CIS Browser Benchmarking: Enforce Secure Browser Configurations at Scale with LayerX

Web browsers are now the primary workspace for AI, SaaS, and enterprise work, and CIS Browser Security Benchmarks help enterprises secure this critical risk surface and make sure their sensitive data stays secure.

Browsers routinely handle sensitive data, identities, and business logic. Misconfigurations in browser settings, such as extension policies, authentication, password storage, and remote access controls, can introduce hidden risks and create blind spots that traditional endpoint and network tools can't see or enforce.

Without continuous enforcement, organizations face:

Inconsistent browser configurations across users and devices

Increased exposure to extension-based threats and account compromise

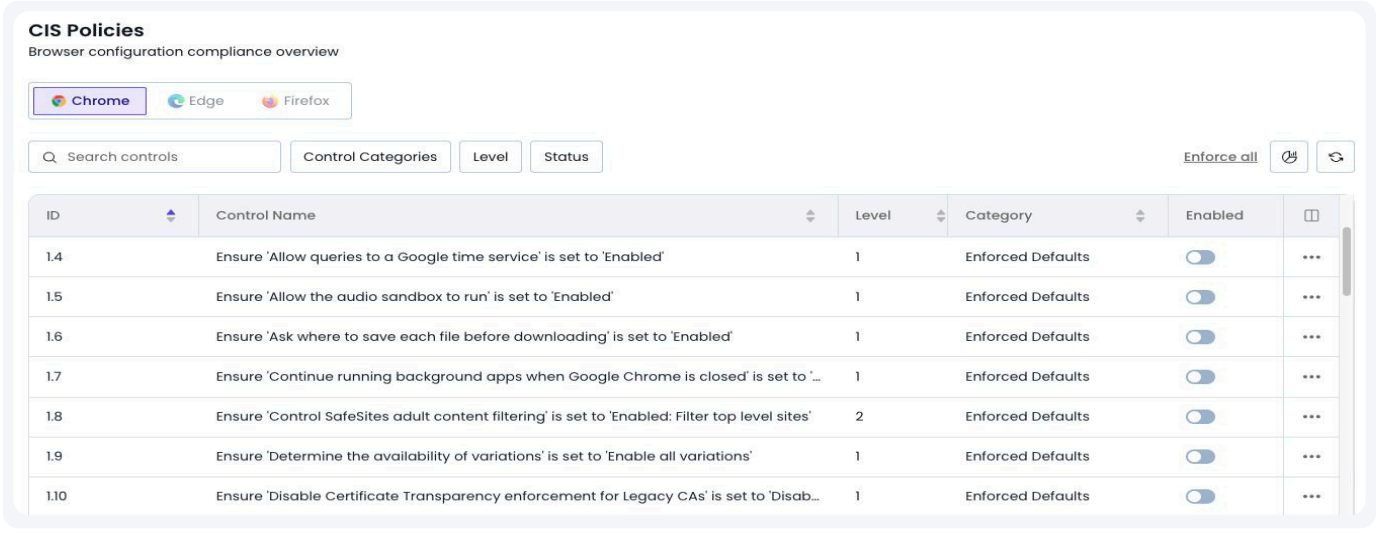
Weak controls over data handling, authentication, and access

Compliance gaps with security frameworks and audit requirements

CIS browser benchmarking ensures every browser operates in a hardened, compliant state.

LayerX CIS Benchmarking for Browsers

LayerX brings CIS benchmarking directly into the browser layer, enabling organizations to continuously assess, enforce, and manage secure browser configurations without disrupting users.



Key Capabilities

Comprehensive Coverage Across All Major Browsers

LayerX enforces CIS benchmark controls across Chrome, Edge, and Firefox, ensuring a consistent security posture regardless of users' choice of browser.

Pre-Mapped CIS Controls for Immediate Value

All relevant CIS browser controls are pre-mapped and categorized, eliminating manual effort and enabling rapid adoption of best practices.

One-Click Enforcement at Scale

Quickly enforce individual controls or apply policies globally with bulk enforcement capabilities, reducing operational overhead.

Real-Time Visibility into Configuration Compliance

Continuously monitor which controls are enabled, misconfigured, or non-compliant without relying on periodic audits.

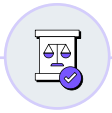
Why It Matters

LayerX transforms CIS benchmarks from static documentation into live, enforceable browser policies, ensuring that every user session adheres to secure configuration standards.

This results in:

Reduced Attack Surface From Misconfigured Browser Settings

Stronger Control Over Extensions, Authentication, And Data Flows



Continuous Compliance Without Manual Audits

No User Disruption, As Policies Are Enforced Seamlessly Within The Browser

About LayerX

LayerX secures all user and agentic interactions in both AI and non-AI applications, across traditional and AI browsers, IDEs, and desktop apps. It is the only AI usage control & Browser Security platform that lets customers control every prompt and data exchange across any channel, without changing their network architecture or disrupting the user experience. Enterprises rely on LayerX's interaction security to secure their hybrid workforce in an AI-first world. For more information, visit https://layerxsecurity.com.