



CIS Control Mapping

CONTROL 02 Inventory and Control of Software Assets

Mapping: 2.5

Data Leakage Control Browser Security Control

- Site identity: visibility around business apps
- Block uploads based on app or file type
- Block downloads based on app or file type

CONTROL 03 Data Protection

Mapping: 3.3, 3.13

Data Leakage Control Insights and Monitoring

- On screen masking of sensitive data
- Restrict source paths for uploads
- Force save path of downloads based on file type
- In browser copy/paste control
- Copy/paste control between browser and non-browser apps
- Save-as control
- In-browser data leakage statistics
- Upload statistics
- Web page watermarking

CONTROL 08 Audit Log Management

Mapping: 8.2, 8.5, 8.6, 8.7

Insights and Monitoring

- Top web apps and usage by category
- Phishing and malware statistics
- Download statistics
- Browser activity monitoring
- Web app usage statistics

CONTROL 09 Email and Web Browser Protections

Mapping: 9.1, 9.2, 9.3, 9.4,

Browser Security Control DNS & Web Content Filtering

- Browser native anti-phishing and anti-malware
- Anti-phishing, anti-malware URL filtering
- Browser extension management
- Category-based content filtering
- Enforce browser updates
- Control native browser security settings

CONTROL 10 Malware Defenses

Mapping: 10.1, 10.2

DNS & Web Content Filtering

- Anti-phishing, anti-malware URL filtering

CONTROL 14 Security Awareness & Skills Training

Mapping: 14.2

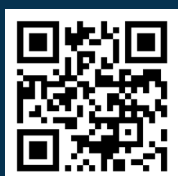
DNS & Web Content Filtering

- Anti-phishing, anti-malware URL filtering with end-user notifications

Find out how the **Atakama Managed Browser Security Platform** can support your security and compliance needs.

Implementation Group Mapping

CONTROL 02 Inventory and Control of Software Assets IG2 2.5 Allowlist Authorized Software Atakama Feature Data Leakage Control Native Browser Settings Control	CONTROL 03 Data Protection IG1 3.3 Configure Data Access Controls list Atakama Feature Data Leakage Control Insights and Monitoring	CONTROL 03 Data Protection IG3 3.13 Deploy a Data Loss Prevention Solution Atakama Feature Data Leakage Control Insights and Monitoring
CONTROL 08 Audit Log Management IG1 8.2 Collect Audit Logs Atakama Feature Insights and Monitoring	CONTROL 08 Audit Log Management IG2 8.5 Collect Detailed Audit Logs 8.6 Collect Query Audit Logs 8.7 Collect Request Audit Logs Atakama Feature Insights and Monitoring	CONTROL 09 Email and Web Browser Protections IG1 9.1 Ensure Use of Only fully Supported Browsers and Email Clients 9.2 Use DNS Filtering Solutions Atakama Feature Native Browser Settings Control DNS and Web Content Filtering
CONTROL 09 Email and Web Browser Protections IG2 9.3 Maintain and Enforce Network-Based URL Filters 9.4 Restrict Unnecessary or Unauthorized Browser and Email Client Extensions Atakama Feature Native Browser Settings Control DNS and Web Content Filtering	CONTROL 10 Malware Defenses IG1 10.1 Deploy and Maintain Anti-Malware software 10.2 Configure Automatic Anti-Malware Software Atakama Feature DNS and Web Content Filtering	CONTROL 14 Security Awareness & Skills Training IG1 14.2 Train Workforce Members to Recognize Social Engineering Attacks Atakama Feature DNS and Web Content Filtering



**Schedule
your demo
today.**