Cloudflare Application Security — Solutions Demo Script

Industry: E-Commerce & Online Retail

Prepared by: Jason **Demo Duration:** 20 Minutes **Demo Domain:** public-api.electric-harbor.sxplab.com

> *Pre-brief industry context and trends are in the separate **pre-brief-industry-context.md** document.*

DEMO SCRIPT: 20-Minute Presentation

The following is a structured talk-track script. "SE" is the Solutions Engineer (you). "Prospect" represents the customer panel. Stage directions are in *italics*. Time markers indicate approximate pacing.

⏱ 0:00 – 4:00 — Opening, Network Overview & What We Heard

SE: Thanks for making time today. Before we jump in, I want to apologize that our account executive couldn't join us today — they had an unavoidable conflict. But we'll make every minute count. I know your team is deep in holiday planning, so let's dive right in. I've spent time understanding PeakCart's architecture and the challenges you briefed us on, and I want to walk through how Cloudflare's Application Security platform addresses each one — with a live look at the products.

SE: But before we get into your specific challenges, let me set the stage with what makes this platform different from anything else you'll evaluate.

Advance to "Cloudflare Global Network" slide.

SE: This is the network that everything runs on. 335+ cities worldwide, 449 terabits per second of capacity, and we process roughly 20% of all Internet traffic — which means our threat intelligence is trained on a dataset no one else has.

SE: The critical architecture point: every server in every data center runs every service. There's no separate scrubbing center for DDoS, no dedicated bot detection cluster, no API gateway appliance. When a request lands on the nearest Cloudflare server, that single server handles DDoS mitigation, WAF, bot scoring, API validation, rate limiting — all in one pass. That's what makes the platform composable and that's why there's no added latency.

SE: Cloudflare builds virtually every service in-house, on commodity hardware. That means the products are designed to work together from day one — shared data models, shared rules engine, shared threat intelligence. When you evaluate competitors who've acquired a bot company, bolted on an API gateway, and bought a client-side monitoring tool, you'll feel the seams. Here, there are no seams — it's one codebase, one architecture, running on the same commodity servers everywhere.

SE: Now, with that context, let me make sure we're aligned on the problem. Based on our earlier conversations, these are the four challenges we're here to solve today.

Advance to "What We Heard" slide.

SE: First — AI-powered bot attacks. Your flash sale conversions dropped from 2% to half a percent while traffic tripled. That's a classic bot inflation signature, and with 60% of bot traffic now AI-driven, it's only getting harder to separate real shoppers from automated ones.

SE: Second — API sprawl. Your headless architecture has created a large API surface, and the reality across our customer base is that most organizations have about a third more public-facing endpoints than they realize. Each undocumented endpoint is an unmonitored attack surface.

SE: Third — client-side supply chain risk. Your checkout pages load scripts from dozens of third-party providers, and PCI DSS 4.0 Requirements 6.4.3 and 11.6.1 are now enforceable. The compliance clock is ticking.

SE: And fourth — DDoS during your peak revenue windows. Last summer's flash sale outage cost roughly $200K in four hours. Application-layer attacks are increasingly targeting checkout and payment APIs exactly when downtime hurts the most.

SE: Does that capture it? Anything we're missing or that's shifted in priority since we last spoke?

Pause for acknowledgment. Adjust demo order if prospect signals a different priority.

SE: Great. So here's how we'll spend the rest of our time. I'll walk through each of these challenges and show you — live — how Cloudflare addresses them. Let me start by showing you what actually happens when a customer hits your site.

SE: When a customer visits peakcart.com, the very first thing that happens is DNS. Your domain resolves to Cloudflare's network — not your origin. That means every request, from every user, everywhere in the world, lands on Cloudflare first. At that point, we terminate the HTTPS connection at the edge. We handle your SSL certificates, enforce TLS 1.3, and establish a secure connection back to your origin. So now the request is sitting on our network, decrypted, and we can inspect it.

SE: This is where the security stack kicks in. Every request — before it ever touches your infrastructure — can pass through DDoS mitigation, WAF rules, bot scoring, API schema validation, rate limiting. It's all inline, all at the edge, all in the same data center within 50 milliseconds of the user. Clean traffic gets forwarded to your origin. That's the fundamental architecture — and everything I'm about to show you builds on it.

Navigate to Analytics & Logs > Account Analytics.

SE: Before we dive into the security products, let me give you the 10,000-foot view. This is Account Analytics — aggregate traffic across all your domains in one place. Requests, bandwidth, security events, cache, errors. You can see at a glance how much traffic Cloudflare is handling and what's being mitigated.

SE: On the logging side, Log Explorer is built right in — think of it as a mini SIEM. Query, filter, and correlate security events across all products without leaving the dashboard. If you already have Splunk or Datadog, Logpush sends request metadata there in real-time. Nothing is a black box.

SE: A few more things at the account level worth calling out. Account Security Analytics shows traffic across all your zones — you can spot attack patterns spanning multiple domains, see if someone's probing staging before hitting production. Account WAF lets you create a single rule and deploy it across every zone at once — one rule, propagated in seconds, every domain.

SE: Beyond security, you also have Workers for compute, R2 for storage, and Cloudflare Images for product image optimization at the edge — resizing, WebP/AVIF conversion, quality adjustment, per request, no origin compute. There's also Turnstile — Cloudflare's client-side CAPTCHA replacement. Think of it as our alternative to reCAPTCHA, but privacy-first — no tracking, no third-party data collection. One JavaScript snippet on your login, signup, or checkout pages and it verifies visitors invisibly. Free, and it works alongside Bot Management for layered protection.

SE: And I'll mention — today is application security, but Cloudflare One covers the internal side: VPN replacement, identity-based access, secure web gateway. Same network, same dashboard. Separate conversation, but one vendor for external and internal security.

SE: Let me quickly show you how the account is managed day-to-day.

Navigate to Manage Account > Members.

SE: Role-based access — SOC gets security, devs get zone-level, finance gets billing. No shared credentials.

Navigate to Manage Account > Notifications.

SE: Alerts for DDoS, cert expiry, origin health, usage — with webhooks into Slack, PagerDuty, your on-call system.

Navigate to Manage Account > Configurations > Lists.

SE: Reusable IP, hostname, and ASN lists referenced across all rules, all domains. Update once, every rule updates automatically. Cloudflare also provides Managed Lists — open proxies, botnets, Tor exit nodes — curated by Cloudflare's threat intelligence team and updated automatically. Reference them in your rules the same way you reference your own.

SE: Alright, that's the account level. Now let me click into the domain.

Click on the demo domain from the account home page.

SE: This is the zone view — everything from here on is specific to this domain. Getting traffic onto Cloudflare is straightforward — you either point your nameservers to us or CNAME specific hostnames. Once traffic is flowing through our network, everything I'm about to show you lights up.

Navigate to SSL/TLS.

SE: First thing once traffic arrives — SSL. Cloudflare can issue certificates for you automatically. We order them, provision them, renew them — you don't touch a thing. Or if you already have your own certificates from a preferred CA, you can upload them directly. Either way, you're covered. TLS termination happens at the edge, and we enforce TLS 1.3 by default. Easy.

Performance — Tiered Caching

SE: Now before we get into security, let's talk about performance for a second — because for an e-commerce company, speed is revenue.

Navigate to Caching.

SE: Cloudflare caches your static content at 335+ data centers worldwide. Tiered Cache organizes those into a hierarchy so your origin only gets a handful of requests instead of 335 data centers each asking independently. During a flash sale when millions of shoppers load the same product pages, this is why your origin doesn't fall over. And this is before we even get to DDoS protection.

SE: Let's get into the security products.

⏱ 2:00 – 6:30 — WAF & Bot Management

Security Overview — Your Starting Point

Navigate to Security > Overview.

SE: This is the Security Overview — it's the first thing you'd see every morning. Cloudflare is continuously scanning your zone and surfacing prioritized suggestions based on your actual traffic and configuration. You'll see detected attacks if there are any active, plus risks and misconfigurations — things like managed rules that should be enabled, settings that could be tightened. Let me click into All Suggestions so you can see the full list.

Click the All Suggestions tab. Briefly scroll through the suggestions.

SE: Each suggestion tells you what the risk is and what to do about it. Some are one-click fixes right from this page. This is the posture management layer — it's not just reacting to attacks, it's proactively telling you where your gaps are. Now let me show you what's already running underneath this.

WAF Managed Rules — Account Takeover Protection

Navigate to Security > WAF > Managed rules. Click "Browse Rules" on the Cloudflare Managed Ruleset. Scroll to the bottom to show the total rule count.

SE: Before I get into the bot problem, I want to show you the foundation everything else sits on. Cloudflare's WAF gives you access to managed rulesets you can enable with one click — the Cloudflare Managed Ruleset and the OWASP Core Ruleset. Between the two, they cover the vast majority of application-layer attacks: SQL injection, cross-site scripting, remote code execution. You choose which rulesets to deploy and can tune individual rules as needed. The Cloudflare Managed Ruleset is the one to pay attention to for zero-days — when a new vulnerability drops, Cloudflare's threat research team pushes a rule globally, often within hours, and you're protected before most vendors have even published an advisory. Auto-updating, no change window required.

Navigate to Security > Settings > Detection Tools.

SE: And on the outbound side, Sensitive Data Detection scans your responses for data that should never leave your origin — passwords, API keys, credit card numbers. If a misconfigured endpoint is leaking sensitive data, Cloudflare catches it.

Bot Management & Account Takeover Demo

SE: Now let me show you how the WAF, bot scoring, and credential detection work together. Let's say an attacker takes a credential dump from a third-party breach and runs it against your login API.

Navigate to Security > Analytics > Bot Analysis.

SE: This is our Bot Analysis dashboard. Every request gets a bot score from 1 to 99 — 1 is highly confident it's automated, 99 is almost certainly human. We derive this from multiple engines — machine learning trained on over 60 million requests per second, behavioral analysis, TLS fingerprinting. All invisible to the real shopper. We never use CAPTCHAs.

Navigate to Security > Security rules. Show the creation of a rule.

SE: Let me build a rule live. Bot score under 30 — likely automated — the request is hitting your login API, and the credentials are from a known breach. Managed Challenge. One rule combines bot detection with leaked credential intelligence to catch credential stuffing cold.

Expression: `(cf.bot_management.score lt 30 and http.request.uri.path contains "/api/v1/auth/login" and cf.waf.credential_check.username_and_password_leaked)`

SE: This propagates globally in under 30 seconds. No hardware, no agent, no maintenance window. That's the composability — WAF signals, bot signals, and credential intelligence all available in one rules engine.

Navigate to Security > Bots > AI Crawl Control.

SE: Last thing on bots — AI crawlers. This dashboard shows you exactly which AI crawlers are hitting your site and how often. You can block, allow, or charge per crawl on a crawler-by-crawler basis.

Transition Question

SE: Before I move on — I'm curious, do you have visibility today into how much of your traffic is automated versus human? Or is that part of the blind spot?

Let prospect respond. Use their answer to reinforce the value of bot analytics and the 'before/after' visibility Cloudflare provides.

⏱ 6:30 – 11:00 — API Security

Discovery & Framing

SE: Great. Now, you mentioned your platform runs on a headless architecture with microservices. That means you have APIs powering everything — product catalog, search, checkout, inventory sync, personalization. Let me ask: how many API endpoints does your team track today?

Let prospect answer. The typical answer is some variation of 'we have documentation for most of them' or a specific number.

SE: That's common. Here's the finding that surprised a lot of our retail customers: across Cloudflare's network, we found that organizations have on average 33% more public-facing API endpoints than they knew about. Shadow APIs — from deprecated services, test environments that were never decommissioned, or integrations that a partner team stood up without going through InfoSec. Each one is an unmonitored attack surface.

API Discovery Demo

Navigate to Security > Web assets > Discovery tab. Show API Discovery results.

SE: This is API Shield. The first thing it does is discovery. Using machine learning, we passively analyze your traffic to identify every API endpoint — including ones not in your OpenAPI spec. We surface them here with traffic volume, methods, and authentication status. Right away, you can see which endpoints are undocumented and whether they're accepting unauthenticated requests.

Schema Validation — Positive Security Model

SE: Now here's where it gets really powerful. Once you've mapped your APIs, you upload or we learn your OpenAPI schema, and we enforce it. This is a positive security model — instead of trying to block known-bad patterns like a traditional WAF, we define what good looks like and reject everything else. If an attacker sends a malformed request, hits an undocumented parameter, or tries to inject a payload through a field that should only accept an integer — it's blocked before it reaches your origin.

[LIVE DEMO — Shadow API Discovery on public-api.electric-harbor.sxplab.com]

Switch to your terminal. Hit the undocumented shadow endpoint — show the response comes back wide open:

```powershell
curl.exe -v https://public-api.electric-harbor.sxplab.com/api/v1/admin/users
```

The response shows admin user emails, roles, and last login timestamps — sensitive data from a forgotten legacy endpoint.

SE: Here's where it gets real. This is `/api/v1/admin/users` — a legacy admin endpoint that isn't in PeakCart's documented schema. Look what it returns: admin email addresses, role assignments, last login timestamps. Your security team may not even know this exists. Right now, this data is wide open.

Navigate to Security > Web assets. Create a fallthrough rule: action = Block for any request to an endpoint not in the uploaded schema. Enable it.

SE: Let me fix that right now. I'm creating a fallthrough rule — any request to an endpoint that isn't in your schema gets blocked. One toggle.

Switch back to terminal. Hit the same endpoint again:

```powershell
curl.exe -I https://public-api.electric-harbor.sxplab.com/api/v1/admin/users
```

Show the 403 Forbidden response header.

SE: Blocked. Same endpoint, same request — now rejected because it's not in the schema. Shadow APIs and the data they expose — eliminated in seconds.

Navigate to Security > Analytics (Events view). Filter by Service = Custom rules. Show the blocked request with violation details.

Rate Limiting & Sequence Mitigation

SE: We also apply intelligent rate limiting per endpoint. API Shield can automatically recommend rate limits based on observed session behavior — so your checkout endpoint gets a different threshold than your product search. And with Sequence Mitigation, we can enforce that API calls happen in the expected order: a user should browse, then add to cart, then checkout. If something jumps straight to the payment API without the preceding steps, that's anomalous and we can flag or block it.

Transition

SE: This is the piece that tends to surprise security teams the most — the gap between what they think their API surface looks like versus what it actually is. Let me know if you have questions before I move to client-side security.

⏱ 11:00 – 14:30 — Page Shield & PCI DSS 4.0

Discovery & Framing

SE: This one is probably the most time-sensitive issue on your plate. PCI DSS 4.0 Requirements 6.4.3 and 11.6.1 are now enforceable. In plain terms, that means you need to: inventory all scripts running on your payment pages, justify the business purpose of each one, ensure the integrity of each script, and detect and alert on any unauthorized changes. Your checkout page alone probably loads scripts from 15 or 20 different third-party providers. Any one of them can be compromised to inject a Magecart-style skimmer.

Client-Side Resources Demo

Navigate to Security > Web assets > Client-side resources tab. Show the script monitor dashboard.

SE: This is the Client-side resources view — what was previously called Page Shield. When you enable it, we inject a lightweight Content Security Policy in report-only mode. Your visitors' browsers report back every script, connection, and cookie they encounter. Within hours, you have a complete inventory right here. No agents, no code changes, no impact on page load.

SE: From there, we flag malicious scripts using ML and threat intelligence, alert you if any approved script changes — even a single line — and let you enforce a real CSP header that blocks anything not on your allow list. Inventory, detection, alerting, enforcement — one dashboard.

SE: This is your direct path to PCI 6.4.3 and 11.6.1 compliance. Script inventory, authorization, integrity monitoring, and enforcement — all from a single dashboard. No additional vendor, no JavaScript tag manager to maintain.

Third-Party Risk Angle

SE: One stat that's worth noting: 30% of all data breaches in 2025 were linked to third-party vendors. Page Shield lets you see not just what scripts are running, but what connections those scripts make — where they're sending data. If your analytics provider suddenly starts making connections to an unfamiliar domain, that's visible and alertable.

Pause. This is often where procurement or compliance stakeholders lean in. Let the conversation breathe.

⏱ 14:30 – 16:00 — DDoS & Peak Revenue Protection

Discovery & Framing

SE: Next up — and your CFO and VP of eCommerce care most about this one: what happens when your site goes down during Black Friday? You told us about the outage during your summer flash sale that cost you roughly $200K in the four hours it took to mitigate. Let me explain why that can't happen on Cloudflare.

DDoS Protection Overview

Navigate to Security > DDoS.

SE: Cloudflare's network capacity is 449 Tbps — the largest attacks ever recorded are a fraction of that. We don't scrub traffic by rerouting it to cleaning centers — every data center runs the full mitigation stack. Volumetric attacks are absorbed automatically with zero configuration, unlimited and unmetered — no surge pricing. Application-layer attacks targeting your checkout API are caught by autonomous edge detection. And you get granular rate limiting on any request attribute to protect specific endpoints without blunt IP blocking.

SE: Notice this is on by default — zero rules to write. There are sensitivity tuning options here if you need them, but out of the box, you're protected.

Waiting Room for Controlled Peak Traffic

Navigate to Security > Waiting Room.

SE: One more tool that's unique to Cloudflare for your use case: Waiting Room. During a product drop or flash sale where you know demand will exceed capacity, Waiting Room creates a fair, branded queue that holds users at the edge while dynamically admitting them based on your origin's capacity. You configure which path to protect — like `/checkout` — set your session limits, and customize the queue page with your branding. No crashed checkout, no oversold inventory, and a much better customer experience than a timeout error.

Switch back to the slide deck. Advance to "Firewall for AI" slide.

⏱ 16:00 – 18:00 — Firewall for AI

Discovery & Framing

SE: There's one more thing I want to show you that's directly relevant to your roadmap. Your team mentioned you're rolling out an AI-powered product recommendation chatbot and a natural-language search feature. Those are LLM-powered endpoints — and they introduce a completely different class of risk.

Traditional APIs accept structured data — integers, strings, enums — and we can enforce a schema like I just showed you. But an LLM endpoint accepts free-text prompts. That means an attacker can try prompt injection to make your model behave in unintended ways, users can submit prompts containing PII — credit card numbers, social security numbers — which could end up in your model's logs or training data, and toxic or harmful content can cause your chatbot to generate inappropriate responses in your brand's voice.

This is actually called out in the OWASP Top 10 for LLMs — prompt injection is the number one risk, and sensitive information disclosure is right behind it.

Firewall for AI Capabilities

SE: Cloudflare's Firewall for AI addresses all three. It sits inline — same edge network, same dashboard — and scans every inbound prompt before it reaches your model. It's model-agnostic.

SE: Three capabilities. **PII detection** — catches credit card numbers, SSNs, phone numbers in prompts before your model ever sees them. **Prompt injection scoring** — every prompt gets a 1-to-99 score, same concept as bot scores, so you set a threshold and block attempts to manipulate your chatbot. And **content safety moderation** — built on Llama Guard, classifies prompts across safety categories so your brand stays protected.

Same Platform, Same Rules Engine

SE: The key point here is that this isn't a separate product you need to learn. Firewall for AI uses the exact same WAF custom rules engine, the same Security Analytics, the same logging we've been looking at all day. You write a rule that says "if prompt injection score is above 50, block" and it works the same way as your bot score rules or your schema validation rules. One platform, one dashboard, one policy layer — now extending to AI.

Shadow AI Discovery

SE: And just like API Shield discovers shadow APIs, Firewall for AI can automatically discover and label LLM-powered endpoints in your traffic that your security team may not know about. Maybe a product team spun up a chatbot prototype and exposed it publicly without going through InfoSec. Firewall for AI finds it and gives you visibility.

If the panel asks about availability: "Firewall for AI is currently available in beta for Enterprise customers. Since you're on Enterprise, your account team can enable it immediately."

⏱ 18:00 – 20:00 — Summary & Close

What We Saw Today

Advance to Summary slide.

SE: Let me bring it all together. Here's what we covered today and what Cloudflare can help you do.

SE: We started at the account level — the platform. Workers for compute, R2 for storage, Images for delivery, account-wide security rules, RBAC, alerting with webhooks, Log Explorer as your built-in mini SIEM. One platform that scales across every domain you manage.

SE: We walked through how traffic gets onto Cloudflare — nameservers or CNAME — and how SSL certificates are handled automatically at the edge. Then we showed how Tiered Cache keeps your origin healthy by dramatically reducing redundant requests, especially during peak traffic.

SE: Then we went deep on security. WAF Managed Rules — the Cloudflare Managed Ruleset and OWASP Core Ruleset available to enable — protecting you from zero-days and account takeover, with Sensitive Data Detection watching what goes out. Bot Management stopping scrapers and inventory hoarders with ML scoring, Turnstile as a privacy-first client-side CAPTCHA replacement, and AI Crawl Control giving you per-crawler visibility and monetization. API Shield discovering shadow endpoints and enforcing schema validation as a positive security model. Page Shield delivering continuous client-side script monitoring for PCI DSS 4.0 compliance. Firewall for AI catching PII, prompt injection, and toxic content before your model sees it. And DDoS protection with 449 Tbps of capacity, autonomous edge mitigation, and Waiting Room to keep checkout alive during peak.

SE: All of that — one network, one dashboard, one vendor. No bolting together five point solutions and hoping they share intelligence. The rules engine is composable, the threat intelligence is shared, and the logging feeds one place.

What Cloudflare Can Help You Do

SE: Specifically for PeakCart:

- **Protect your revenue windows** — stop bots from hoarding inventory and crashing flash sales

- **Eliminate your API blind spots** — discover every endpoint, enforce schema, block shadow APIs
- **Get PCI compliant before your next audit** — continuous script monitoring with zero code changes
- **Secure AI before it goes to production** — guardrails on your chatbot while it's still in beta
- **Survive any traffic spike** — DDoS absorbed at the edge, Waiting Room keeps checkout alive
- **Consolidate your security stack** — replace your aging WAF and five separate tools with one platform

Tailored Next Steps

Advance to Next Steps slide.

SE: Here's what I'd recommend for next steps. First, a proof of value. We can get your traffic flowing through Cloudflare in log-only mode within a day — no inline blocking, just visibility. Within 48 hours, you'll see your real bot traffic percentage, a full API endpoint inventory, a complete client-side script inventory, and visibility into your LLM traffic. That data alone is worth the exercise regardless of vendor decision. Second, I'd like to get your PCI auditor on a 30-minute call with our compliance team to walk through how Page Shield maps to Requirements 6.4.3 and 11.6.1 — that one tends to accelerate timelines. Third, let's get Firewall for AI enabled in beta on your zone so your AI team has guardrails before the chatbot goes to production. And fourth, we can model the rate limiting and DDoS configuration for your summer sale peak. Sound like a plan?

Close. Wait for response. If there are questions, reference the appendix below or offer to go deeper on any product area.

APPENDIX

A. Key Cloudflare Statistics for Conversation

- Cloudflare serves approximately 20% of all Internet traffic
- The network identifies and blocks ~234 billion threats per day
- 335+ data centers in 120+ countries, within 50ms of 95% of Internet users
- 449 Tbps total network capacity
- Named a Leader in the Forrester Wave™: WAF Solutions, Q1 2025
- Recognized as a Representative Vendor in the Gartner Market Guide for WAAP

B. Objection Handling Quick Reference

Objection	Response Framework
"We already have a WAF"	"That's great — WAF is table stakes. The question is whether it also gives you bot scoring, API discovery, client-side script monitoring, AI prompt inspection, and DDoS at the edge. If

Objection	Response Framework
	those are separate tools, you're paying a complexity tax in operational overhead, integration gaps, and slower incident response."
"We're worried about migration risk"	"Completely valid. That's why we start in log-only mode. You can run Cloudflare in parallel with your existing stack for as long as you need, compare detection rates side by side, and only cut over when you're confident. We do this every day with enterprise retailers."
"What about false positives?"	"Our ML models are trained on traffic from millions of sites. The bot feedback loop lets you report false positives directly in the dashboard, and we retrain on that data. During POV, we tune rules with your team in real traffic — you'll see the score distributions before anything blocks."
"How does pricing work?"	"Enterprise Application Security is a unified platform license. DDoS is unmetered and unlimited — no surge pricing, ever. Bot Management, API Shield, Page Shield, and Firewall for AI are add-ons priced by volume. I'll have our account team put together a custom proposal based on your traffic profile after the POV."
"Our AI features aren't live yet — is Firewall for AI premature?"	"This is actually the ideal time. You can enable Firewall for AI in log-only mode during your chatbot beta, get visibility into what kinds of prompts users are sending, and have your security policies in place before you go to production. It's much harder to bolt on AI security after launch."

C. Products Demonstrated

Product	Key Capabilities
Bot Management	ML scoring (1-99), behavioral analysis, JS detections, JA3/JA4 fingerprinting, no CAPTCHAs
API Shield	ML-based API discovery, schema validation (positive security model), sequence mitigation, rate limit recommendations, mTLS, JWT validation
Page Shield	Client-side script monitoring, malicious script detection, change alerts, CSP policy enforcement, cookie tracking, PCI DSS 4.0 compliance
Firewall for AI	PII detection (NER-based), prompt injection scoring (1-99), content safety moderation (Llama Guard), shadow AI discovery, model-agnostic, same WAF rules engine
WAF	Cloudflare Managed Ruleset + OWASP Core Ruleset, custom rules, ML-based WAF Attack Score, Exposed Credentials Check, Sensitive Data Detection (outbound), zero-day protection
DDoS Mitigation	L3/4/7 protection, 449 Tbps capacity, autonomous edge detection, unmetered/unlimited, zero-config

Product	Key Capabilities
Rate Limiting	Granular rules on any request attribute, per-endpoint thresholds, API-aware, session-based limiting
Waiting Room	Fair queuing during peak traffic, branded experience, dynamic origin-capacity admission, edge-based
Turnstile	CAPTCHA replacement, invisible challenge, privacy-first, free tier available
AI Crawl Control	AI crawler visibility and control, per-crawler allow/block/charge, robots.txt compliance monitoring, pay-per-crawl (402 Payment Required), metrics and CSV export

D. Demo Pacing Cheat Sheet

Time	Section	Key Action
0:00 – 4:00	Opening, What We Heard & Agenda	AE apology, walk through pain points slide, confirm priorities
4:00 – 8:00	WAF & Bot Management	Managed rules, ATO story, Bot Analysis dashboard, anti-scraping rule
8:00 – 12:00	API Security	API Discovery, schema validation live demo
12:00 – 15:00	Page Shield & PCI 4.0	Script monitor, CSP policy
15:00 – 16:30	Firewall for AI	PII detection, prompt injection scoring, content moderation
16:30 – 18:00	DDoS & Peak Protection	Capacity stats, Waiting Room
18:00 – 20:00	Platform Value & Close	Consolidation story, next steps

E. Pre-Staged Demo Commands

> Use PowerShell 7+ for single-quote JSON wrapping. See the setup guide for PowerShell 5.1 alternatives.

```powershell

```

```
# --- VALID: List products ---
curl.exe https://public-api.electric-harbor.sxplab.com/api/v1/products

# --- VALID: Get single product ---
curl.exe https://public-api.electric-harbor.sxplab.com/api/v1/products/2

# --- VALID: Filter by category ---
curl.exe "https://public-api.electric-harbor.sxplab.com/api/v1/products?category=electronics"

# --- Shadow API: Undocumented admin endpoint (returns real data!) ---
curl.exe -v https://public-api.electric-harbor.sxplab.com/api/v1/admin/users

# --- Shadow API: Exposed config endpoint ---
curl.exe -v https://public-api.electric-harbor.sxplab.com/api/v1/admin/config
```

F. Firewall for AI — Deep Dive Reference

If the panel asks deeper questions about Firewall for AI:

- **How does PII detection work?** Cloudflare passes the prompt through Presidio's NER-based detection model running on Workers AI at the edge. It identifies entities like credit card numbers, SSNs, phone numbers, and email addresses. The output metadata (was PII found, what type) is then available as fields in WAF custom rules for enforcement.
- **How does prompt injection scoring work?** Each prompt is scored 1-99 for injection likelihood, similar to bot scores. Customers set thresholds and actions using the same WAF rules engine. The scoring model is trained broadly across common LLM attack patterns, not per-customer model.
- **How does content moderation work?** Integrated Llama Guard classifies prompts across safety categories including hate, violence, sexual content, criminal planning, and self-harm. Rules can block specific categories or log for review.
- **What about outbound (response) scanning?** Cloudflare can also scan outbound LLM responses for sensitive data like API keys and financial information using Sensitive Data Detection rulesets.
- **Does it work with any model?** Yes — model-agnostic. Works with self-hosted models, Workers AI, OpenAI, Anthropic, Google, or any LLM behind a Cloudflare-proxied endpoint.
- **Is it GA?** Currently in closed beta for Enterprise customers. Your account team can enable it.
- **What WAF fields are available?** Firewall for AI exposes new fields in custom rules and rate limiting rules, including whether PII was found, PII entity type, prompt injection score, and content safety categories. These compose with all existing WAF fields.
- **Can it do topic enforcement?** Yes. Security and application teams can define allowed topics — for example, a financial services chatbot that should only answer finance questions — and block off-topic

prompts at the edge without modifying application code.