SUE | CLOUDFLARE

Security Modernization Checklist

Identify **risks, inefficiencies, and gaps** in your application security in **3 minutes.**

SUE | CLOUDFLARE

Availability & Performance Risks

- ☐ We've experienced unexplained outages or slowdowns over the past 12 months.
- ☐ We suspect attacks (bots, scraping, DDoS), but lack visibility.
- ☐ Traffic spikes impact user experience or revenue.
- ☐ We don't know how much bot traffic we receive.
- ☐ Neither our CDN nor our WAF can scale automatically.

If any of these are checked →
Modernization needed.

Outdated Tools & Hardware

- ☐ We still use hardware WAF appliances.
- ☐ We experience costly 3 - 5 year hardware refresh cycles.
- ☐ We rely on multiple point solutions stitched together.
- ☐ Our tools don't cover API security or bot management.
- ☐ Managing rules and policies is too time-consuming.
- ☐ We lack a unified dashboard for threat monitoring.

More than two boxes checked →
Cloudflare consolidation recommended.

API Exposure & New Attack Surfaces

- ☐ We don't have a complete inventory of our APIs
- ☐ We're unsure which APIs are exposed externally.
- ☐ Our current tools do not provide API-level protection.
- ☐ We worry about credential stuffing, scraping, or abuse.
- ☐ Developers can deploy APIs without automated safeguards

If you checked any →
You have API security gaps.

Bot & AI Threats

- ☐ We cannot distinguish between good bots (e.g., Google) and malicious ones.
- ☐ We suspect AI scrapers are collecting our data.
- ☐ Bots distort metrics, cost us money, or slow our systems.
- ☐ We've seen spikes in non-human traffic.
- ☐ Our current tools lack modern bot mitigation capabilities.

Bots = the fastest-growing attack vector.
Addressing them is urgent.

Operational & Team Constraints

- ☐ Our security team is overloaded and/or reactive.
- ☐ We lack internal expertise in Cloudflare/WAF/API/bot expertise internally.
- ☐ We have no 24/7 operational coverage.
- ☐ We rely on partners who "aren't proactive anymore".
- ☐ We want fewer tools and simpler management.
- ☐ We want predictable OpEx, not CapEx surprises.

If your team checks three or more →
Managed Cloudflare with SUE is the right step.

Business Impact & Readiness

- ☐ Outages directly impact revenue (e-commerce, parking, bookings, ticketing).
- ☐ Website/app is mission-critical to business continuity.
- ☐ We plan to scale digital usage or customer volume.
- ☐ We want a modern, future-proof security posture.
- ☐ Cloudflare's performance and platform advantages fit our strategy.

If this section resonates, you're ready to modernize.

Conclusion section

Your Score:

0–5 checks:	Emerging need, start with the **Security Review**
6–12 checks:	Clear modernization opportunity, **Cloudflare consolidation**
13+ checks:	High urgency, **immediate risk reduction** needed

Request your Cloudflare Security Review

Recommended next step:
→ Request your Cloudflare Security Review

You'll receive:
→ A full threat & traffic baseline
→ Bot & API exposure analysis
→ Outage risk indicators
→ Recommendations tailored to your stack

Transform your security stack from reactive to proactive.
Cloudflare + SUE = Security Modernization Done Right.

→ Request your review today

About SUE

SUE is the Netherland's most experienced cloud native solution provider, supporting technology-driven organizations with their digital transformation since 1997.
With professional & managed services, we help you to:

→ **Migrate:**	We move your **workloads** securely and efficiently to the cloud.
→ **Modernize:**	We transform your **applications** and **infrastructure** to cloud native solutions.
→ **Manage:**	We optimize and protect your **environment** continuously with proactive monitoring and managed services.

As a **certified Cloudflare partner**, we deliver end-to-end support. Whether you need **implementation**, **expert support**, **ongoing maintenance**, or a **fully managed Cloudflare environment**, we tailor our services to fit your needs.