CYBERLENCE

FOR CISOs, CIOs & RISK LEADERS

Incident Hits. Can You Answer in Minutes, Not Months?

Cyberlence turns fragmented security and infrastructure signals into application-aware incident intelligence, so teams can quickly detect multi-vector incidents, understand the business impact, and recover services predictably. Without it, breaches take 247 days to contain, cost $4.99M on average, and fewer than 1 in 20 organizations fully recover within 50 days.[1]

THE PRESSURE YOU'RE UNDER

Alerts Don't Answer the Questions That Matter

Detection: signals fragmented across 83 tools from 29 vendors hide real incidents in the noise. **Impact Analysis & BIA:** nobody can say which business service is at risk or how far it's spreading. **Adaptive Response, Remediation & Recovery:** broad containment can take down the very apps you're protecting.[2]

CYBERLENCE SOLUTION

Application-Aware Incident Intelligence

Detection: an intent-based policy engine that reasons about intent, not signatures. **Impact Analysis & BIA:** live blast-radius and business impact as the incident unfolds. **Adaptive Response, Remediation & Recovery:** adaptive, role-based workflows that scope containment to what's actually affected, keep the evidence trail intact, and recover the full application — not just the data.

MINUTES TO INSIGHT, NOT WEEKS

Correlate signals across 80+ tools against a live application blueprint — catching multi-vector and zero-day attacks static rules miss, in minutes.

IMPACT YOU CAN DEFEND

Trace attack-path origin and live blast radius to quantified business and regulatory impact — not a snapshot from last quarter's BIA.

WHAT CHANGES

What Your Team Gets

Detection: Intent-based detection flags attacker intent, not just signatures — catching multi-vector and zero-day activity before it spreads.

Impact Analysis & BIA: Live blast-radius and business-impact analysis replace war rooms and guesswork with a defensible, real-time answer.

Adaptive Response, Remediation & Recovery: Adaptive application recovery restores the full running service — not just the data — while containment stays scoped to what's actually affected, with every step logged against the RTO your business set.

Request a briefing mapped to your own applications — info@cyberlence.com

Sources: [1] IBM, Cost of a Data Breach Report 2026. [2] IBM & Palo Alto Networks, Capturing the Cybersecurity Dividend, Jan 2025.
© 2026 Cyberlence. All rights reserved.