Panasonic Strengthens Bot Protection with SiARA Shield

Extending enterprise edge security with application-layer behavioural analysis and human verification

Panasonic already had enterprise-grade Akamai protection in place to filter malicious and automated traffic at the edge.

But what happens to the traffic that remains after edge-layer filtering?

During a controlled 10-day production pilot, **SiARA Shield by CyberSiARA** was deployed on the authentication layer of **Panasonic's ProCell portal**, a digital platform supporting Panasonic Fuel Cell services and contract partners.

The objective was to provide an additional layer of behavioural analysis and human verification and determine whether sophisticated automated activity remained after upstream security filtering.

The deployment revealed previously unseen automated activity reaching the application layer.

SiARA Shield identified and blocked up to 40% of the traffic remaining after upstream edge filtering as automated or malicious activity.

Over the course of the pilot, malicious request volume was progressively reduced to near-zero levels, while legitimate user activity remained stable and unaffected.

[IMAGE 1 — PANASONIC PROCELL PORTAL]

Use: Panasonic ProCell portal/login screenshot from the existing case study.

Caption:
Panasonic ProCell portal protected during the SiARA Shield production pilot.

At a Glance

Customer: Panasonic
Platform: Panasonic ProCell portal
Use Case: Login and authentication protection
Environment: OAuth-based authentication
Existing Security: Akamai CDN, WAF and edge protection
Solution: SiARA Shield by CyberSiARA
Protection Layer: Application-layer behavioural analysis and human verification

Deployment: Live production pilot
Duration: 10 days

Key Results

UP TO 40%

of traffic remaining after upstream edge filtering was identified and blocked by SiARA Shield as automated or malicious activity

70%+

reduction in automated request volume within the first 24 hours

80–90%

reduction in malicious request volume within the first 2–3 days

NEAR ZERO

malicious requests by the end of the 10-day pilot

NO ADDITIONAL FRICTION

legitimate user activity remained stable throughout the deployment

---

The Challenge

Panasonic's ProCell portal was already protected by established enterprise-grade Akamai security at the edge, providing CDN, Web Application Firewall and bot-mitigation capabilities.

This protection formed an important first line of defence, filtering large-scale automated activity, malicious requests and known threats before they reached the application.

However, Panasonic did not previously have visibility into the extent of sophisticated automated activity that remained after upstream filtering and continued to interact with the authentication application.

This was the challenge SiARA Shield was introduced to investigate.

Once deployed, SiARA Shield began analysing live production interactions at the ProCell portal's OAuth authentication endpoint.

The findings revealed that a significant proportion of the remaining application traffic exhibited characteristics associated with automated or malicious activity, including sophisticated interactions displaying human-like behavioural patterns.

At peak, **up to 40% of the traffic remaining after upstream edge filtering was identified and blocked by SiARA Shield as automated or malicious activity.**

The Security Gap

Modern bot protection is not necessarily a single-layer problem.

Edge security plays an essential role in absorbing large-scale attacks, filtering known threats and preventing significant volumes of malicious traffic from reaching an organisation's applications.

However, increasingly sophisticated bots can imitate characteristics of genuine human interaction.

The Panasonic pilot demonstrated the value of analysing traffic again at the application layer — after upstream security controls have already performed their role.

This provides an additional opportunity to distinguish between legitimate users and sophisticated automated activity at the actual point of interaction.

[IMAGE 2 — LAYERED SECURITY ARCHITECTURE]

Recommended redesigned diagram:

Incoming Traffic
↓
Akamai — Edge Protection
CDN • WAF • Bot Mitigation
↓
Traffic Remaining After Edge Filtering
↓
SiARA Shield — Application Layer
Behavioural Analysis • Human Verification • TSM
↓
Verified Human Interaction

Caption:
SiARA Shield complements existing edge security by analysing interactions that reach the application layer.

The SiARA Shield Approach

CyberSiARA deployed **SiARA Shield** as a complementary application-layer security control on the ProCell authentication endpoint.

SiARA Shield did not replace Panasonic's existing Akamai infrastructure.

Instead, it extended protection beyond the edge by analysing the behaviour of interactions reaching the application.

Adaptive Behavioural Analysis

SiARA Shield analyses interaction behaviour in real time to identify patterns associated with sophisticated automated activity.

Real-Time Session Scoring

Individual sessions are dynamically evaluated, allowing suspicious interactions to be identified as they occur.

Invisible Human Verification

Legitimate users can continue their journey without routinely being interrupted by traditional CAPTCHA-style challenges.

Trans-Saccadic Memory (TSM)

Where additional assurance is required, SiARA Shield can activate CyberSiARA's Trans-Saccadic Memory technology as an additional human-verification mechanism.

Privacy-First Architecture

SiARA Shield uses a cookie-free approach designed to provide behavioural verification while maintaining a seamless experience for legitimate users.

Implementation

SiARA Shield was deployed as a controlled **10-day production pilot from 13–23 April** on a single OAuth authentication endpoint within Panasonic's ProCell portal.

The objective was to:

- Analyse traffic remaining after upstream edge filtering.
- Identify residual automated activity at the application layer.
- Evaluate sophisticated human-like bot behaviour.
- Measure mitigation effectiveness using live production traffic.
- Maintain the existing experience for legitimate users.

The deployment operated alongside Panasonic's existing Akamai protection without requiring the edge-security infrastructure to be replaced.

This created a layered architecture in which different technologies performed complementary security functions at different stages of the traffic journey.

The Results

The deployment provided immediate visibility into automated activity reaching the application layer.

The SiARA Shield dashboard showed that, at peak, **up to 40% of the traffic remaining after upstream edge filtering was being identified and blocked as automated or malicious activity.**

The impact of the deployment became visible quickly.

Within the first 24 hours, automated request volume fell by **more than 70%**.

Within the first 2–3 days, malicious request volume had reduced by approximately **80–90%**.

Residual automated activity continued to decline over the following days until, by the end of the 10-day pilot, **malicious requests had reached near-zero levels.**

Importantly, throughout the same period, legitimate login activity remained stable and consistent.

No additional friction was introduced for genuine users.

[IMAGE 3 — TRAFFIC REDUCTION GRAPH]

Use: Redesign the traffic graph from the existing case study for the website.

The graph should clearly show:

- Legitimate traffic remaining stable.
- Automated/malicious traffic declining.
- 70%+ reduction within the first 24 hours.
- 80–90% reduction within 2–3 days.
- Near-zero malicious requests by the end of the pilot.

Caption:
During the 10-day pilot, malicious request volume declined to near-zero levels while legitimate user activity remained stable.

[OPTIONAL IMAGE 4 — SiARA SHIELD DASHBOARD]

If suitable for public use, include a cropped or anonymised screenshot of the SiARA Shield dashboard from the Panasonic pilot.

Where possible, use a view demonstrating the identification of automated versus legitimate interactions without exposing sensitive customer or security information.

Caption:
SiARA Shield provided application-layer visibility into legitimate and automated interactions during the Panasonic pilot.

A Complementary Layered Security Model

The Panasonic deployment demonstrates how edge security and application-layer human verification can perform different but complementary roles.

Layer 1 — Akamai Edge Protection

Akamai provides enterprise-grade edge protection, including CDN, WAF, traffic filtering and bot mitigation, helping prevent large-scale attacks and known threats from reaching the application.

Layer 2 — SiARA Shield Application Protection

SiARA Shield operates closer to the point of user interaction.

It analyses traffic remaining after upstream filtering, applying behavioural analysis and human verification to identify sophisticated automated activity reaching the application.

The objective is not to replace established edge-security infrastructure.

It is to extend protection from the edge to the point of interaction.

The Outcome

The pilot gave Panasonic **new visibility into residual automated activity reaching the application layer after upstream filtering.**

SiARA Shield identified sophisticated automated interactions within the remaining traffic and provided an additional mechanism for mitigating that activity.

During the 10-day deployment:

- Up to 40% of traffic remaining after upstream edge filtering was identified and blocked as automated or malicious activity at peak.
- Advanced automated interactions displaying human-like behaviour were identified.
- Automated request volume reduced by more than 70% within the first 24 hours.
- Malicious request volume reduced by approximately 80–90% within 2–3 days.
- Malicious requests reached near-zero levels by the end of the pilot.
- Legitimate user activity remained stable.
- No additional friction was introduced for genuine users.

The result was an additional layer of security extending beyond the edge and into the application itself.

Why It Matters

As automated threats become more sophisticated, determining whether an interaction is genuinely human becomes increasingly challenging.

An interaction successfully reaching an application does not necessarily mean there is a genuine person behind it.

The Panasonic pilot demonstrates how **SiARA Shield can complement existing enterprise security infrastructure by extending behavioural analysis and human verification to the application layer.**

This provides organisations with additional visibility into traffic remaining after upstream filtering and an additional layer of defence against sophisticated automated activity.

Ultimately, SiARA Shield is designed to answer one critical question at the point where it matters:

Is there a genuine human behind this interaction?

See What Is Reaching Your Applications

Your existing security infrastructure may already be stopping significant volumes of automated and malicious traffic.

But what happens to the traffic that remains?

SiARA Shield by CyberSiARA adds application-layer behavioural analysis and human verification to your existing security architecture, helping identify sophisticated automated activity while maintaining a seamless experience for legitimate users.

Talk to a CyberSiARA Security Consultant →