Frost & Sullivan research services are limited publications that contain valuable market information and are provided to a select group of customers. Our customers acknowledge that, when ordering or downloading, Frost & Sullivan research services are for customers' internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to non-customers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the permission of the publisher.

For information regarding permission, write to: permission@frost.com

Frost & Sullivan Analytics Methodology & Next Steps

Frost & Sullivan Analytics Methodology

Analytics Conceptualization	• Internal topic review by analytics team • Review with commercial team and clients • Develop scope • Develop assumptions and availability of existing data and analytics • Develop detailed outline

Data Procurement	• **Primary research (80%)**
	  ○ Vendors and service providers
	  ○ Customers
	  ○ Value chain partners
	  ○ Trade associations
	• **Secondary research (20%)**
	  ○ Publications
	  ○ Ecosystem websites
	  ○ Online databases
	  ○ Search engines and Generative AI tools

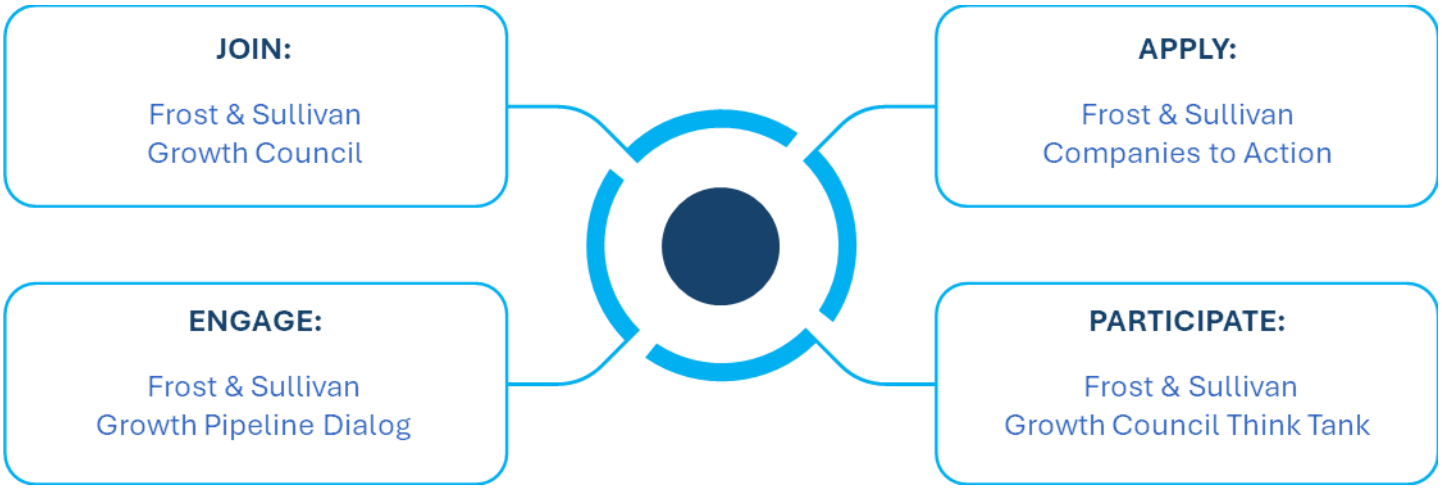
Data Analysis	• Consolidate data collected from secondary sources that is validated with primary interviews • Collate data from internal and external experts • Develop and produce quantitative models and forecasts • Identify data gaps for additional primary interviews
Analytics Intelligence	• Develop analytics structure based on initial outline • Qualitative content development • Quantitative data development • Identify data gaps for additional primary interviews
Analytics Delivery	• Project management and peer review • Editing and quality control checks • Delivery of analytics to clients using multiple delivery mechanisms

DATA VALIDATION (INTERNAL EXPERT & PRIMARY INTERVIEWS)

Source: Frost & Sullivan

Next Steps: Benefits & Impacts of Growth Opportunities

Next Steps: The Transformational Growth Partnership



Source: Frost & Sullivan