



Service description document: Prisma Browser

Introduction to eir Business

eir Business is a leading provider of advanced network, cloud, and IT managed services, supporting public and private sector organisations across the UK and Ireland for almost 30 years. We design, implement, and manage next-generation solutions that strengthen resilience, enhance security, and enable organisations to work seamlessly and securely from anywhere.

Every engagement starts with listening, understanding your environment, your priorities, and the outcomes you need to achieve. From there, we shape solutions that deliver genuine value, long-term performance, and measurable operational impact.

As a trusted managed service provider, we bring together specialist engineering, proactive service management, and a 24x7 operations capability. Our tightly integrated teams work across the full IT and network landscape, including cloud, cybersecurity, WAN/LAN, connectivity, digital workplace, AI and automation, data centre services, and unified communications.

Our managed services are built on industry best practice and underpinned by ITIL principles, ensuring consistency, accountability, and continual improvement. We combine rigorous processes with real human engagement: our service managers, engineers, and analysts work side-by-side with customers to anticipate needs, resolve issues quickly, and identify opportunities for ongoing optimisation.

Service Introduction

Prisma Access Browser is a secure enterprise browser designed to protect users on both managed and unmanaged devices. It delivers security controls directly within the browsing session to enable safe access to web, SaaS and private applications, including for BYOD and contractor use cases. The service integrates with SASE capabilities to enforce zero trust access, apply threat prevention, and reduce data loss risk during browser-based work. Prisma Access Browser helps organisations modernise user access without relying on traditional VDI approaches, while maintaining consistent policy enforcement and visibility.

Key Service Features

Last-mile Data Loss Prevention

Applies data controls inside the browser session to reduce the risk of copy, paste, download, print and upload data leakage.

Zero Trust Network Access (ZTNA) 2.0

Enables identity and context-aware access to private applications without exposing the network.

Advanced Threat Prevention

Prevents web-borne threats through inspection, threat intelligence and malware prevention applied within browsing activity.

Identity-based Policy Enforcement

Integrates with enterprise identity providers to apply policy by user, group and authentication context.

GenAI Security and Redaction

Supports safer use of public generative AI by applying policy controls and content handling to reduce sensitive data exposure.

Secure Enclave for BYOD

Creates a protected browsing environment on unmanaged devices without requiring full device control.

Phishing and URL Filtering

Reduces exposure to malicious sites, credential harvesting, and risky browsing destinations.

Session Recording and Forensics

Supports auditing and investigation through session visibility and security event records.

Just-in-time Multi-Factor Authentication

Enables step-up authentication based on risk, application sensitivity, or user context.

Application Acceleration

Optimises access pathways to improve performance when accessing business applications through the browser.

Key Service Benefits**Cost reduction and VDI replacement**

Supports browser-based secure access patterns that reduce reliance on traditional VDI for many user groups.

Secure BYOD and contractor access

Enables controlled access for third parties and unmanaged endpoints without weakening security posture.

Seamless user experience

Delivers security controls within the browsing environment while maintaining a familiar user workflow.

Last-mile data control

Reduces data leakage risk at the point of interaction where browser activity occurs.

Rapid M&A onboarding

Supports faster onboarding of new users and environments with central policy enforcement.

Instant threat prevention

Protects users during browsing sessions and reduces exposure to web-borne threats.

Simplified zero trust access

Centralises identity-aware policy and access patterns for web, SaaS and private applications.

Enhanced privacy for users

Supports secure browsing patterns that reduce unmanaged device risk while limiting unnecessary data exposure.

Safe use of public GenAI

Provides practical controls for enabling AI tools while protecting sensitive information.

Unified SASE strategy

Supports a consistent access and security approach alongside wider SASE architecture.

Service Scope*Included*

- Secure enterprise browser capability for accessing web, SaaS and private applications
- Policy configuration and management through a central management interface
- Identity integration for user and group-based controls (for example, Okta or Azure AD)
- Browser-based security controls including threat prevention and data control features (as licensed)
- Security monitoring and reporting for operational visibility
- Support and service assistance in line with the selected support level

Optional Add-ons

- Enhanced onboarding and implementation support through professional services
- Technical account management (where required)
- Additional security features or integrations dependent on the selected licence tier
- Integration support for operational tooling and reporting workflows

Not Included

- Internet connectivity or underlying network services
- End-user device provisioning or hardware supply
- Third-party identity platform licensing
- Customer internal operational processes, user training delivery, or change management (unless purchased as professional services)

Onboarding

eir Business supports onboarding using a structured approach appropriate to the customer's scale and security needs. This typically includes initial discovery to confirm objectives and target applications, configuration of core security and access policies, identity integration, testing and validation, and controlled rollout to user groups. Customers can use documentation and guided setup resources, and can also engage professional services for assisted deployment, training sessions, and rollout planning.

Support

Support is available via email or online ticketing, with optional phone and web chat support depending on the selected support model. Response times align to severity-based handling and may differ by support tier.

Indicative response targets supplied for this service are:

- **Platinum:** S1 <15 minutes, S2 <30 minutes, S3 <2 hours, S4 <4 hours
- **Premium:** S1 <1 hour, S2 <2 hours, S3 <4 hours, S4 <8 hours
- **Standard:** Monday to Friday 7am to 6pm (UK time), aligned to Premium response targets within support hours

Third parties engaged by the buyer can be granted access to support features where required by the buyer's operating model.

Dependencies

- A supported device and operating system for end users
- Internet connectivity for access to cloud-delivered service components
- An identity provider integration where identity-based controls are required (for example, Okta or Azure AD)
- Customer-side decisions on policy configuration, user groups, and application access requirements

Service Constraints

- Service performance and end-user experience depend on available internet connectivity and local conditions
- Some capabilities may vary between desktop and mobile experiences due to platform differences (for example, posture, tunnel mode, pre-login behaviour and user experience)
- Planned maintenance windows may apply, with notifications provided through standard channels
- Feature availability may depend on licence tier and enabled modules

Pricing

Prisma Access Browser is provided on a subscription basis. Pricing depends on the required features, user volumes and term. Optional professional services and enhanced support options can be provided at additional cost. Buyers should refer to the applicable G-Cloud pricing document for full commercial details.

Exit and Offboarding

At the end of the contract term, service access is ceased or transitioned in line with renewal or replacement plans. Customers can export relevant service data such as logs, reports and usage information through the management interface, with common export formats available (including CSV and JSON, and report outputs such as PDF where applicable). Where required, eir

Business can support transition activities and data retrieval as a professional service engagement.

