



Enterprise plan: everything included

Lumière PayCheck lets your AI agents pay for services on their own, under your company’s rules. Before any payment happens, we check the seller against continuous trust data and check the payment against your limits, roles, and policies, then answer **allow**, **deny**, or **review**, with a signed receipt and a tamper-evident record. This guide describes everything the Enterprise plan provides.

INCLUDED Every feature All trust data, authorization, and governance features, with Enterprise limits and service.	CUSTOM Terms set for you Agent counts, retention, rate limits, caps, and networks configured for your company.	SERVICE Onboarding to billing Invite-based onboarding, flexible pricing, trials, renewal reminders, and transparent support.
---	---	---

Contents

1	Enterprise at a glance
2	Trust data about sellers
3	Payment authorization
4	Governance: roles, controls, alerts, audit
5	Agent credentials: keys, key-less sign-in, IP allowlists, test keys
6	Custom terms you can have
7	Onboarding, billing, and support
8	Security, privacy, and data retention
9	Plans compared, getting started, and links

1. Enterprise at a glance

Area	Included with Enterprise
Trust data	Monitoring of 17,000+ x402 endpoints every 30 minutes, A–F grades, paid delivery verification, wallet and price change detection, on-chain real usage, community reports, failure logs.
Authorization	Scoped agent keys (up to 1,000, custom), allow/deny/review decisions, Ed25519-signed receipts, human review queue, replayable decisions, CSV export.
Governance	Viewer, Approver, Admin, and Owner roles; freeze switch; company blocklist; company-wide caps; allowed networks; teams and owners; spending reports.
Alerts and integrations	Budget alerts (50/80/100%), spike alerts, signed webhooks, streaming every decision to your SIEM, review notifications.
Audit	Activity log of every change (including ours), hash-chained tamper-evident decisions with one-click verification, 2-year history (custom).
Agent credentials	Agent keys, key-less sign-in with GitHub Actions, Google Cloud, Azure, or Kubernetes identity, IP allowlists, test keys.
Service	Invite-based onboarding, additional administrators, flat or usage-based pricing invoiced via Stripe, trials, renewal reminders, read-only support access, public status page.
Free for everyone	Endpoint grades, the public API (60 requests/minute), and the MCP server for AI assistants.

How a payment decision works

1	The agent asks Before paying, it sends the endpoint, amount, payout wallet, and network, using its own scoped credential.
2	We check the seller Is the endpoint healthy, is the price what we observed, is the payout wallet the one we monitor?
3	We check your rules The agent's limits and allowed sellers, your blocklist, company caps, allowed networks, IP allowlist, freeze switch.
4	We answer and record Allow (with a signed receipt), deny (with every reason), or review (a person decides). The decision is stored and chained.

2. Trust data about sellers

Decisions are only as good as the data behind them. Ours comes from watching every seller continuously, paying them ourselves, and reading real payments on-chain.

Feature	Details
Continuous monitoring	Every endpoint listed in the x402 Bazaar is checked every 30 minutes: uptime, response time, price, payout wallet, and network.
Grades A to F	A 0–100 score over the last 7 days: uptime (40 points), response time (15), stability of price and payout wallet (25), and paid delivery results (20).
Paid delivery verification	We pay endpoints ourselves and check that responses match what the seller advertises. A failure only counts after a second paid check confirms it; problems on our side never count against a seller.
Wallet and price changes	Detects payout-wallet changes and price increases. A wallet change caps the grade (at 40) for the 7-day scoring window.
Real usage from the blockchain	Actual x402 payments (USDC on Base and Solana) into each seller's payout wallet over 30 days: volume, distinct buyers, typical and largest payment, trend, and how concentrated the buyers are.
Community outcome reports	Paying customers can report whether a call delivered. Reports require a valid receipt and only trigger our own re-tests; they never change a grade by themselves.
Public failure log and disputes	Recent failed checks with reasons for any endpoint; sellers can dispute a grade publicly, which triggers a paid re-test.
Free API and MCP server	Look up grades, check payments, and see top endpoints from code or AI assistants (MCP tools: <code>check_endpoint</code> , <code>check_payment</code> , <code>top_endpoints</code> , <code>catalog_stats</code> , <code>get_full_report</code> , <code>report_outcome</code>).

3. Payment authorization

Feature	Details
Scoped agent keys	One key per agent with allowed sellers, a per-payment cap, daily and monthly limits, and an expiry. Replace or revoke instantly. Keys are shown once and stored only as hashes.
Allow / deny / review	Every decision lists its reasons. Denials include every rule that failed, so teams can act on them.
Signed receipts	Each “allow” includes an Ed25519-signed receipt for that exact URL, amount, and payout wallet, valid for 5 minutes. Your wallet can require it, so nothing unapproved can be paid. The public key is published.
Human review	Payments above an agent's threshold, or to a wallet it hasn't paid before, wait for an approver. Reviews expire after 24 hours; notifications can go to a webhook.
Replayable decisions	Every decision stores its full inputs and can be re-evaluated to show exactly why it came out as it did.
CSV export	Export the audit trail, and spending by agent, for finance and compliance.

4. Governance

Roles and permissions

Can...	Viewer	Approver	Admin	Owner
See the workspace, agents, decisions, reports, activity	Yes	Yes	Yes	Yes
Verify the audit trail, replay decisions, export CSV	Yes	Yes	Yes	Yes
Approve or deny payments waiting for review	–	Yes	Yes	Yes
Create, change, replace, and revoke agent keys	–	–	Yes	Yes
Freeze switch, blocklist, alerts, integrations	–	–	Yes	Yes
Invite people, change roles, remove people	–	–	–	Yes
Manage billing	–	–	–	Yes

Each person has their own key and role, invited by a one-time link and removable at any time. Webhook secrets are shown to admins and the owner only.

Company controls

Freeze switch	Pauses every agent in the workspace instantly; payments are denied, with the reason recorded, until it's turned off.
Company blocklist	Sellers (hostnames) and payout wallets that are always denied, whatever each agent's settings say.
Company-wide caps	Daily and monthly spending limits across all agents, a maximum single payment, and allowed payment networks.
Teams and owners	Assign each agent a responsible person and a team or cost center; see spending by team with CSV download.

Alerts and integrations

Budget alerts	At 50%, 80%, and 100% of company caps and agents' daily and monthly limits (thresholds adjustable), once per threshold per period.
Spike alerts	When an agent spends at least 10× its 7-day daily average in a day (multiplier and minimum adjustable).
Delivery	By email and by webhook, signed with your workspace secret (HMAC-SHA256), so you can verify they came from us.
SIEM streaming	Every decision sent to your security tools (Splunk, Datadog, and others) as a signed webhook, including its chain hash.

Audit

Activity log	Who changed what and when: the owner, a named administrator, or Lumière PayCheck (including any support view).
Tamper-evident decisions	Each decision's SHA-256 hash covers the previous one, so any edit or deletion is detectable. One click verifies the chain.
History	2 years of decisions by default on Enterprise, adjustable.

5. Agent credentials

Agent keys	A separate key per agent, shown once, stored as a SHA-256 hash, with its own limits and expiry.
Key-less sign-in	Agents prove who they are with a short-lived token from the platform they run on, with nothing long-lived to leak or rotate. We verify the signature against the platform's published keys, the expiry, the audience, and the exact workload you linked.
Supported platforms	GitHub Actions (repository, branch, or environment), Google Cloud (service accounts), Microsoft Azure (managed identities), and Kubernetes or other OIDC issuers (service accounts, including EKS).
Safeguards	Only asymmetric signatures (RS, PS, ES) are accepted; unsigned and shared-secret tokens are rejected; tokens may live at most 24 hours; key rotation is picked up automatically; raw tokens are never stored.
IP allowlists	An agent key only works from your addresses or ranges (IPv4 and IPv6). We check each request's address but store only whether it matched.
Test keys	For integration: decisions are marked test and never count toward spending, caps, alerts, reports, or billing; receipts carry "test", so production wallets can refuse them.

6. Custom terms you can have

Enterprise settings are configured for your company and take effect on your next request, with no waiting for a release. Your agreed terms are shown on your account page.

Setting	Enterprise default	Can be set to
Agent keys	1,000	1 to 100,000
Audit history	730 days (2 years)	1 to 3,650 days
Authorizations per minute, per agent	3,000	1 to 100,000
Human review	On	On or off
CSV export	On	On or off
Company-wide daily cap	None	Any amount
Company-wide monthly cap	None	Any amount
Maximum single payment	None	Any amount
Allowed networks	Any	e.g. Base only, or Base and Solana
Term	As agreed	Any end date, extended as you renew

7. Onboarding, billing, and support

Onboarding

Access by invite	You receive a one-time access link (single use, expires after 7 days) and create your own owner key. We never see it.
Your team	Invite colleagues with the role they need; each gets their own one-time link and key.
Trials	A time-limited trial workspace to evaluate before you commit, converted to your plan when you're ready.

Billing options

Flat fee	Annual or monthly, invoiced with payment terms.
Usage-based	A base fee, a number of authorizations included each month, and a price per authorization above that. Usage is counted as it happens (test keys never count) and shown as a running estimate on your account page.
Invoices	Sent through Stripe at the start of each month with your payment terms; Stripe emails the invoice and collects payment, and it's marked paid automatically. Each month is invoiced at most once.
Renewals	Reminders before your term ends, to us and optionally to you.

Support and transparency

Support access	When we look at your workspace to help, it's through a read-only view that expires after 15 minutes, can't change anything or see secrets, and appears in your activity log.
Changes we make	Any change we make to your workspace (for example, limits you asked for) is recorded in your activity log.
Status and incidents	Live component health, 90-day uptime, and incident updates at lumierepaycheck.org/status .
Contact	hello@lumierepaycheck.org

8. Security, privacy, and data retention

No custody	We never hold, route, or escrow funds. Agents pay sellers directly from your wallets.
Keys and secrets	192-bit random keys stored only as SHA-256 hashes; secrets kept in the hosting environment, never in code, and masked in logs.
Application	HTTPS with HSTS, strict content security policy, parameterized database queries, rate limits, signed webhooks, and SSRF protection for every outbound request.
Hosting and backups	US East (Virginia). Nightly backups encrypted with AES-256-GCM before leaving our server and stored off-site; our pages load no third-party resources.
Privacy	No IP address logs; visitor counts use a code that changes daily. We never sell data, show ads, or use tracking cookies.
Current limitations	Not yet SOC 2 certified and not yet third-party penetration tested; single-region, single-instance hosting; single sign-on not yet available. We're glad to complete your security questionnaire.

Data retention

Data	Kept
Payment decisions (your audit trail)	Your plan's audit period: 2 years by default on Enterprise, adjustable
Monitoring checks about sellers	Full detail 2 days; hourly totals 8 days; daily totals 90 days; failed checks 8 days
Paid delivery results and events	90 days
On-chain settlement records	31 days individually; daily totals 1 year
Outcome reports / recovery requests	90 days / 30 days
Workspace, administrators, invoice records	Until you ask us to delete them (invoices longer if law requires)
Encrypted backups	Latest 7 daily and 4 weekly copies

9. Plans compared, getting started, and links

	Free	Builder	Business	Enterprise
Price	\$0	\$9 / month	\$49 / month	Custom
Agent keys	–	3	25	Up to 1,000+
Audit history	–	30 days	1 year	2 years+
Authorizations/min per agent	–	120	600	3,000+
Human review, CSV export	–	–	Yes	Yes
Roles, freeze, blocklist, alerts, audit	–	Yes	Yes	Yes
Key-less sign-in, IP allowlists, test keys	–	Yes	Yes	Yes
Company caps, networks, custom limits	–	–	–	Yes
Invoicing, usage pricing, trials	–	–	–	Yes
Billing	–	Card or USDC	Card or USDC	Invoice

Getting started

- 1

Talk to us. Tell us about your agents at lumierepaycheck.org/enterprise; we agree terms or start a trial.
- 2

Open your access link. Create your owner key and invite your team with the right roles.
- 3

Create agents or link identities. One scoped key per agent, or key-less sign-in with your cloud.
- 4

Integrate and go live. Call `/v1/authorize` before each payment; set alerts, blocklist, and SIEM streaming.

Links

Documentation	lumierepaycheck.org/docs
All features	lumierepaycheck.org/docs/features
Administrator guide	lumierepaycheck.org/docs/admin-guide
Integration guide	lumierepaycheck.org/docs/integration
FAQ	lumierepaycheck.org/docs/faq
Security	lumierepaycheck.org/security
Privacy	lumierepaycheck.org/privacy
Status	lumierepaycheck.org/status
Contact	lumierepaycheck.org/enterprise

Lumière PayCheck is operated by Lumière LLC, Connecticut, USA. Scores are automated assessments, not guarantees or financial advice. Features and terms described here reflect the service as of September 2026.