RedQor

HOW TO PACKAGE AND PRICE

YOUR CYBERSECURITY SERVICES

Packaging and pricing your cybersecurity services isn't just about slapping some numbers on a laundry list of tasks. There are many nuances – the right strategy can help you effectively communicate the value you deliver, position your offerings competitively, drive predictable revenue, and stay profitable.

Well defined packages make it easier for MSPs to scale their services and allocate resources cost-efficiently. You can set realistic expectations to improve customer satisfaction and retention. Additionally, a clear and transparent pricing strategy reflects professionalism and competence to help you build trust and augment your brand reputation.

After working with many MSPs over the years, we know how challenging packing and pricing can be. While there's no one-size-fits-all answer, there is a method to the madness. Let's review the core and optional services you should include in your cybersecurity packages, the most commonly used MSP pricing models, and what to consider when creating your service packages.

What MSPs should include in cybersecurity packages

Your basic packages should cover core services like:

RISK ASSESSMENTS

VULNERABILITY SCANNING

COMPREHENSIVE REPORTING

SIEM
(security, information, and event management)

XDR
(extended detection and response)

24/7/365 SOC
(security operations center)

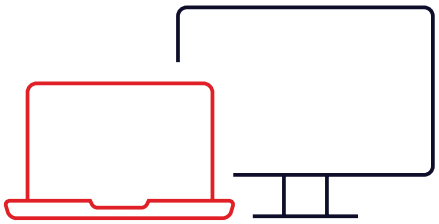
Consider offering add-on services or bundles to differentiate your services and deliver more value. You may include penetration testing, email security, cloud security, patch management, vCISO services, incident response, data loss prevention (DLP), identity access management (IAM), and zero trust network implementation.

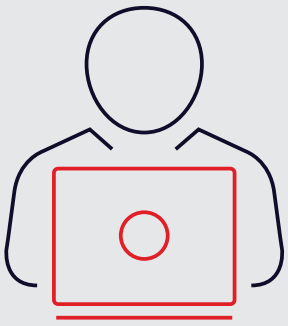
MSP pricing models for cybersecurity services

HERE ARE THE PRICING MODELS MOST COMMONLY USED BY MSPS

Per Device

This model involves charging a fixed amount (e.g. monthly) for each device, and the fee depends on the type of device. This pricing model is simple to execute and easy for clients to understand while providing the flexibility to adapt to changes quickly. However, the billing structure can get complicated as clients add more devices to their networks or implement a bring-your-own-device (BYOD) policy.



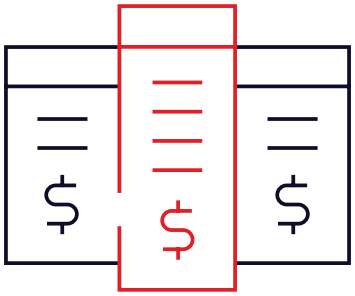


Per User

You charge a flat monthly fee for supporting each user.
This easy-to-understand and flexible pricing model is popular among companies that need to ensure end-users stay connected with multiple devices. However, your revenue may fluctuate depending on a client's employee base. You may see increased costs without adding income if the employee count stays constant but the number of devices rises.

Tiered/Bundle

This model involves building several bundled service packages (e.g. basic, pro, premium) available at different price points based on the type of services, features, and support levels to meet various budget and security requirements. However, you must invest effort into crafting compelling packages that meet client demand and manage them efficiently to drive profitability.

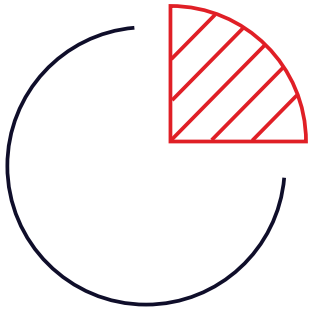


Value-Based ("Cake" Pricing)

You provide all services at a flat fixed rate and act as the extension of the client's IT department. This easy-to-implement model allows you to adjust pricing based on the expected value/outcomes. You can increase profitability while delivering better services. However, some clients may get confused because they can't see a breakdown of the tasks. Also, unforeseen issues may erode your margins.

A la carte

Clients can choose from a menu of standalone services (e.g. patch management and managed backup and disaster recovery) to meet their needs. This pricing model attracts clients who prefer the flexibility to mix and match services. However, managing these custom packages is typically more costly for MSPs because you must tailor communication plans, reporting, and workflows for each client.



What MSPs should consider when packaging cybersecurity services

The "bundle and save" approach offers financial incentives for clients to add multiple services. It encourages long-term and strategic relationships, which often help improve client retention. Meanwhile, the "a la carte" approach allows customers to buy a single service to fill immediate gaps or meet a specific need. Some prefer to start small and build trust with an MSP before committing to a more comprehensive package.

CONSIDER THESE QUESTIONS WHEN DESIGNING YOUR PRICING AND PACKAGING STRATEGY:

- Does the pricing structure support ongoing, predictable revenue?
- Do your bundles include features that address your target audience's needs?
- Are the packages positioned to help differentiate your brand in the market?
- Is the pricing approach transparent and easy to understand?
- Does the pricing balance competitive pricing with maintaining healthy profits?
- Are the packages scalable to support your growth plan?
- Can your pricing models help you improve resource allocation and forecast?
- Can the packages help you penetrate new markets or grow your existing accounts?
- Can you adapt your offerings to meet fast-shifting cybersecurity requirements?
- Do your packages align with your brand image and marketing communication?

Most MSPs will benefit from creating a default pricing model that meets most clients' needs with gross margins of

over 60%.

If you invest in advanced technology (e.g., AI and automation), you should target a gross margin of

over 70%.

Price your packages to grow your revenue and profitability

Well-designed pricing and packaging can help you attract more clients and generate more revenue. However, you must also consider the other side of the profitability equation – costs – to ensure healthy margins while staying competitive.

Streamlining your workflows, automating processes, reducing administrative overhead, minimizing errors, and lowering labor costs all contribute to improving profitability. However, talent shortages and the high costs of hiring and training internal resources have become a profit killer for many MSPs trying to grow their business with cybersecurity offerings.

That's why more MSPs leverage remote staffing solutions to access the talent they need to deliver high-quality services while controlling their recruiting, administrative, and labor costs. However, not all staffing services are created equal. Cybersecurity is a highly specialized discipline, so your provider must have the resources and experience to deliver top-notch outcomes.

RedQor offers a one-stop cybersecurity solution with SOCaaS, M365 security, SaaS security, email security, and awareness training. We partner with leading vendors like inSOC, Augmentt, and Mesh to give you access to world-class security services designed exclusively for MSPs and MSSPs.

For example, we recently helped a large US-based MSP build a remote team to migrate its customers to inSOC, our SOCaaS partner.

Since our team has expertise with inSOC's technology and processes, our solution helped this client shorten time to value while reducing costs.

Learn more about our customized MSP security packages and get in touch to see how we can help.