neoncyber

Workforce Cyber Security Platform (WCP)

Real-Time Observability, Detection & Response—Where the Users Meet the Web

As identity-based attacks and data exposure accelerate—fueled by SaaS sprawl, artificial intelligence (AI) misuse, and human error—organizations need more than after-the-fact detection. They need a live, intelligent defense that can **observe, detect, and respond** in the exact moment a user interacts with the digital world.

Neon Cyber delivers all three—natively in the browser. Our Workforce Cybersecurity Platform uniquely combines Real-time observability with flexible detection and precision response, providing full coverage across workforce interactions, not just infrastructure.

With Neon, organizations can:

- Instantly detect and block unknown identity compromise attempts
- Monitor browser activity providing immediate visibility to protect the workforce
- Warn or stop users from accessing suspicious or malicious websites in real time
- Customize or deploy prebuilt detection rules across any webpage, for any user activity
- Monitor and flag sensitive data being shared with third parties, without breaking workflows
- Leverage behavioral analytics for cyber security to flag or stop risky behaviors as they happen–or stop them in flight

These capabilities address today's most critical security gaps. In 2024, identity-related threats—including compromised credentials, business email compromise (BEC), and reused passwords—were the top cause of breaches. At the same time, users are increasingly leaking data through AI prompts, SaaS forms, and login portals—often unintentionally, but with serious consequences.

neoncyber

Browser Detection and Response (BDR) and Identity Threat Detection and Response fail because they rely on pattern matching and lagging telemetry. Neon takes a radically different approach—almost like a security expert sitting with users as they engage with forms, download/upload files, and input data. **We operate live in the browser. This proactive proximity enables detection at the point of risk, not long after.**

Use Case

In one real-world incident, a Neon design partner saw a marketing user access a generative AI tool outside of SSO controls. The user entered secret product codenames into the AI prompt—while reusing a previously breached password. Attackers, running credential stuffing campaigns, successfully accessed several sites, including the one where sensitive company content was being generated. Neon would have detected this behavior live—flagging both the AI usage and the credential risk, and capturing a forensic timeline for response.

From keyword-level input tracking to identity-based anomaly detection, Neon gives security teams discreet but powerful control over how users access, authenticate, and interact with data across the internet with support for user risk analytics to help prioritize threats and guide response.

This is modern observability, detection and response—built for the realities of the modern workforce.

Neon Cyber: Closing the Gap in Workforce Cybersecurity

By addressing the rising threats tied to identity misuse, SaaS sprawl, and browser-based phishing, Neon Cyber's **Workforce Cybersecurity Platform** gives security teams something they've never had before: **real-time protection they control that travels with the user**—and automatically acts before risk becomes an incident.

Visit neoncyber.com for more information or to connect for a demo.

neoncyber