

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 engagement, creating a more adaptive and intelligent approach to cybersecurity.

Benefits to Joint Customers

By integrating Cloudflare's global security telemetry with Living Security's people-centric risk intelligence, security teams can now **observe and understand AI website access in context**, correlating it with broader behavioral data such as web browsing, policy violations, and data-sharing patterns. This isn't just about catching threats—it's about **identifying trends, reinforcing positive behavior, and focusing effort where it matters most**.

Whether a user visits a GenAI site once or repeatedly, Unify provides actionable insights without overreacting. AI usage is logged, flagged, and layered into broader behavioral risk models—empowering security leaders to take **informed, proportional steps instead of blanket restrictions**.

Why This Integration Matters

- 1 AI Activity + Behavioral Context = Real Risk Insight**
Understand how GenAI fits into your organization's risk landscape. Spot patterns and intervene early.
- 2 Targeted Interventions, Not Just Block/Allow**
Instead of blanket policy enforcement, Unify delivers context-aware engagement (e.g., nudges or guidance) based on actual behavior and organizational standards.
- 3 One Integration, Many Use Cases *Coming Soon***
Beyond GenAI, this partnership opens doors to monitoring risky categories like shadow IT, gambling, or unsanctioned data sharing.
- 4 Enhanced Security Team Efficiency**
Prioritized identity-centric insights allow security operations teams to focus on risky behavior patterns

Integration with workflows and automation for detection, investigation, and education allows teams to spend less time wrangling logs and more time protecting the business.

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.

Cloudflare Gateway domain categories: Expandable visibility into other domain categories across Cloudflare's threat intelligence taxonomy ([see full list](#)).

Web proxy and alert data ingestion: Includes browsing history, blocked attempts, and potential web-based policy violations.

Behavioral correlation: All Cloudflare telemetry is integrated with Unify's behavioral and identity risk models, allowing precise contextual analysis.

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



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