ACIUM

Are You Leaving Your Browser Unprotected?

Identify Hidden Gaps in Your Browser Security

Modern work happens in the browser, but most businesses don't treat it like part of their security perimeter. Use this checklist to find out if your organization has a browser blind spot—and how to close it fast.

Visibility

□ We know what extensions our employees are using in their browsers

□ We can see which SaaS apps are being accessed (and by whom)

□ We have visibility into browser-based file uploads, downloads, or copy-paste behavior

Control

□ We can block or restrict high-risk browser extensions

□ We can prevent logins to unsanctioned apps or personal accounts

□ We can enforce browser-level DLP policies (e.g., block copy/paste of sensitive data)

Policy

□ We apply consistent browser policies across all devices (including BYOD)

□ We require secure login (SSO/MFA) for all browser-accessed apps

□ We've educated employees about browser security risks

Protection

□ We have threat detection for browser-based phishing or malware

□ We use real-time risk scoring for SaaS activity and browser sessions

□ We can respond quickly to suspicious browser activity (alerts, logs, or automated actions)

If you checked fewer than 8 boxes, it's time to take browser security seriously. Acium's Unified Browser Security™ platform can help.

Schedule a risk consult today!

sales@acium.io | +1 (844) GO-ACIUM | Acium.io