## Risk Assessment Table

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Description** | **Impact** | **Risk Level** | **Proposed Mitigation** |
| Overprivileged access for third-party vendors | Critical | High | Implement RBAC, MFA, and isolate vendor access using Cloudflare Zero Trust. |
| Credential compromise through shared or weak vendor accounts | High | High | Enforce strong authentication policies, use unique credentials, and implement Cloudflare’s access control measures. |
| Data leakage via employee use of shadow IT tools (e.g., Google Drive) | High | High | Block unauthorized DNS requests, deploy SSO with approved apps, and train staff on tool usage. |
| Malware introduction from unvetted apps (shadow IT) | High | Medium-High | Use DNS-layer blocking with Cloudflare Gateway and enforce app whitelisting through SSO portal. |
| Productivity loss due to unsanctioned and fragmented app usage | Medium | Medium | Provide centralized tool access via SSO and ensure team training on approved apps. |
| Endpoint device theft without full-disk encryption | Critical | High | Enforce endpoint encryption through MDM and WARP agent checks |
| Insider threat via undetected data exfiltration | Critical | High | Deploy device posture monitoring, logging, and anomaly detection using Zero Trust endpoint solutions. |
| Delayed or inconsistent detection of insider misuse of company data | High | Medium-High | Deploy advanced Endpoint Detection and Response (EDR) tools and improve behavioral analytics. |