Partner Strategy

Managed security services: How partners are becoming cyber risk owners

Managed security services are transforming cybersecurity partners into risk owners. AI-driven platforms, automation and outcome-based models are reshaping partner ecosystems and driving recurring revenue growth.

Bharti Trehan
23 Apr 2026 15:05 IST

Managed security services: How partners are becoming cyber risk owners

Cybersecurity is going through a quiet but fundamental shift. Not in tools. Not in technology. But in responsibility.

In an interaction, **Govind Rammurthy**, **CEO and Managing Director at eScan**, described how the partner ecosystem is moving from selling products to owning security outcomes.

This transition is not optional anymore. It is being driven directly by customer expectations, regulation, and the realities of modern cyber risk.

Partners are no longer just resellers. They are becoming risk owners

The traditional reseller model still exists. And it still works for some customers. But a growing segment of partners is being pulled toward managed services and outcome-based security.

"We don't force partners into MSP models they're not ready for, but for those who want to evolve, we train them to deliver managed services profitably," Rammurthy explained. The challenge, he noted, is not technology. It is clarity.

Partners often struggle with undefined service scope, where customers expect far more than what was originally agreed.

"We help partners define clear service boundaries upfront so they can maintain profitability while delivering value," he said. That clarity is becoming critical as expectations shift toward outcomes.

Compliance is forcing a shift from features to guarantees

Regulation is playing a bigger role than many expected. The demand is no longer about installing solutions. It is about proving results.

"Customers are now asking whether we can guarantee compliance outcomes instead of just deploying software," Rammurthy noted.

This is a subtle but powerful change. It forces partners to rethink how they position cybersecurity. Instead of selling features, they are being pushed to sell assurance. Measurable, enforceable outcomes tied to risk and compliance.

Platforms are evolving to support continuous security operations

Technology is adapting to this shift. Modern cybersecurity platforms are being designed for multi-customer, always-on environments rather than single deployments.

"Our platform allows partners to manage multiple customers from one console, with centralised alerts and automated patching," Rammurthy explained. Automation is playing a decisive role here.

"When ransomware triggers an alert at 2 AM, the system can isolate the endpoint and capture

forensics automatically," he said.

This reduces dependency on manual intervention and allows partners to scale operations without proportional increases in manpower.

The economics of managed services depend on reducing noise

One of the less discussed challenges in cybersecurity is alert fatigue. Too many alerts. Too much noise. Too little signal.

"Partners cannot build profitable services if most alerts turn out to be false positives," Rammurthy pointed out. Reducing this noise has a direct financial impact.

"Our detection improvements reduced alert volumes significantly while maintaining threat detection rates," he added. This is where AI and automation move from being buzzwords to business enablers.

Outcome-based security demands shared accountability

As cybersecurity shifts toward outcomes, the question of responsibility becomes more complex.

Who is accountable when something goes wrong?

"The OEM ensures detection capability, while partners ensure proper deployment and response," Rammurthy said. But real-world scenarios are rarely that simple.

"If a customer ignores remediation recommendations, that decision must be documented to protect all parties," he explained. This highlights the need for clearly defined SLAs.

"Outcome-based contracts must define measurable criteria, not vague promises," he added.

Partner programmes are being rebuilt for recurring revenue

The shift to managed services is forcing OEMs to rethink their partner programmes. Transactional models are no longer sufficient.

"We restructured our program to support recurring revenue models and make them genuinely profitable," Rammurthy said. Infrastructure is also being reimagined.

Instead of partners building their own backend systems, OEMs are offering shared cloud

infrastructure.

“This allows smaller partners to enter the managed services space without a large upfront investment,” he noted. The result is a more inclusive ecosystem, where scale is not limited by capital.

Automation and consolidation are redefining profitability

Operational efficiency is now directly tied to margins. Automation reduces the need for manual analysis. AI reduces noise. Platform consolidation reduces complexity.

“Automation can eliminate a large portion of routine work, allowing analysts to focus on real investigations,” Rammurthy explained. Managing multiple tools is no longer viable.

“Partners cannot efficiently operate across multiple vendor consoles, so unified platforms are becoming essential,” he said. This is not just about convenience. It is about survival in a margin-sensitive business.

The future: a split ecosystem with two clear partner models

Looking ahead, the partner landscape will not converge. It will divide.

“Some partners will remain resellers, while others will fully own managed security outcomes,” Rammurthy observed. Both models will coexist. Both will be profitable. But managed service providers will increasingly specialise.

“Successful MSPs will focus on specific industries rather than trying to serve everyone,” he said. This vertical focus will allow deeper expertise, stronger differentiation, and better pricing power.

The bigger shift: OEMs becoming platforms, partners becoming brands

Perhaps the most significant transformation is structural. OEMs are moving toward platform models. Partners are becoming the customer-facing layer.

“OEMs are evolving into infrastructure providers, while partners build services on top of them,” Rammurthy said. This reverses the traditional dynamic.

Partners become the brand customers trust. OEMs become the engine behind the scenes. And in that model, success is no longer defined by product features. It is defined by how effectively partners can deliver outcomes at scale.