livingsecurity

SOLUTION BRIEF:

Living Security + Cloudflare Integration

Overview: Integrating to Humanize Cybersecurity

Living Security and Cloudflare have partnered to deliver a powerful, data-driven solution for modern enterprises seeking to better manage human cyber risk. This integration combines Cloudflare's leading web and cloud security telemetry with Living Security's Unify Human Risk Management platform to give security teams actionable insights into risky human behavior and provide flexible, targeted interventions that reduce enterprise risk.

Together, Living Security and Cloudflare enable organizations to build on Cloudflare's robust security controls by layering in human-centric risk insights and behavior-based engageme creating a more adaptive and intelligent approach to cybersecurity.

Benefits to Joint Customers

By integrating Cloudflare's security telemetry—including DNS, web proxy, and email access logs—with Unify's people-centric risk models, security teams gain unmatched visibility into user-level activity. This includes enriched metadata such as user identity, access policies, and site categorization, allowing Unify to detect risky behavior (e.g. repeated visits to AI tools, policy-violating domains, high-risk email activity) with full context.

With automation-ready event mappings and identity correlation, teams can take informed action immediately—without relying on time-consuming log analysis or guesswork.

©Living Security. All rights reserved.

Why This Integration Matters

1 **What If You Could See Risk in Real Time?**

Gain identity-linked visibility into user activity across AI tools, shadow IT platforms, gambling sites, and unsanctioned data sharing — all mapped to human risk models automatically.

2 **Human Risk Insight, Not Just Access Logs**

Understand *why* a behavior matters. Whether it's repeated access to GenAI tools, use of unauthorized collaboration platforms, or policy-violating downloads, Unify contextualizes the risk to prioritize the right response.

3 **Smarter Interventions at Scale**

Move beyond binary controls. Trigger nudges, alerts, or automated actions based on observed risk patterns like persistent shadow IT usage or sensitive data uploads to unsanctioned destinations.

4 **Richer Executive Context**

Deliver board-ready insight that connects web and email activity to human behavior trends, demonstrating how security interventions are reducing risk — not just blocking traffic.

Technical Integration: Unifying Cloudflare DNS Logs and Web Proxy Data with Human Risk Intelligence

At the core of the partnership is a technical API and log integration between **Cloudflare Logpush** and the **Living Security Unify platform**. This includes a streamlined log forwarding method through **Cloudflare R2**, which provides S3-compatible access to DNS logs, making it easy for customers to share data securely and efficiently.

Integration Highlights:

DNS log ingestion via Cloudflare R2: Logs are pulled directly from R2 storage using standard AWS S3-compatible API access patterns.

Focused AI website detection: Logs are filtered to target DNS requests categorized as "Artificial Intelligence" (category 184)—enabling insight into GenAI website usage.

Expanded Web + Email Activity Ingestion: Pull from Cloudflare Gateway and Area 1 to ingest browsing history, blocked web categories, and potentially malicious or misdirected email behavior.

Enriched Metadata Extraction: Capture user identity, policy decision, domain category, and request context in every log for better correlation.

AI Access Detection + Email Threats: Surface "Accessed AI Website" events alongside email-based phishing or credential use anomalies to paint a fuller risk picture.

©Living Security. All rights reserved.

Use Case Spotlight: Monitoring and Managing Generative AI Website Access

As enterprises grapple with the security implications of Generative AI (GenAI), monitoring employee access to these tools becomes essential. While GenAI platforms offer tremendous productivity benefits, they also introduce risks—ranging from intellectual property leakage to unauthorized data exposure.

With this integration, **Living Security Unify detects when users access AI-related domains, using Cloudflare's DNS logs and domain categorization engine.** The system flags this activity under a newly introduced "**Accessed AI Website**" event type.

Unify Insight Triggers:

- **Accessed AI Website**
- **Accessed AI Website (5 times in 30 days)**

These behaviors are neutral in impact—not affecting the Human Risk Index (HRI) directly—but are fully available across all Unify features including:

- Correlation with related behaviors and threats
- Insight-driven workflows
- Identity filtering
- Security awareness reporting
- Executive scorecards

Result: Enterprises can now observe patterns of GenAI usage, implement just-in-time guidance, and take action without outright blocking access—striking a balance between innovation and compliance.

About Cloudflare

Cloudflare, Inc. is a global leader in web performance and cybersecurity. Its vast global network spans more than 310 cities in over 120 countries, protecting and accelerating millions of websites, APIs, and applications. Cloudflare's platform provides an integrated suite of security, performance, and reliability solutions—including DDoS mitigation, Zero Trust access, secure web gateways, and threat intelligence.

Enterprises rely on Cloudflare to protect against evolving cyber threats, reduce latency, and simplify network architecture while maintaining secure and compliant user access across distributed workforces. With a mission to help build a better Internet, Cloudflare continues to innovate in edge computing, AI security, and cloud networking.

Learn more at www.cloudflare.com

©Living Security. All rights reserved.

livingsecurity

About Living Security

Living Security is a pioneer in Human Risk Management, helping enterprises measure, manage, and reduce cybersecurity risks stemming from human behavior. Its flagship platform, **Living Security Unify**, delivers a comprehensive solution that analyzes behavioral data, correlates risk signals from across the enterprise ecosystem, and activates real-time security awareness, micro-training, and targeted interventions.

Living Security partners with global enterprises to transform security from a compliance-driven checkbox to a strategic, people-first program. By aligning human behavior with organizational security objectives, Living Security enables proactive risk mitigation, improved operational resilience, and a more engaged workforce.

Learn more at www.livingsecurity.com

©Living Security. All rights reserved.