Browser Security Platform

ATAKAMA

CIS Control Mapping

In today's cybersecurity landscape, aligning your tech stack with industry-standard frameworks is essential. Atakama acknowledges the importance of adhering to CIS controls, providing a comprehensive suite of features mapped to this framework. This empowers MSPs to strengthen their clients' defenses against cyber threats while ensuring compliance with established security practices. The following offers a summary of Atakama's key features and their correspondence to CIS security controls, delivering unparalleled browser protection and visibility.

✓ CIS Control	✓ Atakama Feature
2 Inventory and Control of Software Assets 2.5	**Data Leakage Control | Browser Security Control** • Block uploads and downloads based on website and user-login identity • Block uploads and downloads based on file type
3 Data Protection 3.3	**Data Leakage Control** • On-screen data masking • Web page watermark • Re-direct downloads to secure folder based on file type and contents • Clipboard control - restrict pasting content into non-corporate apps
8 Audit Log Management 8.2, 8.5, 8.6, 8.7	**Insights & Monitoring** • Web app usage and by category • Upload and download statistics • Phishing and malware blocking • Website performance and risk statistics
9 Email & Web Browser Protections 9.1, 9.2, 9.3, 9.4	**DNS & Web Content Filtering | Browser Security Controls** • Native browser security settings enforcement • Category-based content filtering for compliance • Anti-phishing and anti-malware website blocking • Secure browser enforcement • Browser update enforcement
10 Malware Defenses 10.1, 10.2	**DNS & Web Content Filtering | Browser Security Controls** • Anti-phishing and anti-malware website blocking • On-device malware command and control blocking

✉ info@atakama.com   🌐 www.atakama.com