# CrownWall.net — Complete Website Content

## Final handover document for web designer

---

## DESIGNER BRIEFING NOTES

**CMS:** WordPress **Homepage direction:** B — clean SaaS (Cloudflare/Kemp feel). White background, deep navy + teal accent, split hero layout. **Logo:** Provided separately — CrownWall navy crown/wall mark **Client logos:** 50 to follow — build carousel placeholder now, logos drop in later **Pricing figures:** TBD — use placeholder layout, numbers to be confirmed separately **Phone number:** TBD — leave placeholder in Contact page, Emergency page, and footer **Social:** LinkedIn only — link TBD **No company name, no parent brand** anywhere on the site — CrownWall stands alone **Visuals:** Each page flags `[Visual: ...]` recommendations — designer's discretion on execution **Icons:** Use Tabler outline icon set throughout

**Notation used in this document:**

- `[Visual: ...]` = recommended image, diagram, or illustration
- `[BUTTON: ...]` = CTA button label
- `[Designer note: ...]` = layout or component guidance
- `*` after a form field = required field

---

## SITEMAP (final, locked)

```
MAIN NAVIGATION
├── Products ▾
|   ├── Web Application Firewall          /products/waf
|   ├── Bot Management                    /products/bot-management
|   ├── DDoS Protection                   /products/ddos-protection
|   ├── Load Balancing                    /products/load-balancing
|   ├── API Security                      /products/api-security
|   └── Observability & Compliance        /products/observability
|
├── Solutions ▾
|   ├── Financial Services & Fintech      /solutions/financial-services
|   ├── Healthcare & Healthtech           /solutions/healthcare
|   ├── E-commerce & Retail               /solutions/ecommerce
|   ├── SaaS & Technology                 /solutions/saas
|   ├── Gaming & Media                    /solutions/gaming-media
|   └── Public Sector                     /solutions/public-sector
|
```

```
├── How It Works ▾
│   ├── The Platform                    /how-it-works
│   ├── Architecture & Network          /how-it-works/architecture
│   ├── Data Residency                  /how-it-works/data-residency
│   └── Integrations                    /how-it-works/integrations
│
├── Pricing                             /pricing
│
├── Resources ▾
│   ├── Knowledge Hub                   /resources/knowledge-hub
│   ├── Whitepapers & Reports           /resources/whitepapers
│   ├── Success Stories                 /resources/success-stories
│   └── Press & Media                   /resources/press
│
├── Partners                            /partners
│
└── Company ▾
    ├── About                           /company/about
    ├── Trust Centre                    /company/trust-centre
    └── Contact                         /company/contact

UTILITY NAVIGATION (top right)
  [Under Attack? — red pill]   /emergency
  [Sign In]                    portal.crownwall.net
  [Start Free Trial — teal button]

FOOTER COLUMNS
  Col 1: Brand + LinkedIn + copyright
  Col 2: Products (all 6)
  Col 3: Solutions (all 6)
  Col 4: Resources (Knowledge Hub, Whitepapers, Success Stories, Press)
  Col 5: Company (About, Trust Centre, Partners, Contact)

FOOTER BOTTOM BAR
  Privacy Policy · Terms of Service · Cookie Policy · Under Attack?
```

---

---

# PAGE 1 — HOMEPAGE

**Page title:** CrownWall — Application Delivery & Web Security **URL slug:** /

---

## NAVIGATION BAR

**Logo:** CrownWall [logo mark] **Nav links:** Products · Solutions · How It Works · Pricing · Resources
**Right utility:** [Under Attack? — red pill] · [Sign In] · [Start Free Trial — teal filled button]

---

## HERO SECTION

`[Designer note: split layout — text and CTAs on the left, live threat-activity panel on the right. Full-width section, white background with subtle geometric pattern or gradient hint in the upper right behind the panel.]`

**LEFT COLUMN:**

**Eyebrow badge (teal pill, small caps):** Application Delivery & Web Security

**H1:** The wall your web applications stand behind.

**Subhead:** WAF, bot management, DDoS protection, load balancing, and API security — in one platform, under one predictable price. Built for businesses that have outgrown free tools.

**[BUTTON primary — teal: Start free trial] [BUTTON secondary — outline: Request a demo →]**

**Trust line (small muted text below buttons):** 14-day full-feature trial · No credit card required · Deploy in under 30 minutes

---

**RIGHT COLUMN — Live threat activity panel:** `[Designer note: dark navy card, teal and gold accents. Animated counters or subtle live-updating numbers to make it feel active. This is a mock dashboard panel — not a real data feed at launch, but should look like one.]`

**Panel header label (small monospace, muted):** Live threat activity

**Three metric rows (each: colour dot · label · progress bar · count badge):**

- [Teal dot] WAF rules — [bar 75%] — 2,847 requests blocked
- [Gold dot] Bot management — [bar 55%] — 1,203 bots stopped
- [Blue dot] DDoS mitigation — [bar 30%] — 412 attacks mitigated

**Below rows (small muted text):** All clean traffic: 99.97% pass rate · Avg latency 12ms

---

## STATS STRIP

`[Designer note: full-width band, light grey background, 3 equal columns]`

**73%** of organisations globally experienced a successful web application attack last year *Verizon DBIR*

**311bn** web application attacks recorded worldwide in a single year *Akamai State of the Internet*

**$4.9m** average global cost of a data breach involving web applications *IBM Cost of a Breach*

---

## CLIENT LOGOS

`[Designer note: full-width marquee/carousel, continuous scroll, 2 rows on mobile. 50 logos to be provided by client. Display in greyscale, reveal colour on hover. Label above:]`

**Label (small, muted):** Trusted by organisations across financial services, healthcare, SaaS, e-commerce, gaming, and public sector

---

## SECTION — One platform

**Eyebrow (small caps, teal):** THE PLATFORM

**H2:** Every layer of web defence, from one engine.

**Body:** Stitching together a WAF from one vendor, bot protection from another, and a load balancer from a third creates gaps — and gaps are where attacks succeed. CrownWall runs delivery and security in a single pipeline. Every layer sees the full request context. One dashboard. One bill. No gaps.

`[Visual: horizontal request pipeline — Client → TLS → Bot Check → WAF → Rate Limit → Load Balance → Origin. Clean left-to-right flow, teal accent on each step node.]`

**[BUTTON: See how it works →]** (links to /how-it-works)

---

## SECTION — Six capabilities

**Eyebrow:** WHAT'S INCLUDED

**H2:** Six capabilities. One subscription.

`[Designer note: 3×2 card grid. Each card: Tabler outline icon, title, one-line description, "Learn more →" link. Hover: subtle lift + border highlight.]`

| Title | Description | Link |
|---|---|---|
| Web Application Firewall | OWASP Top 10, custom rules, and shadow-mode testing for precise API protection. | /products/waf |
| Bot Management | Stop credential stuffing, scrapers, and AI bots — without touching the traffic you want. | /products/bot-management |
| DDoS Protection | Absorb volumetric and application-layer attacks at the edge, before they reach your origin. | /products/ddos-protection |
| Load Balancing | Health-aware routing across all your backends — included as standard, not an add-on. | /products/load-balancing |
| API Security | Per-endpoint rate limiting, schema validation, and abuse detection for modern APIs. | /products/api-security |
| Observability & Compliance | Real-time analytics and one-click audit reports for PCI-DSS, NIS2, GDPR, and more. | /products/observability |

---

## SECTION — Why CrownWall

**Eyebrow:** WHY CROWNWALL

**H2:** Built around what actually matters.

`[Designer note: 3×2 grid of value prop cards. Each: small Tabler icon, short bold title, 2-sentence body.]`

**Everything included** WAF, bot, DDoS, load balancing, and compliance reporting in every plan. No per-feature billing, no surprise charges when an attack hits.

**Honest, flat pricing** One predictable monthly number. You pay for legitimate traffic — attack volume doesn't inflate your invoice.

**Compliance built in** One-click audit reports formatted for PCI-DSS, NIS2, GDPR, SOC 2, and ISO 27001. Ready when the auditor asks.

**Data residency you choose** Your traffic processed in the region your business or regulator requires. A contractual commitment, not a setting.

**Real human support** Email, chat, and phone with response SLAs at every plan tier. No chatbot triage. Engineers respond.

**Deploy in minutes** Point DNS, confirm your origin, go live. No appliances, no professional services, no weeks of onboarding.

---

## SECTION — Solutions by sector

**Eyebrow:** WHO WE PROTECT

**H2:** Configured for the sectors with the most to lose.

`[Designer note: 6-card horizontal row, each card links to its solution page. Hover: reveals 2-3 relevant compliance framework names.]`

- **Financial Services** — Transaction protection, credential stuffing defence, PCI-DSS alignment → /solutions/financial-services
- **Healthcare** — Patient data protection, structured audit trails, data residency → /solutions/healthcare
- **E-commerce** — Bot mitigation, traffic spike resilience, PCI scope support → /solutions/ecommerce
- **SaaS & Technology** — API protection, multi-tenant logging, SOC 2 evidence → /solutions/saas
- **Gaming & Media** — Low-latency DDoS mitigation, content protection, bot management → /solutions/gaming-media
- **Public Sector** — Data sovereignty, NIS2 alignment, Cyber Essentials Plus → /solutions/public-sector

**[BUTTON: Explore all solutions →]** (links to /solutions)

---

## SECTION — Trust & certifications

**Eyebrow:** TRUST & COMPLIANCE

**H2:** Certified, verified, and auditable.

`[Designer note: certification logo strip — ISO 27001, SOC 2 Type II, PCI-DSS, Cyber Essentials Plus, NIS2 aligned. Each logo links to Trust Centre.]`

**[BUTTON: View Trust Centre →]** (links to /company/trust-centre)

---

## SECTION — Success story spotlight

**Eyebrow:** SUCCESS STORIES

**H2:** Relied on when it matters.

`[Designer note: 2-column layout — pull quote left, 3 outcome metrics right. Client logo above quote. Rotates between 2-3 featured stories. Links to /resources/success-stories. Content to be populated once client provides stories.]`

**[BUTTON: Read success stories →]** (links to /resources/success-stories)

---

### FINAL CTA BAND (dark navy, full width)

**H2:** Defend what you've built.

**Subhead:** Start a free trial today or talk to our team about your environment.

**[BUTTON primary — teal: Start free trial] [BUTTON secondary — outline white: Request a demo]**

---

### FOOTER

**Column 1 — Brand** [CrownWall logo] Application Delivery & Web Security [LinkedIn icon → CrownWall LinkedIn page] © 2026 CrownWall. All rights reserved.

**Column 2 — Products** Web Application Firewall · Bot Management · DDoS Protection · Load Balancing · API Security · Observability & Compliance

**Column 3 — Solutions** Financial Services · Healthcare · E-commerce · SaaS & Technology · Gaming & Media · Public Sector

**Column 4 — Resources** Knowledge Hub · Whitepapers & Reports · Success Stories · Press & Media

**Column 5 — Company** About · Trust Centre · Partners · Contact

**Bottom bar:** Privacy Policy · Terms of Service · Cookie Policy · [Under Attack? — red link → /emergency]

---

---

## PAGE 2 — WEB APPLICATION FIREWALL

**Page title:** Web Application Firewall — CrownWall **URL slug:** /products/waf

### Hero

**Eyebrow:** PRODUCTS / WEB APPLICATION FIREWALL

**H1:** Block what shouldn't reach your applications.

**Subhead:** A complete WAF with OWASP Top 10 coverage, custom rule groups, and traffic labelling — built to protect modern API-driven applications, not just static websites.

**[BUTTON primary: Start free trial] [BUTTON secondary: Request a demo]**

`[Visual: stream of requests entering the platform — malicious ones stopped, clean traffic passing through. Abstract, geometric.]`

---

## Section

**H2:** Inspection at the edge, before the damage.

**Body:** CrownWall's web application firewall sits in front of your application and inspects every HTTP request before it reaches your origin. It blocks the known patterns of attack — SQL injection, cross-site scripting, file inclusion, sensitive-file probing — while letting legitimate traffic through untouched.

Unlike rule-based firewalls that only match fixed signatures, CrownWall combines managed rule groups, kept current by our security team, with custom rules you can build, test, and deploy from the dashboard without restarting anything.

---

## Section

**H2:** Protected against the attacks that matter, from day one.

**Body intro:** Every CrownWall account starts with managed rulesets covering the most common application-layer attack vectors:

- **OWASP Top 10** — the industry-standard list of critical web application security risks, refreshed continuously
- **SQL injection** — classic and blind injection patterns, including parameterised-query bypass attempts
- **Cross-site scripting (XSS)** — reflected and stored variants
- **Local & remote file inclusion (LFI/RFI)** — attempts to access or execute files outside your application's scope
- **Sensitive file attacks** — probes for `.env` files, backups, version-control directories, and config leaks
- **Path traversal** — attempts to escape your application's directory structure

---

## Section

**H2:** Protect what's specific to your application.

**Body:** Managed rules cover the common ground. Custom rules let you protect what's unique to you — your API endpoints, your authentication flow, your business logic.

Build rules visually using a clear condition-and-action structure. Match on request method, path, headers, body content, source IP, geography, or any combination. Trigger actions like block, challenge, log-only, rate-limit, or label-and-forward for downstream analysis.

**Callout box: Shadow-mode testing** — Test new rules without enforcement. CrownWall tags matching traffic so you can review exactly what a rule would have done, then turn enforcement on with confidence. No more blocking real customers by accident.

---

### Section

**H2:** Designed for API workloads, not retrofitted for them.

**Body:** Most firewalls were built for traditional websites and had API support bolted on later. CrownWall treats API protection as a first-class concern: per-endpoint rule scoping, JSON body inspection, query-parameter validation, and rate limiting that understands the difference between a public marketing page and an authenticated API call.

---

**Feature tags strip:** OWASP Top 10 · SQLi protection · XSS protection · LFI/RFI blocking · Custom rule builder · Shadow-mode testing · Per-endpoint scoping · JSON body inspection · Geo filtering · Managed rule updates

---

### CTA band

**H2:** Put a wall in front of your applications. **[BUTTON: Start free trial] [BUTTON: Request a demo]**

---

---

## PAGE 3 — BOT MANAGEMENT

**Page title:** Bot Management — CrownWall **URL slug:** /products/bot-management

### Hero

**Eyebrow:** PRODUCTS / BOT MANAGEMENT

**H1:** Stop the bots that are actually targeting you.

**Subhead:** Multi-layer protection that identifies and blocks malicious automation — credential stuffing, scrapers, vulnerability scanners, DDoS tools — without breaking the legitimate bots you depend on.

**[BUTTON primary: Start free trial] [BUTTON secondary: Request a demo]**

`[Visual: traffic being sorted — humans and good bots passing through cleanly, malicious bots being filtered.]`

---

## Section

**H2:** Bot traffic is now the majority. Most of it isn't yours.

**Body:** A few years ago, bot protection meant blocking obvious crawlers. Today, automated traffic makes up more than half of all web requests — and the harmful share is increasingly sophisticated, using residential proxies, rotating identities, and behavioural mimicry to evade simple detection.

CrownWall identifies and acts on automated clients across multiple categories — without breaking the search engines, monitors, and integrations you actually want.

---

## Section

**H2:** Know the difference between a threat and a customer.

`[Visual: bot category cards or icon grid]`

- **Credential stuffing** — automated login attempts using leaked credentials. The most common attack against authenticated APIs.
- **Vulnerability scanners** — probes for known CVEs, exposed admin panels, default credentials, and misconfigurations.
- **Scrapers & crawlers** — content theft, price scraping, inventory monitoring, data harvesting.
- **AI & LLM scrapers** — the fast-growing category harvesting content to train models, often ignoring robots.txt.
- **DDoS tooling** — application-layer denial-of-service tools that flood specific endpoints with low-volume, hard-to-detect traffic.
- **Verified good bots** — Googlebot, Bingbot, monitoring tools, partner APIs. Identified and allowed — never blocked by mistake.

---

## Section

**H2:** Not every bot needs the same answer.

**Body intro:** Apply different responses per category, tuned to your tolerance:

- **Block** — for clearly malicious categories like credential stuffing
- **Challenge** — a JavaScript or browser-fingerprint challenge real browsers pass invisibly
- **CAPTCHA** — interactive challenge for borderline cases
- **Allow** — for legitimate categories you want through
- **Log-only** — observe without acting while you refine your policy

**Callout box: Why this matters for SaaS** — if your application has paying customers logging in through authenticated API calls, credential stuffing isn't hypothetical. It's happening now, and standard firewall rules won't catch it.

---

**Feature tags:** Credential-stuffing detection · AI scraper blocking · CAPTCHA · JavaScript challenges · Verified search-engine bots · Per-category actions · Behavioural fingerprinting · IP reputation

---

### CTA band

**H2:** Take back control of your traffic. **[BUTTON: Start free trial] [BUTTON: Request a demo]**

---

---

## PAGE 4 — DDoS PROTECTION

**Page title:** DDoS Protection — CrownWall **URL slug:** /products/ddos-protection

### Hero

**Eyebrow:** PRODUCTS / DDoS PROTECTION

**H1:** Stay online through the storm.

**Subhead:** Absorb volumetric and application-layer DDoS attacks at the edge, before they ever reach your origin — with no latency penalty for your real users.

**[BUTTON primary: Start free trial] [BUTTON secondary: Request a demo]**

`[Visual: large flood of attack traffic hitting an edge filtering layer, thin clean stream continuing to origin. Abstract, not literal.]`

---

### Section

**H2:** Attacks stop at the edge. Your users never notice.

**Body:** DDoS attacks work by overwhelming your infrastructure with traffic until legitimate users can't get through. CrownWall absorbs that traffic at the network edge — far from your origin — filtering out the attack while clean requests continue uninterrupted.

Because filtering happens in-line as part of the same pipeline handling your WAF and bot protection, there's no separate appliance to deploy and no detour that adds latency for real users.

---

### Section

**H2:** Protection across every layer attackers use.

`[Visual: layered diagram — L3/L4 volumetric at bottom, L7 application-layer at top]`

- **Volumetric attacks (L3/L4)** — UDP floods, SYN floods, amplification and reflection attacks that try to saturate your bandwidth.
- **Protocol attacks** — attacks that exhaust connection-state resources on servers, firewalls, and load balancers.
- **Application-layer attacks (L7)** — low-and-slow request floods, HTTP floods, and targeted endpoint exhaustion designed to look like real traffic.

**Callout box: The hard one is L7.** Volumetric attacks are loud and relatively easy to spot. Application-layer attacks hide inside normal-looking requests — and that's where CrownWall's combined WAF, bot, and rate-limiting intelligence makes the difference. The same engine that knows your traffic patterns knows when they're being faked.

---

### Section

**H2:** An attack shouldn't cost you twice.

**Body:** With usage-metered providers, a large attack means a large bill — you pay for the malicious traffic you didn't want. CrownWall's flat pricing means an attack costs you nothing extra. You pay for legitimate traffic; the attack is our problem, not your invoice.

---

**Feature tags:** L3/L4 volumetric mitigation · Protocol attack defence · L7 application-layer protection · Edge filtering · No added latency for clean traffic · Flat pricing under attack · Automated attack alerts

---

### CTA band

**H2:** Don't wait for the attack to find out you're exposed. **[BUTTON: Start free trial] [BUTTON: Under attack now? →]** (links to /emergency)

---

---

## PAGE 5 — LOAD BALANCING

**Page title:** Load Balancing & ADC — CrownWall **URL slug:** /products/load-balancing

## Hero

**Eyebrow:** PRODUCTS / LOAD BALANCING

**H1:** Intelligent traffic distribution, included.

**Subhead:** Health-aware routing, dynamic DNS resolution, and response caching across all your backends — built into the platform, not sold as a separate add-on.

**[BUTTON primary: Start free trial] [BUTTON secondary: Request a demo]**

`[Visual: traffic distributed across multiple healthy backend servers, unhealthy server shown bypassed.]`

---

## Section

**H2:** Delivery and security, from one engine.

**Body:** CrownWall is a complete application delivery controller — the same category of infrastructure that sits in front of enterprise applications worldwide, delivered as a cloud-native platform. Load balancing isn't an afterthought or a paid extra; it's a core capability in every plan.

That matters because real applications have more than one backend. A typical deployment runs at least two application servers behind a balancer, often more. Charging extra for that fundamental capability — as several WAF-only vendors do — is a billing decision, not a technical one.

---

## Section

**H2:** Route traffic the way your application needs.

- **Round-robin** — distribute requests evenly across all healthy backends
- **Hash-based** — route consistently by source IP, session cookie, or URL, for sticky sessions without server-side state
- **Weighted** — assign more traffic to backends with more capacity
- **Least connections** — route to the backend currently handling the fewest active connections

---

## Section

**H2:** Failures handled before your users see them.

**Body:** CrownWall continuously checks the health of every backend, removing unhealthy nodes from rotation automatically and restoring them when they recover.

- **HTTP health checks** — request a URL, expect a specific status code and optional response body
- **TCP health checks** — verify port availability for non-HTTP services
- **gRPC health checks** — using the standard gRPC health-checking protocol
- **Configurable thresholds** — tune how aggressively flapping backends are removed

---

### Section

**H2:** Built for infrastructure that moves.

**Body:** Modern backends rarely have static IPs — they live in autoscaling groups, container orchestrators, and cloud environments. CrownWall resolves backend hostnames dynamically, picking up new instances and dropping terminated ones with no manual reconfiguration.

Optionally cache responses at the edge, with full control over cache keys, TTL, and which requests bypass the cache — reducing origin load and improving performance for read-heavy workloads.

**Callout box: What this replaces.** For many customers, CrownWall replaces a separate reverse proxy, a cloud load balancer, a bolt-on WAF, and a paid bot management plugin — with one subscription, one dashboard, and one logging pipeline.

---

**Feature tags:** Round-robin · Hash-based · Weighted · Least-connections · HTTP/TCP/gRPC health checks · Dynamic DNS · Response caching · Keep-alive · Automatic failover

---

### CTA band

**H2:** Deliver every request to a healthy backend. **[BUTTON: Start free trial] [BUTTON: Request a demo]**

---

---

## PAGE 6 — API SECURITY

**Page title:** API Security — CrownWall **URL slug:** /products/api-security

### Hero

**Eyebrow:** PRODUCTS / API SECURITY

**H1:** Protection that fits how APIs actually work.

**Subhead:** Per-endpoint rate limiting, schema validation, and abuse detection — built for the authenticated, machine-to-machine reality of modern APIs, not retrofitted from website tooling.

**[BUTTON primary: Start free trial] [BUTTON secondary: Request a demo]**

`[Visual: API requests with keys/tokens being validated and rate-limited per endpoint.]`

---

## Section

**H2:** Limit by what the abuse actually looks like.

**Body:** Basic protection throttles by source IP. That works for crude floods but fails for everything else — authenticated abuse, distributed attacks from residential proxies, API-key sharing, and credential stuffing all bypass IP-based limits easily.

CrownWall's Layer 7 controls work with full request context. You build limits that match the real abuse pattern, not just a generic ceiling.

---

## Section

**H2:** Granular by design.

- **Per IP** — the classic baseline limit
- **Per header / API key** — limit each unique API key to its own rate
- **Per cookie / session** — limit per authenticated session
- **Per URL parameter** — limit by user ID, account ID, or similar identifiers
- **Per request-body field** — for POST endpoints where the identifier sits in the JSON body
- **Per concurrency** — cap in-flight requests, not just requests per second

**Callout box: API protection in practice** — the right limit often isn't "100 requests per second per IP." It's "no more than 5 password-reset requests per email address per hour." That kind of business-logic limit is exactly what CrownWall's API controls are for.

---

## Section

**H2:** Reject malformed requests before they reach your code.

**Body:** Validate incoming requests against your API schema — reject calls with unexpected fields, wrong types, or malformed payloads at the edge, before they touch your application. CrownWall also surfaces the endpoints actually receiving traffic, helping you identify shadow APIs you didn't know were exposed.

---

**Feature tags:** Per-key rate limiting · Per-endpoint scoping · Schema validation · Concurrency limits · Composed rules · Shadow API discovery · JSON inspection · 429 + Retry-After handling

---

### CTA band

**H2:** Give your APIs protection that understands them. **[BUTTON: Start free trial] [BUTTON: Request a demo]**

---

---

## PAGE 7 — OBSERVABILITY & COMPLIANCE

**Page title:** Observability & Compliance Reporting — CrownWall **URL slug:** /products/observability

### Hero

**Eyebrow:** PRODUCTS / OBSERVABILITY & COMPLIANCE

**H1:** Auditable. Exportable. Built for the questionnaire.

**Subhead:** Real-time analytics across traffic, threats, and rules — plus one-click compliance reports formatted for the frameworks your auditors actually ask about.

**[BUTTON primary: Start free trial] [BUTTON secondary: Request a demo]**

`[Visual: split — live metrics dashboard on left, generated PDF compliance report on right.]`

---

### Section

**H2:** Understand what's happening, at a glance.

**Body:** Most security tools hand you raw log dumps and leave you to work out what they mean. CrownWall gives you pre-aggregated metrics across every dimension you'd want: requests by domain, by rule, by tenant; attack types blocked; bot categories; top-targeted endpoints; response codes; latency distributions.

Everything is available as interactive dashboards and exportable as CSV, JSON, or Prometheus metrics for your own observability stack.

---

### Section

**H2:** A complete, queryable record.

- **Request ID logs** — every request gets a unique ID logged on ingress and egress, with full request/response correlation
- **Tenant access logs** — attributed to the specific tenant or customer in multi-tenant deployments
- **Domain metrics** — request volume, error rates, and latency per protected domain
- **WAF rule metrics** — which rules fire, how often, against which sources
- **Bot category metrics** — what's hitting you and what action was taken
- **Rule change audit trail** — every configuration change, who made it, when, and what changed

---

## Section

**H2:** The evidence your auditor wants, in one click.

**Body:** Every business in a regulated sector eventually faces the same question from an auditor: show me your WAF coverage, your incident log, and your change history. Most vendors leave you to assemble that by hand from raw logs. CrownWall generates it in one click, formatted for the specific framework you're being assessed against.

`[Visual: compliance framework badge grid — PCI-DSS, NIS2, GDPR, ISO 27001, SOC 2, Cyber Essentials]`

- **PCI-DSS v4** — covers Requirement 6.4.2 with the artefacts assessors request
- **NIS2** — incident reports formatted to the directive's structured reporting timelines
- **GDPR** — what was processed, where, with which controls applied
- **ISO 27001** — control mappings for the relevant Annex A controls
- **SOC 2** — evidence for the relevant Trust Services Criteria
- **Cyber Essentials Plus** — the technical controls evidence assessors specifically request

**Callout box: Why this matters.** Assembling WAF coverage evidence for a PCI-DSS audit typically takes a small team several days. With CrownWall it's a single export. For many customers, this one feature is the reason they switched.

---

**Feature tags:** Request ID logs · Tenant access logs · Domain & rule metrics · Bot analytics · One-click compliance reports · PCI-DSS / NIS2 / GDPR / ISO 27001 / SOC 2 · Prometheus export · Change audit trail

---

## CTA band

**H2:** Make your next audit a one-click export. **[BUTTON: Start free trial] [BUTTON: Request a**

**demo]**

---

---

# PAGE 8 — SOLUTION: FINANCIAL SERVICES & FINTECH

**Page title:** Web Security for Financial Services & Fintech — CrownWall **URL slug:** /solutions/financial-services

## Hero

**Eyebrow:** SOLUTIONS / FINANCIAL SERVICES & FINTECH

**H1:** Web security built for the sector where downtime means regulatory events.

**Subhead:** Financial services organisations face the most demanding combination of attack volume, compliance pressure, and operational expectation. CrownWall is configured for all three.

**[BUTTON primary: Start free trial] [BUTTON secondary: Request a demo]**

`[Visual: abstract representation of secure transaction flow. Dark navy. No literal bank or money imagery.]`

---

## Section

**H2:** The financial sector is the most targeted. For good reason.

**Body:** Fintechs and financial services organisations are targeted by both opportunistic attackers and organised groups. The threats are familiar — credential stuffing against customer login portals, card-testing attacks against payment APIs, transaction manipulation attempts — but the consequence of failure is amplified. Lost funds, regulatory escalation, mandatory notification, and customer trust erosion arrive simultaneously.

---

## Section

**H2:** Every layer, mapped to your compliance obligations.

**WAF + PCI-DSS v4** CrownWall's WAF satisfies PCI-DSS Requirement 6.4.2 with exportable evidence for QSA review — coverage reports, rule audit trails, and incident logs formatted for assessors, not engineers.

**API protection for transaction endpoints** Granular L7 rate limiting at the endpoint level prevents card-testing, BIN enumeration, and high-volume API abuse against payment flows. Per-key and per-session limits — not blunt per-IP throttling.

**Credential stuffing defence** Bot control tuned for authentication endpoints. Challenge options for high-risk login patterns without friction for legitimate customers.

**Incident logging for regulatory reporting** Structured logs matching the categorisation frameworks regulators and insurers expect. Full request/response correlation for forensic reconstruction.

**Data residency** Deploy in the jurisdiction your regulatory framework requires. EU, UK, North America, and APAC available — with explicit data location commitments in the contract.

---

### Compliance frameworks

`[Visual: badge grid]` PCI-DSS v4 · DORA · UK GDPR · EU GDPR · NIS2 · ISO 27001 · SOC 2 · Cyber Essentials Plus

---

### CTA band

**H2:** Protect your applications. Satisfy your auditors. **[BUTTON: Request a demo] [BUTTON: Contact our team]**

---

---

## PAGE 9 — SOLUTION: HEALTHCARE & HEALTHTECH

**Page title:** Web Security for Healthcare & Healthtech — CrownWall **URL slug:** /solutions/healthcare

### Hero

**Eyebrow:** SOLUTIONS / HEALTHCARE & HEALTHTECH

**H1:** For systems where patient data is the asset — and the liability.

**Subhead:** Healthcare operates under the most stringent data protection requirements. CrownWall provides the technical controls and audit evidence to meet them.

**[BUTTON primary: Start free trial] [BUTTON secondary: Request a demo]**

---

### Section

**H2:** Healthcare is the highest-value target for data theft. The evidence trail matters as much as the protection.

**Body:** Healthtech faces a unique combination: the most sensitive personal data category under data protection law, tight integration with health authority infrastructure, and regular assessments from regulators, commissioners, and enterprise clients. A breach affecting patient data carries reporting obligations, regulatory investigation, and reputational consequences that are disproportionate to what the original technical failure might suggest. Prevention is important. Documented prevention is essential.

---

### Section

**H2:** Protection and auditability, together.

**Patient portal protection** Bot control tuned for authentication endpoints, with step-up challenge options for sensitive access flows. Credential stuffing against patient login portals is the most common attack vector in the sector.

**Structured incident logging** Logs formatted to support the 72-hour breach notification timeline required under data protection law. Full request-response correlation for forensic reconstruction.

**Data residency you can document** All traffic processed in your specified jurisdiction. No third-country transfers. A direct answer to data-location questions in every enterprise and public-sector procurement.

**One-click compliance exports** Evidence packages formatted for the frameworks healthcare organisations face — structured for assessors, not security engineers.

---

### Compliance frameworks

UK GDPR · EU GDPR · NIS2 · ISO 27001 · ISO 27701 · SOC 2 · Cyber Essentials Plus

---

### CTA band

**H2:** Protect patient data. Document every control. **[BUTTON: Request a demo] [BUTTON: Contact our team]**

---

---

## PAGE 10 — SOLUTION: E-COMMERCE & RETAIL

**Page title:** Web Security for E-commerce & Retail — CrownWall **URL slug:** /solutions/ecommerce

**Eyebrow:** SOLUTIONS / E-COMMERCE & RETAIL

**H1:** Stay online during your busiest moments. And your most attacked ones.

**Subhead:** E-commerce sites face high bot volume, unpredictable traffic spikes, and PCI scope. CrownWall handles all three — so a Black Friday attack doesn't become a Black Friday outage.

**[BUTTON primary: Start free trial] [BUTTON secondary: Request a demo]**

---

## Section

**H2:** Your traffic peaks are your most vulnerable moments.

**Body:** E-commerce operations face a particular blend of pressures: bot traffic at scale, credential stuffing against customer accounts, unpredictable spikes during sale events that expose any capacity weakness, and annual PCI assessments. Attackers know that sale days are the worst time for your team to handle an incident. The timing is deliberate.

---

## Section

**H2:** Resilience and compliance, built in.

**Bot mitigation that distinguishes threat from customer** Block price-monitoring bots, inventory checkers, and scrapers without disrupting Googlebot or legitimate price-comparison services.

**Credential stuffing protection** Automated login attacks using leaked credentials are the primary threat to customer account integrity. Bot control tuned for authentication endpoints catches what standard WAF rules miss.

**Load balancing during traffic spikes** Health-aware routing distributes load automatically. A slow database doesn't drag down the storefront. Unhealthy backends are removed and restored without manual intervention.

**Response caching** Cache product pages and static content at the edge — reducing origin load during peak periods and keeping response times consistent when traffic multiplies.

**PCI scope confirmation** Exportable WAF coverage evidence for PCI-DSS Requirement 6.4.2, formatted for QSA review.

---

## Compliance frameworks

PCI-DSS v4 · GDPR · ISO 27001 · Cyber Essentials Plus

---

**H2:** Protect your revenue. Especially when it matters most. **[BUTTON: Request a demo]** **[BUTTON: Contact our team]**

---

---

## PAGE 11 — SOLUTION: SaaS & TECHNOLOGY

**Page title:** Web Security for SaaS & Technology Companies — CrownWall **URL slug:** /solutions/saas

### Hero

**Eyebrow:** SOLUTIONS / SaaS & TECHNOLOGY

**H1:** Protection built for how SaaS actually works.

**Subhead:** API-first, multi-tenant, authenticated by default. Most WAFs were designed for static websites. CrownWall was built for the reality of modern SaaS.

**[BUTTON primary: Start free trial] [BUTTON secondary: Request a demo]**

---

### Section

**H2:** Between free and enterprise, there's a gap — and that's where most SaaS companies sit.

**Body:** Free-tier cloud WAFs lack the custom rules, per-endpoint controls, and compliance evidence that enterprise customers and security questionnaires expect. Enterprise security platforms are priced for Fortune 500 budgets and sold through procurement cycles measured in quarters. CrownWall occupies the middle — built for API-first SaaS architectures, priced for growing businesses, with the compliance features paying customers and their auditors ask for.

---

### Section

**H2:** Every layer of a modern SaaS stack.

**Per-endpoint protection** Different rules for your public site, your authenticated API, and your admin interface — all on one platform, one dashboard, one logging pipeline.

**API key rate limiting** Limit per API key, not per source IP. The only model that makes sense when your customers integrate from shared egress infrastructure.

**Multi-tenant logging** Attribute every request to the right tenant. Per-tenant metrics for support triage and security investigations — and proof of isolation for enterprise customers.

**Customer-facing compliance evidence** Your customers send security questionnaires. CrownWall provides the WAF, bot, and API protection evidence sections — exportable as PDF, formatted for SOC 2 and ISO 27001 assessors.

**Audit trail for SOC 2 / ISO 27001** Every rule change, every configuration modification, every incident logged with timestamps and user attribution. Exactly what auditors request.

---

### Compliance frameworks

SOC 2 Type II · ISO 27001 · GDPR · CCPA · Cyber Essentials Plus · NIS2 (where applicable)

---

### CTA band

**H2:** Security your customers can evidence. Infrastructure your engineers can trust. **[BUTTON: Request a demo] [BUTTON: Contact our team]**

---

---

## PAGE 12 — SOLUTION: GAMING & MEDIA

**Page title:** Web Security for Gaming & Media — CrownWall **URL slug:** /solutions/gaming-media

### Hero

**Eyebrow:** SOLUTIONS / GAMING & MEDIA

**H1:** Low-latency protection for experiences where milliseconds matter.

**Subhead:** Gaming and media platforms face constant DDoS, relentless bot activity, and traffic spikes without warning. CrownWall defends your infrastructure without adding latency your players and viewers will notice.

**[BUTTON primary: Start free trial] [BUTTON secondary: Request a demo]**

---

### Section

**H2:** Gaming is the most attacked sector by volume. Media platforms are the most scraped.

**Body:** Online gaming attracts DDoS attacks designed to knock players offline, disrupt competitive events, and extort platform operators. Bots manipulate game economies and player rankings. Media platforms face content scrapers harvesting paywalled content, ad fraud bots, and origin floods timed to high-traffic moments. Both sectors share zero tolerance for latency. Protection that adds noticeable delay is not protection — it's a different kind of problem.

---

### Section

**H2:** Edge filtering that happens before your infrastructure sees the traffic.

**DDoS absorption at the edge** Volumetric and application-layer attacks absorbed at the network edge. Clean traffic continues uninterrupted. Players and viewers stay online.

**Bot management with gaming context** Differentiate between legitimate game clients, cheating tools, credential stuffing bots, and inventory-manipulation automation — without challenging legitimate players.

**Load balancing for traffic spikes** Event-driven traffic is unpredictable. Health-aware routing distributes load automatically and maintains performance as traffic multiplies.

**Content protection for media** Rate limiting and bot controls tuned for content-delivery endpoints. Protect paywalled content and manage crawler access without breaking legitimate aggregation.

---

### CTA band

**H2:** Stay online. No matter what's coming at you. **[BUTTON: Request a demo] [BUTTON: Contact our team]**

---

---

## PAGE 13 — SOLUTION: PUBLIC SECTOR

**Page title:** Web Security for Public Sector Organisations — CrownWall **URL slug:** /solutions/public-sector

### Hero

**Eyebrow:** SOLUTIONS / PUBLIC SECTOR

**H1:** Sovereign, compliant, and resilient by design.

**Subhead:** Public sector web infrastructure demands data sovereignty, verifiable compliance, and resilience against politically-motivated attack. CrownWall is built to meet all three.

**[BUTTON primary: Request a demo] [BUTTON secondary: Contact our team]**

---

### Section

**H2:** Public sector infrastructure is a target because disruption is the point.

**Body:** Attacks on public sector web infrastructure are frequently motivated by disruption rather than financial gain. A government service going offline, a citizen portal becoming unavailable, or a public authority website being defaced carries political and reputational consequences entirely disproportionate to the technical incident. Compliance obligations are also more demanding: data residency requirements are non-negotiable, procurement requires demonstrable certification, and supply-chain standards mandate documented controls throughout.

---

### Section

**H2:** Data sovereignty, documented compliance, and continuous resilience.

**Data residency with contractual commitment** All traffic processed in the jurisdiction you specify. A contractual commitment — not a dashboard setting.

**NIS2 alignment** Structured incident logging and reporting tools support mandatory notification timelines and evidence requirements for operators of essential services.

**Cyber Essentials Plus evidence** Increasingly required for government supply-chain participation. CrownWall provides the technical controls evidence assessors specifically request.

**Always-on availability** DDoS absorption at the edge, health-aware load balancing, and automated failover — so citizen-facing services remain available regardless of attack scale.

---

### Compliance frameworks

NIS2 · UK GDPR · ISO 27001 · Cyber Essentials Plus · NCSC guidance alignment · DORA (where applicable)

---

### CTA band

**H2:** Build services the public can rely on. **[BUTTON: Request a demo] [BUTTON: Contact our team]**

---

---

## PAGE 14 — HOW IT WORKS: THE PLATFORM

**Page title:** How CrownWall Works — CrownWall **URL slug:** /how-it-works

### Hero

**Eyebrow:** HOW IT WORKS

**H1:** One engine for delivery and security.

**Subhead:** CrownWall is a complete application delivery controller — delivery and security running in the same pipeline, because they were always the same job.

`[Visual: horizontal request pipeline — Client → TLS Termination → Bot Check → WAF Inspection → Rate Limit → Load Balance → Backend Origin. Left-to-right flow, teal accent on each stage node.]`

---

## Section

**H2:** Security bolted on is security with gaps.

**Body:** Most organisations arrive at CrownWall having assembled a stack: a cloud load balancer here, a WAF plugin there, a bot management service on top, a compliance reporting tool pulling from three different log sources. Each product sees a fragment of the traffic. None of them see the whole picture. The gaps between them are where attackers operate.

CrownWall processes every request through a single, ordered pipeline. Every layer sees the full request context. WAF rules can reference rate-limit state. Bot decisions inform load-balancing choices. Logs from every layer arrive in one place, correlated by a single request ID. There are no gaps.

---

## Section

**H2:** What happens to every request, in order.

`[Visual: 8-step numbered pipeline diagram]`

**1. TLS termination** Connection terminated at the CrownWall edge using your certificate — provided by you or managed automatically via Let's Encrypt. HTTP/1.1, HTTP/2, and WebSocket supported natively.

**2. Protocol normalisation** Request parsed and normalised. Encoding-bypass attempts neutralised at this stage before any rule evaluation.

**3. IP reputation & geo checks** Fast lookup against continuously updated IP reputation data. Geographic filters applied if configured.

**4. Bot identification** Client classified as known good bot, known bad bot, or unclassified. Unclassified clients are fingerprinted for behavioural analysis.

**5. WAF rule evaluation** Managed and custom rulesets evaluated against the full request — referencing bot classification, geo data, and header context.

**6. Rate limit checks** All configured rate limits evaluated across all configured dimensions: per IP, per key, per session, per endpoint, per concurrency.

**7. Routing decision** Backend selected based on load-balancing configuration and live health-check state. Response served from cache if configured.

**8. Origin forward** Request forwarded to the selected backend. Original client information preserved in standard headers. Unique request ID logged end-to-end.

**Callout box:** Each layer runs in single-digit milliseconds. The full pipeline typically adds 10–20ms to request latency. For cached responses, the origin is not contacted at all.

---

### Section

**H2:** Live in four steps.

`[Visual: 4-step numbered flow]`

**1. Add your domain** — Add the domain you want to protect. CrownWall verifies ownership and provisions your edge configuration. **2. Configure your origins** — Tell CrownWall where your application runs. Set up health checks for multiple backends. **3. Apply your security policy** — Managed WAF rulesets active by default. Refine with custom rules. Test in shadow mode before enforcing. **4. Point your DNS** — Update DNS to point at CrownWall. Traffic flows through within minutes of propagation.

**[BUTTON: Start free trial — deploy today]**

---

---

## PAGE 15 — ARCHITECTURE & NETWORK

**Page title:** Architecture & Global Network — CrownWall **URL slug:** /how-it-works/architecture

### Hero

**Eyebrow:** HOW IT WORKS / ARCHITECTURE

**H1:** Built to absorb. Built to scale.

**Subhead:** CrownWall's distributed edge architecture processes and filters traffic close to its source — reducing latency for clean requests and neutralising attacks before they reach your origin.

---

### Section

**H2:** The further from your origin the better.

**Body:** Every component of CrownWall's security pipeline runs at the edge — geographically close to the users and attackers sending traffic. Clean requests travel a short path to your origin.

Attacks are absorbed and discarded without ever placing load on your infrastructure.

This architecture makes DDoS mitigation effective at scale. A volumetric attack that would overwhelm most origin servers is distributed across CrownWall's edge capacity, where the ratio of filtering capacity to attack volume is fundamentally different.

---

### Section

**H2:** Key architecture principles.

`[Visual: 3-column principle cards]`

**Multi-node distribution** No single point of failure. Traffic is processed across multiple nodes, and your workload is automatically redistributed if any node becomes unavailable.

**Asynchronous logging** All request logging happens out of the live request path. Logging latency never affects application response times. Logs are complete, not sampled.

**Health-aware routing** Continuous health checks against all configured backends. Unhealthy origins removed from rotation within seconds of a check failure and restored automatically on recovery.

**Horizontal scaling** Capacity scales with traffic volume. No appliances to size, no hardware limits to plan around, no performance degradation during attack events.

---

### Section

**H2:** Available regions.

`[Visual: clean world map with region markers]`

European Union · United Kingdom · North America · Asia-Pacific

For specific sovereignty requirements or multi-region deployments, contact our team.

---

---

## PAGE 16 — DATA RESIDENCY

**Page title:** Data Residency & Sovereignty — CrownWall **URL slug:** /how-it-works/data-residency

### Hero

**Eyebrow:** HOW IT WORKS / DATA RESIDENCY

**H1:** Your data stays where you need it to.

**Subhead:** Data residency is a contractual commitment in CrownWall, not a configuration option. Your traffic is processed and logged in the region you specify.

---

## Section

**H2:** A dashboard setting is not a compliance answer.

**Body:** For regulated organisations, "we try to keep your data in region" is not an acceptable answer to a data-protection audit. The question is whether the commitment is contractual, documented, and verifiable.

CrownWall's data residency options are written into your service agreement, enforced by region-isolated architecture, and documented in your compliance reports — showing where traffic was processed and when.

---

## Section

**H2:** Common regulatory questions, direct answers.

**GDPR Article 44 — third-country transfers** Traffic processed in your specified EU or UK region does not constitute a third-country transfer. No Schrems II analysis required for that traffic.

**NIS2 — data location for essential services** For operators of essential services with specific data-location obligations, CrownWall's regional isolation and contractual commitments support compliance.

**Sector-specific sovereignty requirements** For financial services, healthcare, public sector, and defence-adjacent organisations with more specific requirements, custom data-residency arrangements are available. Contact our team.

---

## Section

**H2:** Available regions.

`[Visual: region cards]`

**EU** — Frankfurt · Amsterdam **UK** — London **North America** — New York · Toronto **Asia-Pacific** — Singapore · Sydney

**[BUTTON: Discuss your requirements →]** (links to /company/contact)

---

---

# PAGE 17 — INTEGRATIONS

**Page title:** Integrations — CrownWall **URL slug:** /how-it-works/integrations

### Hero

**Eyebrow:** HOW IT WORKS / INTEGRATIONS

**H1:** Fits into your stack. Doesn't replace it.

**Subhead:** CrownWall sits in front of your existing infrastructure. No agents, no code changes, no rearchitecting — and it pushes data to the security and observability tools your team already uses.

---

### Section

**H2:** A reverse proxy in front of what you already have.

**Body:** CrownWall operates as a transparent reverse proxy. Your application receives requests with standard forwarded-for headers and a unique request ID for correlation. No SDK, no agent, no library to install. DNS change, then done.

---

### Section

**H2:** Outbound integrations.

`[Visual: integration logo grid — 3×2 cards]`

**SIEM & logging** Push access logs, WAF events, and attack notifications to your SIEM via syslog, webhook, or direct integration. Supported formats: CEF, JSON, W3C. Supported platforms: Splunk · Elastic/ELK · Datadog · Sumo Logic · Microsoft Sentinel · IBM QRadar

**Alerting & incident response** Attack notifications, threshold alerts, and health-check failures delivered via webhook. Connects to PagerDuty, Opsgenie, Slack, and any webhook-compatible platform.

**Metrics & observability** Prometheus metrics endpoint for scraping. Datadog and Grafana dashboard templates available.

**Infrastructure as code** REST API for full configuration management. Terraform provider available. Rules and policies managed as code through your existing pipeline.

**DNS providers** Works with any DNS provider — Cloudflare DNS, Route 53, Azure DNS, GoDaddy, and any provider supporting CNAME records.

---

### Section

**H2:** Full API for teams that automate everything.

**Body:** Every configuration action available in the dashboard is available via REST API. Create domains, manage rules, retrieve logs, pull metrics, manage tenants — all programmable. API documentation and client libraries available in our documentation portal.

**[BUTTON: API documentation →]**

---

---

# PAGE 18 — PRICING

**Page title:** Pricing — CrownWall **URL slug:** /pricing

## Hero

**Eyebrow:** PRICING

**H1:** Simple plans. No surprises.

**Subhead:** Everything included at every tier. No per-feature billing. No extra charges during an attack. Cancel or change plan any time.

---

## Pricing tiers

`[Designer note: 4-column pricing table. Business tier highlighted with teal border + "Most popular" badge above. Each column: tier name, price, description, feature list, CTA button. Sticky on scroll.]`

**Note to designer:** Pricing figures are TBD — use `[price TBC]` placeholder. Numbers to be confirmed separately and dropped in before launch.

---

### Starter

**Price:** [price TBC] /month **Description:** One domain. For a single web app or SaaS product getting started.

- WAF + managed OWASP rules
- Bot management (standard)
- DDoS protection
- Load balancing (2 origins)
- Basic observability
- Email support
- ✗ Compliance reports

- ✗ Custom rules (max 5 included)

**[BUTTON: Start free trial]**

---

**Business — ⭐ Most popular**

**Price:** [price TBC] /month **Description:** Up to 5 domains. The compliance-ready tier for growing companies.

- Everything in Starter
- Unlimited custom rules
- Load balancing (up to 10 origins)
- Compliance audit reports (PCI-DSS, NIS2, GDPR)
- API security controls
- 30-day log retention
- Email + chat support, 4hr response SLA

**[BUTTON: Start free trial]**

---

**Professional**

**Price:** [price TBC] /month **Description:** Unlimited domains. For multi-property businesses and platform operators.

- Everything in Business
- Multi-tenant portal
- Unlimited origins
- 90-day log retention
- Phone support, 1hr response SLA
- Onboarding session with our team

**[BUTTON: Start free trial]**

---

**Enterprise**

**Price:** Contact our team **Description:** Dedicated tenancy, custom SLAs, and tailored data residency.

- Everything in Professional
- Dedicated infrastructure
- Custom data residency commitments
- 15-min response SLA, 99.99% uptime SLA

- Named account manager
- Custom contracts and invoicing
- MSP / white-label options

**[BUTTON: Contact our team]**

---

## Annual discount callout

`[Callout box — teal left border]` **Save 20% with annual billing.** All plans available on annual prepaid terms. Contact us to arrange.

---

## Feature comparison table

`[Designer note: full feature comparison table — sticky header on scroll, tick/cross/text values, rows = features, columns = 4 tiers.]`

| Feature | Starter | Business | Professional | Enterprise |
|---|---|---|---|---|
| Domains | 1 | 5 | Unlimited | Unlimited |
| Requests/month | 5M | 50M | 200M | Custom |
| Custom WAF rules | 5 | Unlimited | Unlimited | Unlimited |
| Bot management | Standard | Advanced | Advanced | Advanced |
| DDoS protection | ✓ | ✓ | ✓ | ✓ |
| Load balancing | 2 origins | 10 origins | Unlimited | Unlimited |
| API security | ✓ | ✓ | ✓ | ✓ |
| Log retention | 7 days | 30 days | 90 days | Custom |
| Compliance reports | — | PCI / NIS2 / GDPR | + SOC 2 / ISO 27001 | Custom |
| Multi-tenant portal | — | — | ✓ | ✓ |
| Support channel | Email | Email + chat | Phone | Named contact |
| Response SLA | — | 4 hours | 1 hour | 15 minutes |
| Uptime SLA | 99.9% | 99.95% | 99.99% | 99.99% |
| Data residency | Shared | Shared | Shared | Dedicated |
| Free trial | 14 days | 14 days | 14 days | POC available |

## FAQ

**H2:** Common questions.

**Q: Is there a free tier?** There is no permanent free tier. All paid plans include a 14-day full-feature free trial — no credit card required.

**Q: Does attack traffic count toward my request allowance?** No. Blocked and mitigated requests do not count. You pay only for legitimate traffic reaching your origins.

**Q: What happens if I exceed my request allowance?** Your service continues uninterrupted. We'll notify you when you approach the limit and discuss upgrading your plan.

**Q: Can I change plan mid-month?** Yes. Upgrades take effect immediately. Downgrades take effect at the next billing cycle.

**Q: Are there setup or onboarding fees?** None. No setup fees on any plan. The Professional plan includes an onboarding session at no additional cost.

**Q: Do you offer volume pricing for MSPs?** Yes. Contact our team to discuss reseller and MSP pricing arrangements.

---

### CTA band

**H2:** Not sure which plan is right for you? **Body:** Talk to our team. We'll recommend the right fit based on your domains, traffic, and compliance requirements. **[BUTTON: Contact our team]**

---

---

## PAGE 19 — KNOWLEDGE HUB

**Page title:** Knowledge Hub — CrownWall **URL slug:** /resources/knowledge-hub

### Hero

**Eyebrow:** RESOURCES / KNOWLEDGE HUB

**H1:** Understand the threats. Choose the right protection.

**Subhead:** In-depth guides, threat analysis, compliance frameworks explained, and technical deep-dives for security professionals and decision-makers.

---

### Section — Categories

`[Designer note: 3-column card grid, each linking to filtered content]`

**Threat Intelligence** Understand the attack landscape — DDoS trends, bot evolution, web exploitation techniques, and how the threat is changing.

**Compliance Guides** Plain-language explanations of PCI-DSS v4, NIS2, GDPR, SOC 2, ISO 27001, and Cyber Essentials — what they require, what evidence they need, and how CrownWall supports each.

**Technical Guides** Deep-dives into WAF rule construction, rate-limiting patterns, API security design, and load-balancing architectures.

---

### Section — Featured articles

`[Designer note: 3-column article card grid. Each card: category label, title, 2-line description, read time, "Read →" link. These are article templates — fill with`

`content over time.]`

**Article 1** Category: Threat Intelligence Title: The 2025 web application attack landscape — what changed and what to watch Read time: 8 min

**Article 2** Category: Compliance Guides Title: PCI-DSS v4 Requirement 6.4.2 — what the WAF mandate actually means Read time: 6 min

**Article 3** Category: Technical Guides Title: Why per-IP rate limiting fails against modern credential stuffing Read time: 5 min

**Article 4** Category: Technical Guides Title: API security in practice — designing rate limits that match real abuse patterns Read time: 7 min

**Article 5** Category: Compliance Guides Title: NIS2 incident reporting — timelines, obligations, and what to prepare Read time: 6 min

**Article 6** Category: Threat Intelligence Title: Bot traffic in 2025 — how to distinguish threats from customers at scale Read time: 9 min

---

---

# PAGE 20 — WHITEPAPERS & REPORTS

**Page title:** Whitepapers & Reports — CrownWall **URL slug:** /resources/whitepapers

## Hero

**Eyebrow:** RESOURCES / WHITEPAPERS & REPORTS

**H1:** Research you can take to the table.

**Subhead:** Downloadable reports and guides for security teams, compliance leads, and IT decision-makers.

---

## Report library

`[Designer note: report card grid — each card has a cover thumbnail (publication-style design), title, brief description, format badge (PDF), download button. These are templates — populate with real reports over time.]`

**Report 1** Title: Annual Threat Report — Web Application Security [Year] Description: Analysis of web application attack trends, volumes, and patterns, with implications for defensive posture. Format: PDF [BUTTON: Download free]

**Report 2** Title: PCI-DSS v4 Compliance Guide for Web Applications Description: Plain-language guide to Requirement 6.4.2 — what it requires, how to demonstrate compliance, and what evidence assessors request. Format: PDF [BUTTON: Download free]

**Report 3** Title: NIS2 Directive — Practical Guide for Web Infrastructure Operators Description: What NIS2 means for organisations with internet-facing web applications and APIs. Timelines, obligations, and practical steps. Format: PDF [BUTTON: Download free]

**Report 4** Title: The Bot Management Buyer's Guide Description: How to evaluate bot management platforms — what questions to ask, what capabilities to require, and how to avoid common selection mistakes. Format: PDF [BUTTON: Download free]

---

---

# PAGE 21 — SUCCESS STORIES

**Page title:** Success Stories — CrownWall **URL slug:** /resources/success-stories

## Hero

**Eyebrow:** RESOURCES / SUCCESS STORIES

**H1:** Relied on when it matters.

**Subhead:** How organisations across financial services, healthcare, e-commerce, SaaS, and the public sector have used CrownWall to protect their applications and satisfy their auditors.

---

## Client logo grid

`[Designer note: full-width logo grid — 50 client logos to be provided. Greyscale, colour on hover. 5–6 per row on desktop, 3 per row on mobile.]`

**Label above grid:** Trusted by organisations across 30+ countries

---

## Success story cards

`[Designer note: 3-column card grid. Each card: client logo, industry badge, one-line outcome headline, pull-quote snippet, "Read story →" link. Cards link to individual story pages.]`

`[Content to be populated once client provides story details and approvals. Individual story page template below.]`

---

## Individual success story page template

`[Designer note: each success story uses this layout. URL pattern: /resources/success-stories/[client-slug].]`

---

**[Client logo] [Client name] — [Industry] — [Region]**

**H1:** [One-sentence outcome headline] *Example: "How [Client] reduced audit preparation time from three days to one export."*

---

**Pull quote (large, prominent):** *"[Client quote — 1–2 sentences. Specific, credible, direct.]"* — [Name, Title, Client]

---

**Three metric cards:**

- [Metric 1]: e.g. 99.99% uptime maintained during peak attack period
- [Metric 2]: e.g. PCI-DSS assessor review completed in 3 hours
- [Metric 3]: e.g. Zero false positives in first 30 days

---

**The challenge:** [3–4 sentences: what problem the client was facing before CrownWall. Specific — what was failing, what was at risk, what triggered the decision to change.]

**The solution:** [3–4 sentences: what they deployed, how it was configured, which capabilities they used. Link to relevant product pages.]

**The result:** [3–4 sentences: specific, measurable outcomes. Concrete numbers where possible.]

---

**Products used:** [Pill badges linking to relevant product pages]

**[BUTTON: Read next story →] [BUTTON: Start your free trial]**

---

---

# PAGE 22 — PRESS & MEDIA

**Page title:** Press & Media — CrownWall **URL slug:** /resources/press

## Hero

**Eyebrow:** RESOURCES / PRESS & MEDIA

**H1:** News, coverage, and announcements.

---

`[Designer note: tabbed layout — tabs: Press Releases · Media Coverage · Awards. Vertical list of cards below tabs. Newest first.]`

**Each card structure:**

- Date: [DD Month YYYY]
- Headline: [announcement or coverage headline]
- Teaser: [2 sentences]
- [Read →] link

`[Content populated as releases are issued. Template structure above.]`

---

### Media enquiries

**H2:** For press enquiries.

**Body:** For interview requests, product briefings, or analyst relations, please use the form below. We respond to press enquiries within one business day.

`[Form fields: Name · Organisation · Email · Nature of enquiry (dropdown: Interview request / Product briefing / Analyst relations / Other) · Message. Submit button.]`

---

---

## PAGE 23 — PARTNERS

**Page title:** Partner with CrownWall **URL slug:** /partners

### Hero

**Eyebrow:** PARTNERS

**H1:** Deliver world-class web security under your brand.

**Subhead:** CrownWall works with resellers, managed service providers, and technology partners worldwide. If you're interested in adding web application security to your portfolio, we'd like to hear from you.

---

### Section

**H2:** Why partner with CrownWall.

`[3-column card grid]`

**Full-featured platform** A complete WAF, bot, DDoS, load balancing, and compliance platform — not a single-feature tool. High value to end customers, high retention for you.

**White-label ready** Multi-tenant portal designed for MSP and reseller deployments. Your brand, your customers, your billing.

**Commercial flexibility** Volume pricing, reseller margin structures, and co-selling arrangements. We build a model that works for your business.

---

### Section

**H2:** Who we work with.

- **Managed Service Providers (MSPs)** managing web security across multiple client estates
- **IT resellers** adding cloud security to their portfolio
- **System integrators** working with financial services, healthcare, or public sector clients
- **Technology partners** building CrownWall into their platforms

---

### Contact form

**H2:** Interested in partnering?

**Body:** Tell us about your business and what you're looking to achieve. Our partnerships team will be in touch within two business days.

`[Form fields:]`

- Your name *
- Your email *
- Organisation name *
- Country *
- Organisation type (dropdown: MSP · IT Reseller · System Integrator · Technology Partner · Other)
- Number of clients / end customers (dropdown: 1–10 · 11–50 · 51–200 · 200+)
- Tell us about your interest (textarea)

**[BUTTON: Send enquiry]**

---

---

## PAGE 24 — ABOUT

**Page title:** About CrownWall **URL slug:** /company/about

## Hero

**H1:** CrownWall.

**Subhead:** Application delivery and web security for businesses that have outgrown free tools — and don't want an enterprise sales cycle to get protected.

---

## Section

**H2:** One platform. Every layer of web defence.

**Body:** CrownWall is a cloud-native application delivery and web security platform. We combine WAF, bot management, DDoS protection, load balancing, API security, and compliance reporting in a single platform — deployed in minutes, managed from one dashboard, billed as one predictable subscription.

We exist because the market between "free tier with limits" and "enterprise with a six-month sales cycle" has been poorly served for too long. Growing businesses have real exposure and real compliance obligations. They need production-grade protection that fits their scale today and grows with them — without requiring a dedicated security team to operate it.

---

## Section

**H2:** Global operations. Direct support.

**Body:** CrownWall serves customers across EMEA, North America, and Asia-Pacific. Our support team responds directly — engineers, not tier-one script readers. Our sales process is a conversation, not a procurement cycle.

We operate edge infrastructure in the EU, UK, North America, and APAC, with data residency options that meet the regulatory requirements of every major market we serve.

---

## Certifications strip

`[Same certification logo strip as homepage — ISO 27001, SOC 2, PCI-DSS, Cyber Essentials Plus, NIS2. Links to Trust Centre.]`

**[BUTTON: View Trust Centre →]**

---

## LinkedIn

Follow us on LinkedIn for product updates, threat intelligence, and security industry news.
`[LinkedIn icon + link to CrownWall LinkedIn page]`

---

---

# PAGE 25 — TRUST CENTRE

**Page title:** Trust Centre — CrownWall **URL slug:** /company/trust-centre

## Hero

**Eyebrow:** COMPANY / TRUST CENTRE

**H1:** Security, compliance, and reliability — documented.

**Subhead:** Everything you need to evaluate CrownWall's security posture, confirm our certifications, and understand our operational commitments.

---

## Certifications

`[Designer note: 2×3 card grid. Each card: certification logo, name, brief description, action link.]`

**ISO 27001** International standard for information security management systems. Covers the policies, procedures, and controls governing how we manage and protect information assets. [View certificate →]

**SOC 2 Type II** Third-party audit of our security, availability, and confidentiality controls over a sustained period. Report available under NDA for enterprise evaluations. [Request report →]

**PCI-DSS Level 1 Service Provider** The highest level of PCI compliance for service providers. `[Status and badge to be added when achieved]`

**Cyber Essentials Plus** UK government-backed certification confirming technical controls against common cyber threats. Independently assessed. [View certificate →]

**NIS2 Aligned** CrownWall's platform and operational processes are aligned with the requirements of the EU NIS2 Directive for digital service providers.

**ISO 27701** Privacy information management system standard, extending ISO 27001 with privacy-specific controls. `[Status to be confirmed]`

---

## Security practices

**H2:** How we protect the platform that protects yours.

**Infrastructure security** All CrownWall infrastructure runs on hardened, patched systems with access limited by role and enforced by multi-factor authentication. All changes are logged and reviewed.

**Data handling** Customer traffic data is processed only in the regions specified in your service agreement. No customer data is used for training, sold to third parties, or accessed without your authorisation.

**Vulnerability management** We operate a continuous vulnerability disclosure programme. Security patches are applied on a defined schedule. Critical patches applied within 24 hours of availability.

---

### SLA table

**H2:** Operational commitments.

| Plan | Uptime SLA | Support response |
|---|---|---|
| Starter | 99.9% | Email |
| Business | 99.95% | 4 hours — email + chat |
| Professional | 99.99% | 1 hour — phone |
| Enterprise | 99.99% | 15 minutes — named contact |

---

### Responsible disclosure

**H2:** Report a security vulnerability.

**Body:** If you believe you have found a security vulnerability in CrownWall's platform, please report it to us before public disclosure. We commit to acknowledging reports within 48 hours and working with reporters in good faith.

`[Form: Name · Email · Vulnerability description · Severity (self-assessed: Critical / High / Medium / Low) · Steps to reproduce. Submit button.]`

---

---

## PAGE 26 — CONTACT

**Page title:** Contact CrownWall **URL slug:** /company/contact

### Hero

**H1:** Get in touch.

---

### Two-column layout

`[Designer note: generous whitespace, clean two-column split. Left: contact form. Right: phone number, brief directional text, LinkedIn link.]`

**LEFT — Contact form**

- Your name *
- Work email *
- Organisation *
- Your role (dropdown: Founder / Director · CTO / Engineering · IT Manager · Security / CISO · Compliance / DPO · MSP / Reseller · Other)
- I'm enquiring about (dropdown: Product information · Starting a trial · Compliance requirements · MSP or reseller partnership · Urgent security incident · Other)
- Tell us about your environment (textarea — optional)

**[BUTTON: Send message]**

*Small text below button:* We'll respond within one business day. Your details will only be used to reply to this enquiry.

---

**RIGHT — Phone & direct contact**

`[Display phone number prominently — TBC by client]`

`[LinkedIn icon]` Follow us on LinkedIn

---

*For urgent security incidents — use the* **Under Attack?** *link at the top of every page.*

---

---

# PAGE 27 — UNDER ATTACK / EMERGENCY

**Page title:** Under Attack? — Emergency Response · CrownWall **URL slug:** /emergency

`[Designer note: this page is urgent and single-purpose. Dark full-screen background — deep navy. Large clear headline. Single action above the fold. Minimal navigation — no mega-menu, no distractions. No footer links beyond Privacy Policy and "back to main site". The entire focus of this page is getting the visitor to`

`submit the form or call the number. Every design decision should serve that single goal.]`

## Hero (full screen, dark)

**H1:** We can have you protected in under 15 minutes.

**Subhead:** If your application is under active DDoS attack or web exploit right now, our emergency response team is standing by — 24 hours a day, 365 days a year.

---

## Emergency form (centred, prominent)

`[Designer note: form sits above the fold, large and clear. No distracting elements around it.]`

- Your name *
- Your email *
- Your domain or IP under attack *
- Describe what you're seeing * (textarea)

**[BUTTON — large, urgent red/teal: Get help now →]**

---

**Below form (prominent):** Or call us directly: **[Emergency phone number — TBC]**

---

## What happens next (3 steps, brief)

`[Designer note: visible below the form, very brief. Reassures the visitor while they wait. No marketing.]`

**1. We respond within 15 minutes** Our team contacts you by phone or email — whichever you provided.

**2. We assess your situation** Understanding what you're facing before we deploy anything.

**3. We route your traffic through CrownWall** A DNS change is all it takes. Protection active within minutes of your decision.

---

`[Minimal footer: CrownWall · Privacy Policy · Back to main site]`

---

---

# END OF DOCUMENT

## Summary — page count by section

| Section | Pages |
|---|---|
| Homepage | 1 |
| Product pages | 6 |
| Solution pages | 6 |
| How It Works | 4 |
| Pricing | 1 |
| Resources (Knowledge Hub, Whitepapers, Success Stories, Press) | 4 |
| Partners | 1 |
| Company (About, Trust Centre, Contact) | 3 |
| Emergency page | 1 |
| **Total** | **27** |

## Placeholders to complete before launch

| Item | Location | Action |
|---|---|---|
| Pricing figures | /pricing + pricing tier cards | Client to confirm — drop in before launch |
| Phone number | /company/contact + /emergency + footer | Client to confirm |
| 50 client logos | Homepage carousel + /resources/success-stories | Client to provide |
| Success story content | /resources/success-stories + homepage spotlight | Client to provide briefs; content can be written once received |
| Certification badges | /company/trust-centre + homepage + /company/about | Add when each certification is confirmed/achieved |
| LinkedIn page URL | Footer + /company/about + /company/contact | Client to provide |

| Item | Location | Action |
| --- | --- | --- |
| API documentation URL | /how-it-works/integrations | Link to documentation portal when live |