CyberSagacity

CASE STUDY

Hyperscale Cloud Infrastructure Provider

Supply chain & third-party software governance.

“Third-party software risk is often completely unmanaged and unmeasured until an outage or exploitation occurs.”

FORMAT	ROLE	PRODUCT
Case Study	Head of Vendor Risk · CPO	CyberSagacity Platform

CYBERSAGACITY.COM

ABOUT THE CUSTOMER · THE CHALLENGE

Only as strong as your weakest vendor.

INDUSTRY	Hyperscale Cloud Infrastructure Provider
RISK DOMAIN	Critical infrastructure dependent on external third-party software providers
GOVERNANCE MODEL	Contractual and compliance-driven procurement frameworks
CORE PAIN POINTS	Unmanaged third-party code · no contractual security enforcement · operational downtime risk

Security is only as strong as the weakest vendor in the software supply chain. A premier hyperscale provider needed to manage systemic risk from a vast network of third-party providers — **but because third-party code is historically opaque, it had no way to measure vendor exposure or hold vendors accountable.**

PRODUCT IN ACTION · HOW RESULTS WERE ACCOMPLISHED

From opaque vendor code to enforceable accountability.

01

Structured AppSec risk modeling

Defined a customized, structured AppSec risk model specifically for third-party software.

02

Operational risk linking

Mathematically linked code-level vulnerabilities to operational risk and downstream infrastructure downtime.

03

Contractual enforcement

Translated risk into concrete, measurable AppSec requirements embedded in governance agreements and contracts.

04

Continuous vendor governance

Established continuous enforcement — moving from blind trust to automated verification of vendor obligations.

From blind trust to automated verification of every vendor obligation.

BUSINESS VALUE & IMPACT METRICS

85% less risk across the third-party ecosystem.

CyberSagacity replaced check-the-box vendor assessments with defensible, data-backed risk governance — and made security accountability contractually enforceable.

85%

Reduction in effective risk exposure

Across the entire third-party software ecosystem.

Binding

Contractual security accountability

Verifiable AppSec obligations embedded directly in vendor governance agreements.

Continuous

Defensible risk governance

Automated verification replaces arbitrary check-the-box assessments.

Learn more at www.cybersagacity.com →