CASE STUDY

ULTRARED

From Noise to Proof: How Tempo Validated Real Risk Across Its Expanding Cloud, Web, and AI Infrastructure

TEMPO BEVERAGES

Head Office: Israel
Industry: Food & Beverage
Website: www.tempo.co.il

Results within hours

High-risk AI infrastructure gap closed

Same day remediation from discovery to fix

41 validated findings prioritized and addressed

Background

Tempo Beverages, one of Israel's leading food and beverage companies, operates a broad and growing digital ecosystem, spanning consumer websites, international brand properties, and an expanding portfolio of cloud-hosted services, including AI-powered applications on Microsoft Azure.

But as Tempo accelerated its digital transformation, its external attack surface expanded even faster. New services, brand sites, and AI endpoints were being deployed continuously — far outpacing what traditional, point-in-time assessments could reliably track.

Customer Challenges

As its digital ecosystem evolved, Tempo faced new security challenges across its web properties, cloud services, and AI infrastructure:

Expanding cloud footprint with no visibility

Azure cloud services, APIs, and AI capabilities were creating new internet-facing endpoints faster than traditional security reviews could track, introducing potential blind spots in the attack surface.

AI services introducing novel attack vectors

The introduction of new AI workflow services created a new class of risk: without automated validation, critical vulnerabilities in these services could have remained undetected.

WordPress misconfigurations across brand sites

Multiple WordPress sites had directory listing enabled across dozens of paths, exposing internal file structures, theme libraries, plugin configs, and media uploads externally.

Need for continuous, automated validation

Point-in-time assessments could not keep up with the pace of change. Ongoing monitoring was needed to detect new exposures as cloud infrastructure and web properties changed daily.

The Tempo Approach: Why ULTRA RED

Tempo selected ULTRA RED to gain continuous visibility into its external attack surface through **External Attack Surface Management (EASM)** and to validate real risk across its full digital footprint.

What set ULTRA RED apart was its validation-first approach: not just identifying potential exposures, but proving which ones are exploitable in real-world conditions. Unlike traditional EASM and vulnerability scanners that generate long lists of theoretical CVEs, ULTRA RED delivers verified attack vectors with full proof-of-concept evidence, enabling precise, confident action.

Its agentless, continuous model required no deployment, no agent installation, and no whitelisting, making it immediately effective across all assets, including cloud-hosted AI services that had never been part of any previous assessment scope.

Key Selection Criteria:

Proven, Exploitable Findings Only

ULTRA RED validates every exposure before surfacing it, ensuring Tempo's team focuses only on confirmed, real-world risk, not theoretical vulnerabilities.

Real-World Proof with Actionable Evidence

Each finding includes full proof-of-concept (PoC) evidence, with precise request/response data and actual exploit path that remove ambiguity and enable immediate action.

Immediate Coverage, Zero Deployment

Real-time discovery of internet-facing assets and exposures across cloud, web, and AI — with no deployment, agents, or whitelisting required.

Faster Remediation, Smaller Exposure Window

By eliminating noise and prioritizing only validated findings, Tempo's team resolved issues 2–3× faster and significantly reduced overall exposure.

> **ULTRA RED found a critical vulnerability in our AI infrastructure that we didn't know about. The proof-of-concept evidence made it immediately clear what needed to be fixed — we remediated it the same day. This speed and certainty is exactly what we need."**
>
> *Tempo Security Team*

Implementation & Results

ULTRA RED was deployed across Tempo's full external attack surface: consumer websites, brand domains, Azure cloud APIs, and AI services, with immediate continuous coverage and zero operational overhead.

Continuous Asset Discovery

ULTRA RED continuously discovers all internet-facing assets, including cloud services, WordPress installations, Azure API gateways, and AI endpoints, delivering a live, accurate view of Tempo's full external attack surface.

Validated Risk Prioritisation

Rather than CVE lists, ULTRA RED validated which vulnerabilities were actually exploitable — allowing Tempo's team to focus on the highest-impact findings with confidence.

AI Infrastructure Security

ULTRA RED identified and validated critical security gaps in Tempo's Azure AI services, with proof-of-concept evidence, enabling same-day remediation before any attacker could exploit it.

Web Asset Hardening

Systematic discovery of misconfigurations across customer-facing websites enabled a structured hardening program, significantly reducing unnecessary exposure of internal site information.

How Tempo Discovered and Fixed a Critical Vulnerability in Hours

Shortly after onboarding, ULTRA RED discovered that one of Tempo's cloud-hosted AI workflow services was exposed to the internet with insufficient access controls. ULTRA RED validated the exposure as a critical, fully exploitable vulnerability with a clear technical evidence demonstrating how the risk could be realized. The Tempo team remediated the issue the same day, implementing the necessary controls before any malicious actor could discover it.

> **ULTRA RED didn't just flag a potential issue, it delivered verified proof that our AI service had a critical exposure. That clarity allowed us to prioritize and fix it immediately."**
>
> *Tempo Security Team*

Looking Ahead: Maturing Continuous Security

Tempo continues working with ULTRA RED to address remaining weaknesses and build a mature, continuous security program:

Application and web security hardening:
Establishing consistent hardening standards across public-facing digital properties to reduce unnecessary exposure and attacker reconnaissance.

Communication infrastructure security:
Strengthening email and related communication channels to prevent impersonation, phishing abuse, and brand misuse.

AI and cloud security governance:
Embedding authentication, access control, and exposure checks as standard requirements for new cloud and AI services so risks are identified and addressed on an ongoing basis.

> **Continuous validation has changed how we approach security. Instead of waiting for the next penetration test to discover what changed, we have live visibility into our attack surface and proof that what ULTRA RED surfaces is real risk, not noise."**
>
> ***Tempo Security Team***

About Tempo

Tempo Beverages is one of Israel's leading food and beverage companies, operating consumer brands with a growing digital and cloud infrastructure. Learn more at www.tempo.co.il.

About ULTRA RED

ULTRA RED is a pioneer provider of Continuous Threat Exposure Management (CTEM), built on a validation-first approach. Our platform helps security teams reduce exposure by continuously identifying, validating, and prioritizing gaps across the entire attack surface. Learn more at www.ultrared.ai.