monarx

WHITEPAPER

PRICING FOR HOSTING SECURITY

How to protect customers and drive revenue

A practical guide to setting the security baseline, packaging premium protection, choosing upsell moments, pricing the offer, launching a pilot and measuring results.

Based on an August 2026 analysis of 65 hosting providers with company examples, a practical implementation playbook, and ready-to-use worksheets.

PUBLISHED

September 2026

EXECUTIVE SUMMARY

Protect every customer, and still build security revenue

Hosting providers are trying to solve two problems at the same time: protect every customer site and create profitable security revenue. Basic protection should be part of the hosting service. Premium protection can then create additional margin when it delivers a clear, higher-value outcome.

The answer is not to choose one or the other. Start with a baseline that keeps the platform and every customer account reasonably safe. Then build paid tiers around stronger outcomes: proactive application-layer protection, deeper database cleanup, priority response, expert remediation and recovery commitments.

This guide shows how hosting providers are packaging security today and turns the findings into a practical playbook for product, revenue, security and operations teams.

The analysis shows three clear patterns: 37 of 65 hosting providers (57%) include advanced protection at no extra cost, 31 (48%) sell a separate website-security product, and 18 (28%) do both. Only 20 hosting providers (31%) publish a price for the add-on. The full breakdown is in Section 2.

57%

of providers (37 of 65) include advanced protection at no extra cost

48%

of providers (31 of 65) sell a separate website-security product

31%

of providers (20 of 65) publish a price for the security add-on

What this guide gives you

- A framework for evaluating the current security and packaging model.
- A four-model view of how hosting providers monetize security.
- A reference baseline and two-tier premium value ladder.
- Guidance on segmentation, pricing, messaging, checkout and in-product placement.
- A launch process covering billing, support, remediation, analytics and experimentation.
- An extended appendix with research methodology, worksheets, a pilot scorecard and company examples.

Contents

1	**Security and revenue are not a trade-off**	The cost of an add-on-only model
2	**What the market tells us about security packaging**	65 providers, four packaging models
3	**Build the right security package**	Baseline, premium tiers, funding
4	**How to build the model: a practical playbook**	Seven steps to launch
5	**A practical example**	Package, pricing and revenue model
6	**Launch, measure and optimize**	Pilot design and decision rules
7	**About Monarx and next steps**	Where to start
A–E	**Appendices**	Methodology, sources, worksheets, checklists

SECTION 1

Security and revenue are not a trade-off

Give every customer a meaningful security baseline, then build premium tiers around stronger protection. The two goals reinforce each other.

Hosting providers are trying to do two things at once: protect every customer site and grow security revenue. These goals do not have to compete. The strongest model is to give every customer a meaningful security baseline, then build premium tiers around stronger protection.

Historically, hosting providers separated security into two buckets: platform security was treated as a cost of running the service, while customer-facing website security was sold as a paid add-on. This created the impression that providers had to choose between protecting every customer and generating security revenue. In reality, the two can work together.

Why the split exists

- **Infrastructure and platform security:** controls operated by the hosting provider to protect servers, networks and the shared environment. These may include firewalls, malware detection, process monitoring, DDoS mitigation and abuse controls.
- **Customer-facing website security:** capabilities positioned as a visible service for an individual site or account, such as malware scanning, automatic cleanup, WAF coverage, vulnerability protection, reputation monitoring, security reporting or expert recovery.

This distinction is useful for packaging, but it is not a technical rule. Server-deployed security can still protect each customer site when it provides account-level detection, remediation and visibility. What matters is the outcome every customer receives, not where the software runs.

Look at the full cost

Security add-on revenue is easy to measure. The cost of infected sites is often spread across support, malware cleanup, abuse handling, IP reputation work, suspensions, cancellations and lost trust. Leave those costs out, and an add-on-only model can look more profitable than it really is.

Where an add-on-only model breaks down

Premium security can be a strong revenue product. The problem starts when meaningful protection is available only to customers who notice, understand, and buy the add-on. Everyone else can still create security risk and operational cost for the provider.

- More infected sites and abuse incidents across the fleet.
- Higher support and remediation workload.
- More account restrictions or suspensions, with associated revenue loss.
- Customer frustration when a hosting plan described as secure does not prevent or remediate a common compromise.
- Risk that paying customers share infrastructure and IP reputation with compromised neighbors.

30%

Account infection rate at hosting providers where security comes primarily from open-source tools and site-security add-ons

Source: Monarx analysis of customers migrating to Monarx from those solutions.

EVIDENCE FROM ONE DEPLOYMENT

In one hosting environment where the only malware protection was a legacy signature-based scanner sold as a paid add-on, Monarx found active infections affecting **30% of hosted users** at full deployment. Around **1,000 accounts** were being suspended each month, and between **5% and 10%** of accounts suspended after a malware incident went on to cancel service, roughly 100 lost accounts a month at the upper end of that range. That attrition placed approximately **$18,000 of annual recurring revenue at risk each month**, or about **$216,000 across a year**.

This is one deployment, not a market average. It shows the type of cost an add-on-only model can create. Results will vary by account mix, security posture and operating model.

The better model

Hosting providers do not have to choose between customer security and margin. A stronger model gives every customer essential protection, then creates a clear path to paid outcomes that are easier to understand and sell. The next sections show how to build it.

SECTION 2

What the market tells us about security packaging

In August 2026, Monarx analyzed 65 hosting providers, reviewing public pricing, product and support pages, to answer two questions: what protection is included with hosting, and what security products are sold separately.

There is no single industry standard. Packaging depends on the provider's segment, base-plan price, operating model, brand and the role security plays in the platform. The analysis groups the market into four practical models.

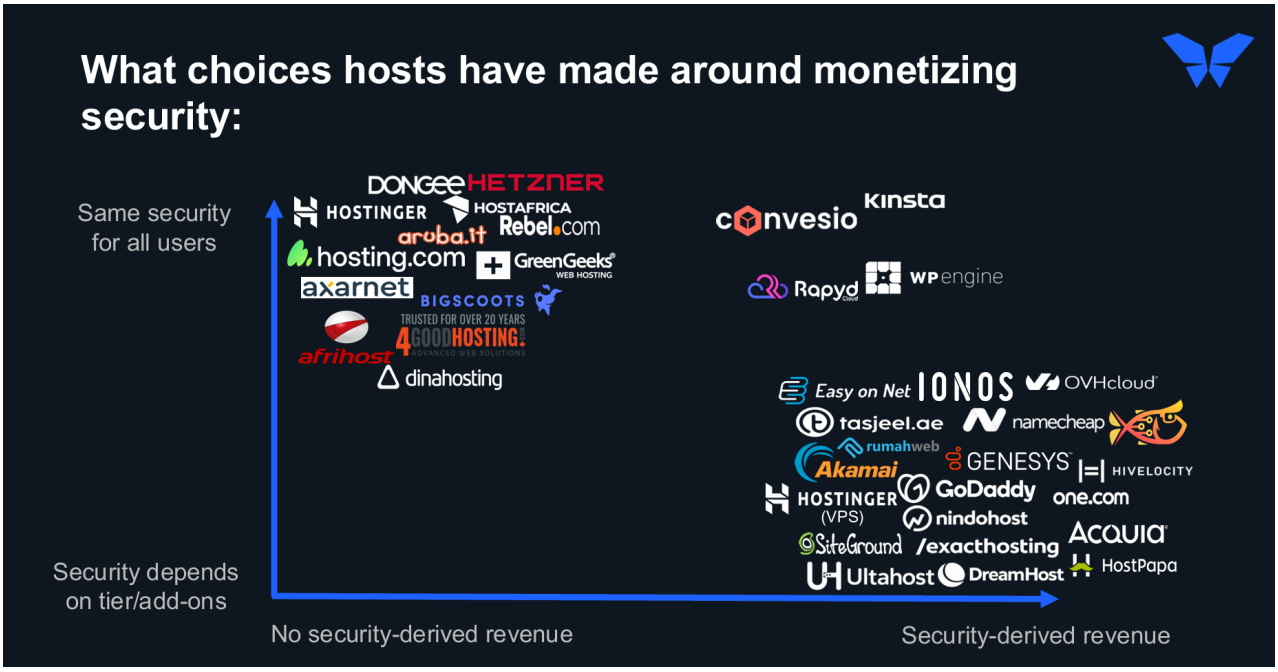


Figure 1. How hosting providers position security across included protection and security-derived revenue. Source: Monarx analysis of public hosting pricing and support pages.

Four packaging models

A

Included platform security

Malware and firewall protection is included across the core hosting range. Security is not sold as a separate SKU.

ADVANTAGES

Simple customer story, broad protection, lower platform risk.

RISKS

No direct security attach revenue; investment must be justified through retention, differentiation and lower operating cost.

B

Add-on-led security

Core plans include only basic platform controls; customer-facing malware or WAF protection is sold separately during checkout or later.

ADVANTAGES

Clear incremental revenue and easy price discrimination.

RISKS

Protection depends on customers seeing and buying the add-on; support still carries the risk from accounts that decline.

C

Premium bundled security

A higher base hosting price funds a broader security and managed-service bundle.

ADVANTAGES

Strong premium positioning and consistent protection.

RISKS

Hard to apply to low-cost hosting; fewer additional upsell opportunities.

D

Baseline plus premium upsell

Malware detection and automatic file remediation are included for all customers, with paid tiers for application-layer protection, deeper cleanup and expert recovery.

ADVANTAGES

Balances fleet-wide safety with a clear monetization ladder.

RISKS

Requires clear feature boundaries, billing rules, lifecycle messaging, remediation ownership and support readiness.

Company examples

The examples below show how providers present different packaging models to customers. They illustrate positioning and packaging rather than the relative effectiveness of the underlying security technology.

Provider	Illustrative model	How the offer is presented
hosting.com	A. Included platform security	Core hosting pages state that every plan includes malware protection; its managed WordPress security page describes always-on WAF, monitoring and cleanup included with every plan.
GoDaddy	B. Add-on-led security	Website Security is sold in Standard, Advanced and Premium tiers with malware scanning, WAF and different cleanup allowances; some hosting products include a trial or bundled access.
Convesio	C. Premium bundled security	Managed WordPress plans position security as part of the premium hosting package, including Cloudflare, malware scanning and hack repair.
Rapyd Cloud	D. Baseline plus premium upsell	All plans include firewall, DDoS protection and automatic malware detection, with Advanced SiteShield offered as a separately priced add-on.
Bluehost	B. Add-on-led security	Core plans include WAF and DDoS protection, while a separate website-security product is sold alongside hosting in three priced tiers.
DreamHost	B. Add-on-led security	Some current hosting plans include monthly DreamShield scans, while DreamShield Protect is sold separately for daily scans and additional monitoring.

Packaging examples in practice

Provider screenshots make the packaging models easier to understand at a glance. The following examples include security, paid add-ons, and premium bundles as presented on provider websites in August and September 2026.

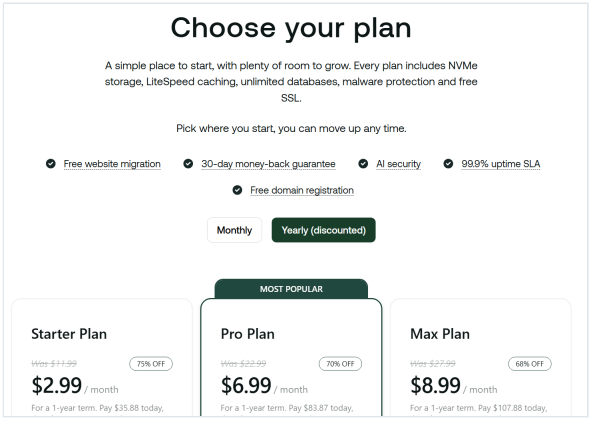


Figure 2. hosting.com presents malware protection as part of the core hosting package. Source: hosting.com, accessed August 2026.

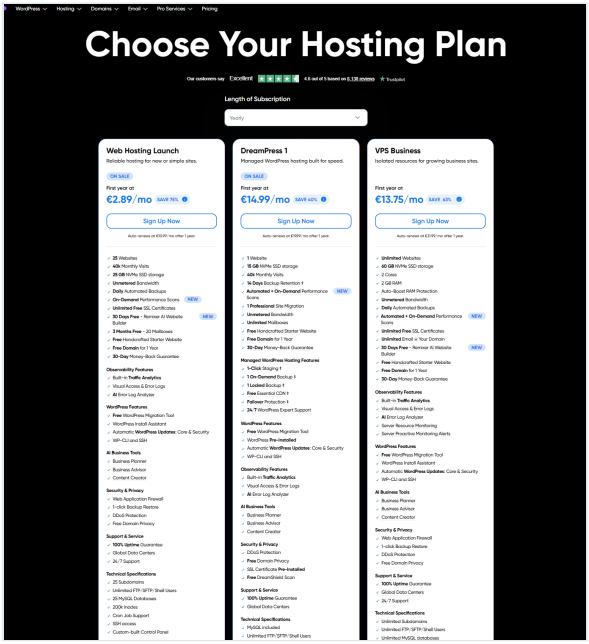


Figure 3. DreamHost presents DreamShield as a per-site security add-on. Source: DreamHost, accessed August 2026.

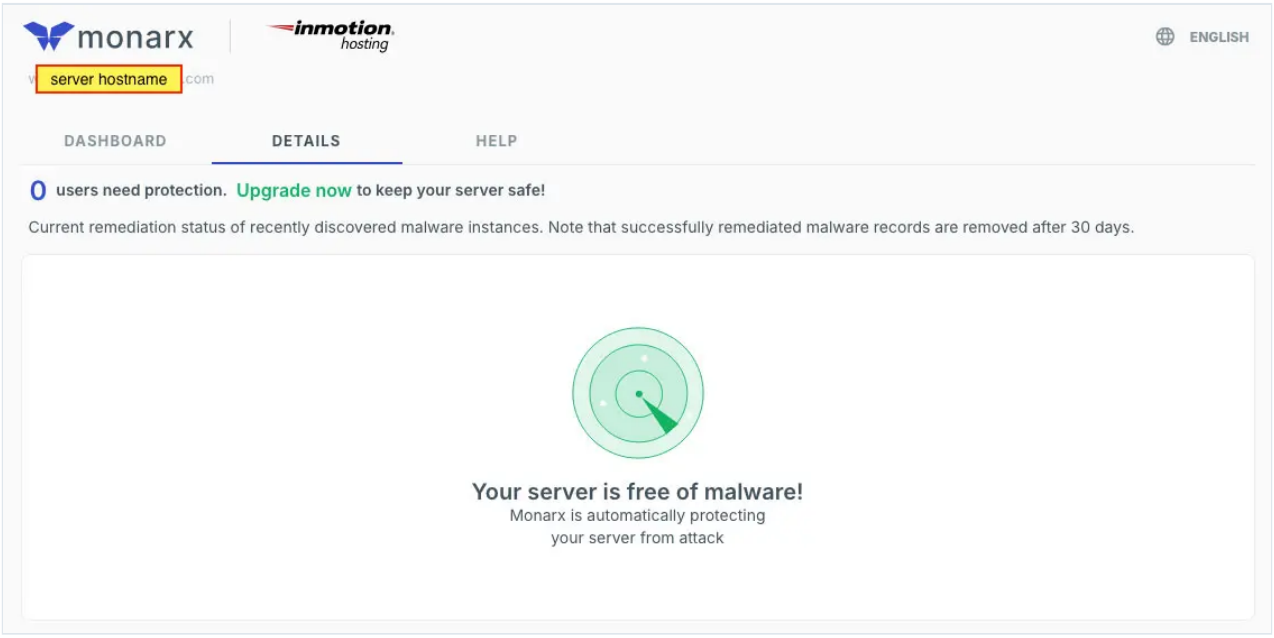


Figure 4. InMotion Hosting integrates Monarx directly into its hosting environment, giving customers visibility into their malware status. Source: InMotion Hosting, accessed August 2026.

What the analysis found

For each provider, the analysis captures what a prospective customer can see: what the hosting plan includes, whether a separate security product is sold, what it contains and what it costs.

How security is positioned	Providers (of 65)
WHAT THE HOSTING PLAN INCLUDES AT NO EXTRA COST	
Advanced website protection included (dataset classification)	37 (57%)
Basic platform controls only; advanced website protection not included in the core plan	12 (18%)
Advanced website protection explicitly excluded from the core plan	4 (6%)
Not classified	12 (18%)
WHETHER A SEPARATE SECURITY PRODUCT IS SOLD	
Website malware or WAF product sold separately	31 (48%)
Only non-malware add-ons sold: SSL, backup, email or domain privacy	9 (14%)
No separate security add-on found	4 (6%)
Public information reviewed but inconclusive	2 (3%)
Not classified	19 (29%)

Table 1. Two independent codings of the same 65 hosting providers; each block sums to 65. Percentages use 65 as the denominator and may not total 100% because of rounding. "Advanced website protection" is the classification used in the August 2026 analysis and describes the published offer, not independently tested effectiveness. "Public information reviewed but inconclusive" means the pages were checked but did not answer the question.

Included protection is already common

37 of the 65 hosting providers (57%) include advanced protection at no extra cost, while only four (6%) explicitly exclude it. Including a credible baseline is already a common market position. Just as importantly, included protection and paid security are not alternatives: 18 of those 37 providers (49%) also sell a separate website-security product. All four hosting providers that explicitly exclude advanced protection sell a paid security product instead.

Segment	Providers	Advanced website protection included at no extra cost	Sell a separate website-security product
Mass-market / large hosting brands	12	5 (42%)	10 (83%)
Independent / smaller and mid-sized hosting	46	26 (57%)	18 (39%)
Hosting focused on Managed WordPress	7	6 (86%)	3 (43%)

Table 2. The August 2026 analysis split by provider segment. Percentages are calculated within each segment.

The clearest difference is between mass-market and managed WordPress providers. Among mass-market and large hosting providers, 42% include advanced protection and 83% sell a separate product. Among managed WordPress hosting providers, 86% include advanced protection and 43% sell an add-on. These segments are making different promises to customers, so providers should choose the model that fits their market and operating structure.

Who the security add-on is branded by

Selling a security add-on does not require building the product. Among the hosting providers that sell a revenue-driving security add-on, most put someone else's brand on it, which shapes how much margin the provider keeps and how much of the security story belongs to the host.

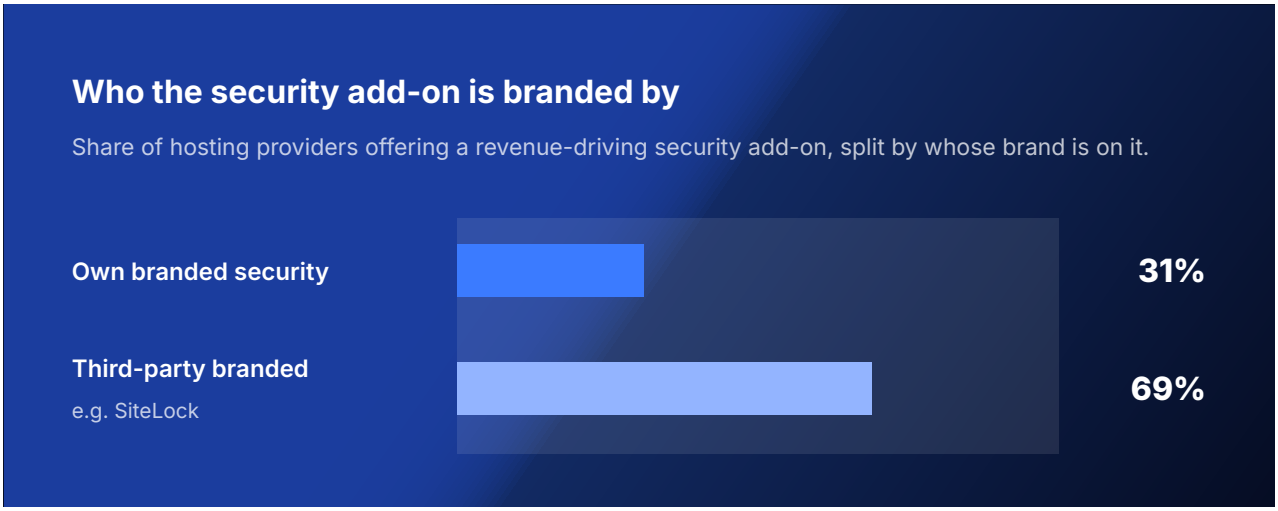


Figure 5. Of the hosting providers selling a revenue-driving security add-on, roughly two in three present it under a third-party brand. Source: Monarx analysis of public hosting pricing and support pages, August 2026.

Published security add-on pricing

What we measured	Result	What it means
Providers analyzed	**65**	Total research sample.
Providers publishing a security add-on price	**20 of 65 (31%)**	20 of 65 hosting providers published a security add-on price and were included in the pricing analysis.
Published offers that could be compared directly	**10 of 20 (50%)**	These offers used per-site, monthly US dollar pricing.
Published offers excluded from direct comparison	**10 of 20 (50%)**	These used SSL-only, non-USD, per-server, estimated or unclear-period pricing.
Comparable entry-level price range	**$1.92–$7.99 per site/month**	A directional range for entry pricing, not a market median.
Midpoint of the 10 comparable entry prices	**$5.44 per site/month**	A reference point within this small comparable sample.
Providers using three or more visible tiers	**16 of 20 (80%)**	Multi-tier packaging is common among providers that publish pricing.

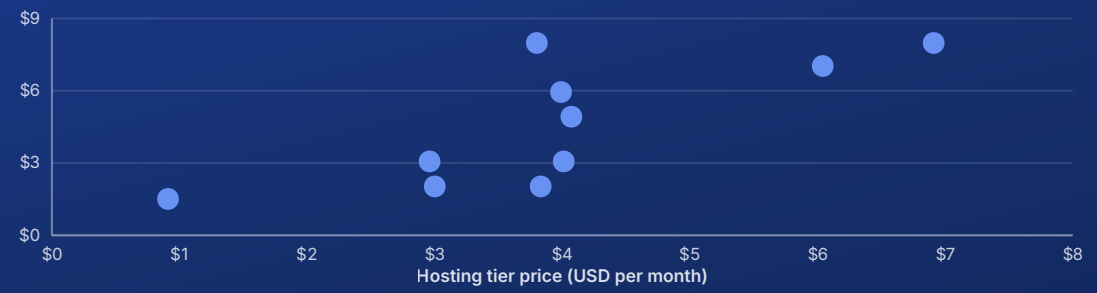
Table 3. Public security add-on pricing, August 2026. Percentages use the denominator shown in each row.

Of the 65 providers analyzed, **20 published a security add-on price and were included in this pricing analysis**. Ten of those offers could be compared directly because they used per-site, monthly US dollar pricing. Their entry prices ranged from **$1.92 to $7.99 per site per month**, with a midpoint of **$5.44**. Security pricing also varies relative to the underlying hosting package. In the August 2026 analysis, the lowest security tier was around 1.1x the price of the lowest hosting tier, while middle and highest security tiers were around 1.9x and 2.4x respectively. Looking at security pricing relative to hosting price can provide additional context across providers, markets and regions, but should still be treated as a directional benchmark.

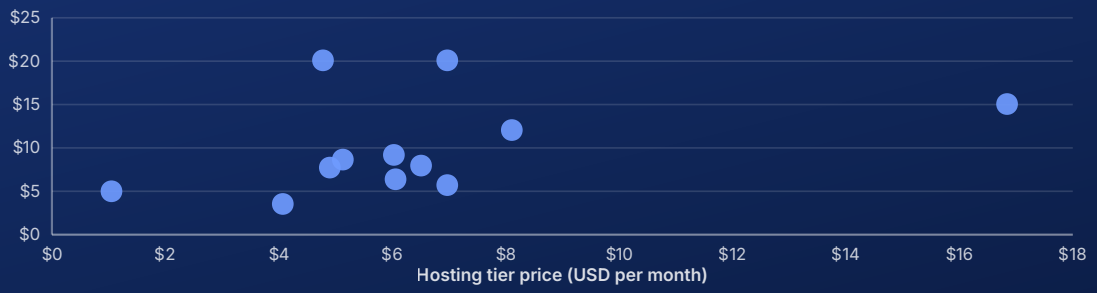
Security add-on price against hosting price

Each point is one hosting provider. Vertical axis: security add-on price at that tier; horizontal axis: hosting price at the same tier.

Lowest tier **add-on ≈ 1.1x the hosting price** 10 providers



Middle tier **add-on ≈ 1.9x the hosting price** 12 providers



Highest tier **add-on ≈ 2.4x the hosting price** 12 providers

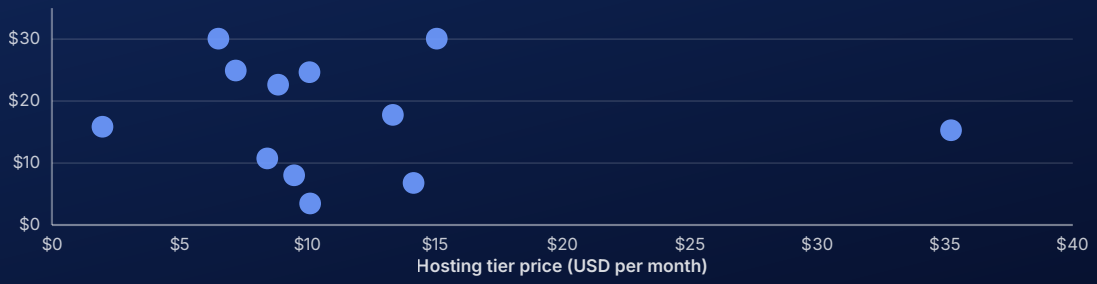


Figure 6. Security add-on price against hosting price at the lowest, middle and highest tiers. Source: Monarx analysis of public hosting pricing and support pages, August 2026.

Use the benchmarks as a starting point

The pricing data is a useful reference, not a fixed rule. Security offers vary by billing unit, feature scope, support level and renewal price.

Some products cover one site; others cover an account, plan, server or portfolio. The package may combine scanning, automatic cleanup, WAF protection, backups, monitoring or expert remediation.

Use the analysis to compare market ranges, included capabilities and upgrade logic. Final pricing should still reflect your customer segments, hosting prices, support model, delivery cost and target margin.

SECTION 3

Build the right security package

Include a meaningful baseline for every customer, then sell premium tiers that deliver stronger outcomes. This protects the fleet without giving up the revenue opportunity.

Security can and should drive revenue. But add-on revenue is less valuable when the base stack still leaves providers with widespread infections, support work, abuse, suspensions and churn.

For most shared hosting and managed WordPress portfolios, **Model D** is the strongest starting point: include a meaningful baseline for every customer, then sell premium tiers that deliver stronger outcomes. This protects the fleet without giving up the revenue opportunity.

Always include the essentials

Start with an always-on baseline that is strong enough to protect customers who do not buy an upgrade. The baseline should reduce avoidable infections, support work and platform risk. Define it at the same time as the paid tiers, rather than adding new SKUs around whatever tools already run on the servers.

Capability	Recommended position	Product rationale
Malware detection	Included	Detect known and suspicious malicious files across every account.
Automatic file remediation	Included	Remove or quarantine common infections without requiring a purchase after the incident.
Continuous or near-continuous scanning	Included	Avoid using scan frequency as the main reason to buy basic protection.
Malicious process detection and termination	Included	Stop active malicious behavior, not only stored files.

Capability	Recommended position	Product rationale
Customer dashboard and alerts	Included	Show security status and actions taken in a way customers can understand.
Platform-level WAF or equivalent request filtering	Include when the hosting stack supports provider-managed request filtering	Reduce common exploit traffic across the fleet.
Database scanning and cleanup	Typically paid tier 1	Find and remediate malicious injections and compromised content stored in the database, extending protection beyond files alone.
Proactive application-layer shielding	Typically paid tier 1	Block exploitation attempts at the application layer, including attacks targeting vulnerable software, before they can lead to compromise.
Human expert cleanup and recovery SLA	Typically paid tier 2	Adds expert-led cleanup, priority escalation and a defined recovery process.

Build premium tiers around stronger outcomes

Paid tiers need to offer more than extra scans. Tier 1 can add proactive protection and deeper cleanup for small businesses, agencies and higher-risk sites. Tier 2 can add expert recovery, priority response and service commitments for business-critical sites.

INCLUDED

Safe by default

BEST-FIT CUSTOMER

All customers

- ✓ Automatic detection and file remediation
- ✓ Continuous scanning
- ✓ Status dashboard
- ✓ Process protection
- ✓ Platform WAF where applicable

Malware detection and automatic file remediation are active across every account.

PAID TIER 1

Proactive Protection

BEST-FIT CUSTOMER

Small businesses, agencies, ecommerce sites and sites with prior incidents or higher revenue dependency

- ✓ Database scanning and cleanup
- ✓ Proactive application shielding
- ✓ Injection remediation
- ✓ Security seal
- ✓ More detailed reporting

Add application-layer protection, database cleanup and detailed incident reporting.

PAID TIER 2

Managed Recovery

BEST-FIT CUSTOMER

Sites where downtime, customer data or recovery time has a material business impact

- ✓ Everything in tier 1
- ✓ Expert cleanup
- ✓ Priority response
- ✓ Documented recovery scope
- ✓ Incident escalation and optional compliance reporting

Add expert recovery, priority response and a defined incident process.

Recommended security feature ladder

A safe baseline for every customer, with premium outcomes layered on top.

Capability	Included baseline	Paid tier 1	Paid tier 2
Malware detection	✓	✓	✓
Automatic file remediation	✓	✓	✓
Continuous or near-continuous scanning	✓	✓	✓
Customer security dashboard	✓	✓	✓
Database scanning and cleanup	×	✓	✓
Proactive application shielding	×	✓	✓
Injection attack remediation	×	✓	✓
Human expert cleanup and priority recovery	×	×	✓

Figure 7. Recommended feature ladder for combining an included security baseline with two differentiated premium tiers.

Fund the baseline before launch

An included baseline has a real cost. Before approval, decide how it will be funded and model the impact across the full portfolio.

Funding lever	How it works
Change the licensing unit	Server-level or fleet-level licensing decouples the cost of the baseline from the number of protected sites. Extending detection and automatic cleanup to every account then costs materially less per site than the retail price of a per-site add-on, which is what makes an included floor affordable at all.
Consolidate what is already being paid for	Most portfolios run overlapping scanners, a cleanup vendor, manual remediation hours and sometimes a third-party add-on billed through the control panel. Consolidating these often funds a large share of the baseline without any new budget.

Funding lever	How it works
Convert existing add-on subscribers rather than losing them	Customers already paying for basic scanning should move to a paid tier whose scope clearly exceeds the new baseline. This is a scope upgrade at the same price, not a downgrade, and it needs to be designed before launch rather than handled as an exception.
Price the baseline into the plan where the market allows it	A modest base-plan increase applied to new plans and at renewal, positioned as an included capability, is often more durable than add-on revenue with a low attach rate. Model this against competitor plan pricing, not against the add-on price.
Count avoided operational cost as real funding	Cleanup labor, abuse handling, IP reputation work, suspension-driven churn and security support contacts are the offset that justifies the baseline. They belong in the same business case as the add-on revenue, which is why the worksheet in Appendix C treats them as a single model.

Decide how existing subscribers will move before launch. They can keep their current price with broader coverage, move to the equivalent new tier, or receive a credit. Model the full cost of protecting the fleet, not only the accounts that would have bought an add-on anyway.

Choose the billing unit and pricing structure

- **Per site:** easiest for customer comprehension and evidence-based upsell, but can create friction for agencies and multi-site accounts.
- **Per hosting account or plan:** simpler operationally, but value can be unclear when one account contains many sites.
- **Per server:** appropriate for infrastructure products, but usually weaker for customer-facing self-service upsell.
- **Portfolio or agency pack:** useful for multi-site buyers and can improve attach rate by reducing repeated purchase decisions.

Choose the billing unit that matches how customers see value and what the platform can provision, meter, downgrade and report reliably.

SECTION 4

How to build the model: a practical playbook

The model only works when product, security, billing, support and customer experience are planned together. Seven steps from mapping the current setup to being operationally ready on launch day.

Start with the current setup, define the baseline and premium tiers, and make sure the operational commitments are ready before launch. Section 6 covers the pilot and measurement plan.

STEP 1

Map the current model and customer journey

Map the current setup before creating new tiers. Document what is included, what is sold separately, what customers are promised, what they actually receive, how incidents are handled and where revenue is generated.

- Inventory every included control, paid add-on, trial, manual service and third-party product.
- Map the provisioning unit: site, domain, account, server or plan.
- Document infection, cleanup, support, suspension and escalation workflows.
- Review all customer-facing claims on pricing pages, checkout, onboarding, the control panel and support content.
- Capture current metrics: infections, support tickets, cleanup cost, suspensions, attach rate, ARPU, churn and refunds.
- Identify gaps between the security promise and the actual customer outcome.

STEP 2

Set objectives and guardrails

Do not judge the program only by attach rate. Set revenue goals together with security, customer, operational and brand guardrails so the upsell improves the business without weakening the hosting product.

Objective area	Example goal
Commercial	Increase security ARPU, attach rate and gross contribution while keeping refunds and churn within agreed thresholds.
Security	Reduce infected accounts per 1,000 active accounts, abuse incidents and median time to remediation against the pilot baseline.
Customer	Confirm customers understand included versus paid coverage and keep complaint rates within the agreed threshold.
Operational	Keep provisioning failures, cleanup workload and security-related support contacts within agreed thresholds.
Brand	Document whether security is part of the host platform story, a co-branded specialist product or a third-party add-on.

STEP 3

Segment customers by risk and need

Customers buy security for different reasons. A hobby-site owner wants simplicity and automatic cleanup. An ecommerce business cares about revenue protection and fast recovery. An agency needs portfolio visibility and predictable cleanup. Use those needs to shape the tiers, pricing and messaging.

Segment	Context	Primary job	Likely offer
Personal or hobby site	Low business dependency; price-sensitive	Simple status, automatic cleanup, no technical maintenance	Included baseline; offer an upgrade only after a specific detected risk or stated customer need
Small business	Reputation, leads and local commerce depend on the site	Stay online, avoid blacklisting, recover without technical work	Tier 1 proactive protection
Ecommerce or membership	Transactions, customer data and logged-in users	Reduce exploit risk, protect revenue, prioritize recovery	Tier 1 by default; tier 2 when recovery time or incident support is critical
Agency or freelancer	Multiple client sites and repeated operational work	Portfolio visibility, bulk coverage, predictable cleanup	Agency pack or volume-priced tier 1

Segment	Context	Primary job	Likely offer
Revenue-dependent or regulated site	Downtime, customer data or incident response has material consequences	Defined response, expert cleanup and auditable reporting	Tier 2 Managed Recovery with a documented response commitment

STEP 4

Select the right upsell moments

Do not treat the upsell as one checkbox at checkout. Use the customer lifecycle: purchase, onboarding, routine management, security events, support, renewal and pre-suspension. At each stage, show what is already included and why the upgrade matters.



Moment	Customer context	Best use	Guardrail
Checkout	Customer is comparing plans and total price	A concise, optional protection upgrade with clear outcomes	Make the value of the upgrade clear without implying that the base hosting plan is unsafe.
Onboarding	Customer is configuring a new or migrated site	Security-health setup and a time-limited trial	Delay the upsell until the customer understands the baseline.
Control-panel dashboard	Customer is managing an existing site	Persistent but non-intrusive security status and upgrade path	Show current coverage before selling more.
Evidence-based alert	A scan finds malware, suspicious behavior or a specific unresolved risk	Show what was detected, what the baseline already fixed and which paid capability addresses the remaining risk	Do not hold basic remediation hostage if it is part of the baseline.
Support interaction	Customer asks about a compromise or prevention	Recommend a tier based on the detected issue, site type and required recovery time	Train agents to diagnose rather than default to the highest tier.

Moment	Customer context	Best use	Guardrail
Renewal or plan review	Customer is reassessing value and commitment	Move the customer to a plan or annual term that includes the relevant security tier	Be clear about what security is included in the renewed plan and what costs extra.
Pre-suspension workflow	An infected account may be restricted	Provide remediation steps, a timeline, a support route and an optional upgrade	Do not restrict access solely to force a purchase; provide a clear recovery path.

STEP 5

Set pricing and build the business case

Use market pricing as a check, not the pricing strategy. Set the price around the customer outcome, delivery cost, recovery commitment, target segment and relationship to the hosting plan.

- Start with willingness to pay by segment and the cost of delivering the promised outcome.
- Model both direct contribution and avoided cost: support, cleanup, abuse handling, suspensions and churn.
- Use promotional and renewal pricing transparently; calculate both in the unit economics.
- Keep tier differences easy to explain in one sentence.
- Test monthly, annual and portfolio pricing rather than assuming one billing structure.

CORE REVENUE FORMULA

Eligible accounts × attach rate × monthly price = incremental monthly recurring revenue. Subtract vendor cost, cleanup cost, support cost, payment fees, discounts and expected refunds to calculate gross contribution.

Rule of thumb for 100,000 eligible accounts: each 1 percentage point of attach rate equals 1,000 paid accounts. For a single $5.99 tier, that adds **$5,990 MRR** or **$71,880 ARR** before delivery and support costs.

STEP 6

Write clear messaging

Customers should immediately understand what the hosting plan already protects, what the paid tier adds and why the upgrade is valuable. Clear, evidence-based messaging builds trust. Vague or fear-based copy makes the base plan look unsafe.

Message role	Example language
Included baseline	Your hosting plan already includes continuous malware detection and automatic file remediation for common threats.
Tier 1	Add application-layer exploit protection, database cleanup and detailed reporting for threats that go beyond file malware.
Tier 2	Add expert cleanup, priority response and a defined recovery process for a revenue-dependent site.
Evidence-based prompt	We found a security issue on this site. Here is what we found, what we already fixed and which paid capability can address the remaining risk.
Agency offer	Protect and monitor all client sites from one place with portfolio pricing and consolidated reporting.

Avoid claims such as "complete security" unless the product can support them. State what is included, what the upgrade adds, what the customer still needs to manage and which response or recovery commitments apply.

STEP 7

Prepare operations before launch

A premium security tier creates real service commitments. Before launch, define provisioning and billing, remediation and escalation ownership, what support can see and promise, how false positives are handled, and what happens when a customer upgrades, downgrades or requests a refund.

Readiness area	Question to resolve
Provisioning	Can the platform enable, disable and migrate protection reliably at the chosen billing unit?
Billing	How are trials, prorating, annual terms, multi-site packs, renewals, refunds and downgrades handled?
Incident response	What is handled automatically, and who owns manual cleanup, escalation and customer communication?
Support	What can frontline agents see, explain and change? What is the escalation process and expected response time?
Product analytics	Can events be tracked from impression to purchase, activation, incident and renewal?
Legal and claims	Do the terms, service descriptions and guarantees match the actual scope and response commitments?
Existing customers	Will they receive the baseline automatically? Are paid products grandfathered, migrated or credited?

SECTION 5

A practical example

A complete product concept for a mid-market host: an included baseline, two premium tiers, a simple revenue model and a lifecycle that does not withhold essential protection from customers who decline the add-on.

Example package

INCLUDED WITH HOSTING

Baseline

Included in the plan price

- ✓ Continuous malware detection
- ✓ Automatic file remediation
- ✓ Process protection
- ✓ Customer dashboard
- ✓ Platform WAF where applicable
- ✓ Support through existing hosting support channels

Malware detection and automatic file remediation are active for every customer.

PAID TIER 1

Proactive Protection

$5.99 per site/month

- ✓ Database scanning and cleanup
- ✓ Proactive application shielding
- ✓ Injection remediation
- ✓ Security seal
- ✓ Detailed reports

For businesses and agencies that need application-layer protection, database cleanup and detailed incident reporting.

PAID TIER 2

Managed Recovery

$14.99 per site/month

- ✓ Everything in Proactive Protection
- ✓ Expert cleanup
- ✓ Priority response
- ✓ Documented recovery scope
- ✓ Incident escalation

For sites where downtime, customer data or recovery time has a material business impact.

Example revenue scenarios



Figure 8. Illustrative ARR sensitivity for 100,000 eligible accounts. These figures are examples, not forecasts or market benchmarks.

Even a relatively modest attach rate can create meaningful recurring revenue, but the headline number is only the starting point. Hosting teams should model revenue together with delivery cost, support and remediation cost, refunds, and the operational savings created by fewer infections and suspensions.

Scenario	Eligible accounts	Overall attach rate	Tier 1 customers (80%)	Tier 2 customers (20%)	Tier 1 MRR	Tier 2 MRR	Total MRR	Total ARR
Conservative	100,000	**5%**	4,000	1,000	$23,960	$14,990	**$38,950**	**$467,400**
Expected	100,000	**10%**	8,000	2,000	$47,920	$29,980	**$77,900**	**$934,800**
High-performing	100,000	**15%**	12,000	3,000	$71,880	$44,970	**$116,850**	**$1,402,200**

These scenarios assume that 80% of paid customers select the $5.99 Proactive Protection tier and 20% select the $14.99 Managed Recovery tier. At 100,000 eligible accounts, a 5% overall attach rate generates approximately **$467,400 ARR**, a 10% attach rate generates **$934,800 ARR**, and a 15% attach rate generates approximately **$1.4 million ARR** before delivery and support costs.

Example lifecycle

1. At checkout, the customer sees the included baseline and an optional Proactive Protection upgrade.
2. During onboarding, the panel confirms that baseline protection is active and offers a 14-day upgrade trial for eligible business sites.
3. The dashboard continuously shows coverage and detected events.
4. If a material issue is detected, the customer sees what was found, what the baseline already remediated, and whether a premium feature would reduce recurrence or provide deeper recovery.
5. At renewal, the customer receives an outcome summary: threats blocked, incidents remediated, response activity and current tier.

> **WHY THIS WORKS**
>
> The customer receives basic protection without making an emergency purchase after an incident. Premium tiers sell stronger prevention, deeper cleanup and faster recovery, outcomes that are easier to understand and pay for.

SECTION 6

Launch, measure and optimize

Launch the baseline and premium tiers as a measured pilot. Track both sides of the model: security outcomes across the fleet, and revenue from customers who need stronger protection.

Once the baseline and premium tiers are defined, launch them as a measured pilot. Track both sides of the model: security outcomes across the fleet and revenue from customers who need stronger protection, deeper cleanup, faster recovery or expert support.

Measure security and revenue together

Metric family	What to track
Commercial	Attach rate; conversion rate by placement; security ARPU; MRR/ARR; gross contribution; trial-to-paid rate; renewal rate; refund and cancellation rate.
Security	Infected accounts per 1,000 active accounts; median time to detection; median time to remediation; repeat infection rate; suspended accounts; abuse incidents.
Customer	Customer understanding of included versus paid coverage; complaints per 1,000 eligible accounts; security-related support contacts per 1,000 accounts; NPS/ CSAT; recovery satisfaction.
Operational	Cleanup minutes per incident; escalation rate; manual remediation cost per incident; provisioning failure rate; false-positive rate.
Portfolio	Results by segment, plan, geography, acquisition channel, site age and prior incident history.

Plan the pilot before launch

Start with one product line, geography or new-customer cohort. Use a control group where possible, and test both commercial and security outcomes.

- Define the hypothesis and the minimum success threshold before launch.
- Choose one or two variables: price, tier structure, placement, trial, message or billing unit.
- Run long enough to observe activation, first invoice, early refunds and at least one renewal point where practical.
- Even a modest attach rate can create meaningful recurring revenue. But the headline number is only the start. Model delivery, support, remediation, refunds and the operational savings from fewer infections and suspensions.
- Document the rollout decision: scale, revise, retest or stop.

Set the decision rules

Attach rate alone is not enough. An upsell can convert well and still be the wrong product decision if it increases complaints, adds support work, leaves the fleet exposed or weakens the base hosting offer.

- **Scale** when contribution and security outcomes improve without breaching customer or operational guardrails.
- **Revise** when conversion is promising but customers do not understand the tier boundary or support load is too high.
- **Stop or redesign** when revenue depends on coercive incident messaging, hidden terms, or withholding controls required for a safe baseline.

What a strong model looks like

Security monetization is more than a checkout checkbox. A strong model protects every customer at a credible baseline, sells premium tiers around distinct outcomes and connects the offer to the full lifecycle from purchase to incident and renewal.

The process is straightforward: map the current setup, define the baseline, segment customers, build the premium tiers, choose the right upsell moments, model the economics, prepare operations, run a pilot and optimize. Done well, the result is safer customer sites, lower operational cost and sustainable security revenue.

SECTION 7 · ABOUT MONARX

A credible baseline for every account, with premium protection on top

Monarx provides server-side malware detection, prevention and automatic remediation for hosting providers. The platform is built to support the model described in this guide: a credible baseline for every account, with premium protection for proactive defense, deeper remediation and expert recovery.

The framework, worksheets and scorecard can be used with any security stack. The goal is to help providers build a model that protects customers, makes commercial sense and can be delivered operationally.

Where to start

- **Model your numbers.** Complete the worksheet in Appendix C with Finance, Support and Security Operations so new revenue and avoided cost are assessed together.
- **Size the opportunity.** Apply the ARR formula in Section 5 to your own eligible account base, attach-rate assumptions and price points.
- **Pressure-test the baseline.** Ask what a customer who declines every upgrade receives today, and whether support can stand behind that promise.
- **Talk it through with us.** Monarx can help review the packaging, pricing and launch plan with your team.

Talk to Monarx

monarx

Monarx, monarx.com. This guide is provided for planning purposes and does not constitute legal, tax or accounting advice. Provider offers described in this guide were accurate as presented on the dates cited and may since have changed.

APPENDIX A

Research methodology

This analysis looks at how hosting providers include, package and monetize security on public pricing, product and support pages.

Scope of the analysis

The analysis covers 65 hosting providers. For each provider, we covered protection, separately sold security products, published pricing and any third-party vendor named on the page.

How the findings were interpreted

Security products are not directly comparable. Some are priced per site, while others cover an account, plan, server or portfolio. The analysis therefore compares packaging and customer outcomes first, using price only as a directional benchmark. Public pages do not always answer every question, and the analysis did not test detection quality, remediation success or false-positive rates.

Using the findings

Use the findings to compare market ranges, feature boundaries and upgrade logic. Validate final pricing against your own customer segments, cost structure, delivery model and pilot results.

APPENDIX B

Market examples and official sources

These official pages support the company examples in the guide. They were accessed in August and September 2026, and offers may change over time.

hosting.com · Core hosting plans
https://hosting.com/hosting/

hosting.com · Managed WordPress security
https://new.hosting.com/hosting/platforms/wordpress-hosting/security/

GoDaddy · Website Security plans
https://www.godaddy.com/en/web-security/website-security

Convesio · Managed WordPress pricing
https://convesio.com/monthly-pricing

Rapyd Cloud · Plan specifications
https://support.rapyd.cloud/en/articles/11179623-site-limits-for-multi-site-plans

Bluehost · Website Security
https://www.bluehost.com/website-security

DreamHost · DreamShield
https://www.dreamhost.com/products/dreamshield/

InMotion Hosting · Monarx Security
https://www.inmotionhosting.com/support/security/monarx-security/

APPENDIX C

Business-case worksheet

Use this worksheet to turn headline ARR into a realistic contribution model. Complete it with Finance, Support, Security Operations and the delivery team so direct cost and avoided cost are measured together.

Input	Definition	Value
Eligible accounts	Unique accounts/sites technically eligible for the offer and shown it during the measurement period	
Attach rate	Paid activations divided by eligible accounts/ sites shown the offer	
Monthly price	Average net monthly revenue per paid activation after discounts, tax and channel share where applicable	
Gross MRR	Eligible accounts × attach rate × monthly price	
Vendor / technology cost	Technology cost per account, site or server, or the applicable revenue share	
Remediation cost	Average automatic and human cleanup cost attributable to the product	
Support cost	Security-related contacts multiplied by average handling cost	
Payment and refund cost	Payment processing, chargebacks and refunds attributable to the product	
Gross contribution	Gross MRR minus direct delivery costs	
Avoided support cost	Reduction in security-related ticket volume multiplied by average handling cost, compared with the baseline or control	

Input	Definition	Value
Avoided revenue loss	Verified retained revenue from lower churn, suspensions or account closures, compared with the baseline or control	
Net monthly impact	Gross contribution plus verified avoided support cost and avoided revenue loss	

Scenario planning

Scenario	Eligible accounts	Attach rate	Price	Gross MRR	Gross contribution
Conservative					
Expected					
High-performing					

APPENDIX D

Pilot scorecard

Before launch, define the pilot hypothesis, cohort, guardrails and decision rule. This scorecard keeps the team from judging the result on conversion alone.

Field	Pilot definition
Hypothesis	State the expected change, target threshold and guardrail. Example: dashboard prompts increase attach rate by at least X% without raising complaints above Y per 1,000 eligible accounts.
Cohort	Product line, geography, acquisition cohort, segment, eligibility rules and sample size.
Control	Existing experience or alternate packaging, with the same eligibility and measurement window.
Offer	Tier, price, billing term, trial, included capabilities and eligibility rules.
Placement	Checkout, onboarding, dashboard, alert, support or renewal.
Primary metric	One preselected metric with a documented formula and success threshold.
Security metric	One preselected security metric with a documented formula and success threshold.
Guardrails	Maximum acceptable complaint rate, support load, refunds, churn and false-positive rate.
Duration	Minimum observation period, first invoice point and renewal point where practical.
Decision rule	Numeric thresholds for scale, revise, retest or stop.
Owner	Named product owner and accountable teams for security, support, billing and analytics.
Result	Observed data, variance from target, decision and next action.

APPENDIX E

Launch checklist

Use this checklist for the cross-functional launch review. The tier is ready only when the customer promise, technical entitlement, billing, remediation, support, analytics and public claims all match.

Area	Ready when a named owner and evidence are recorded
Strategy	Baseline capability list approved; paid tiers have distinct outcomes; target segments and brand model documented.
Product	Tier names, entitlements, eligibility, trial, upgrade and downgrade rules are documented and approved.
Engineering	Provisioning, deprovisioning, telemetry, dashboard, alerts, event tracking and failure recovery pass documented QA tests.
Billing	Test transactions pass for monthly and annual billing, proration, taxes, refunds, renewals and multi-site plans.
Security operations	Remediation ownership, escalation path, false-positive process, response scope and response times are documented.
Support	Agents can view coverage, use approved scripts, complete training and follow a tested escalation path.
Marketing	Pricing, checkout, onboarding and lifecycle copy state included coverage, paid outcomes and eligibility clearly.
Legal	Terms, disclaimers, guarantees, privacy language and service descriptions are reviewed and approved.
Analytics	Dashboard reports defined commercial, security, customer and operational metrics using documented formulas.
Pilot governance	Hypothesis, control, thresholds, guardrails, duration, owner and decision rule are approved before launch.
Existing customers	Migration, grandfathering, customer communication and credit rules are documented and tested.