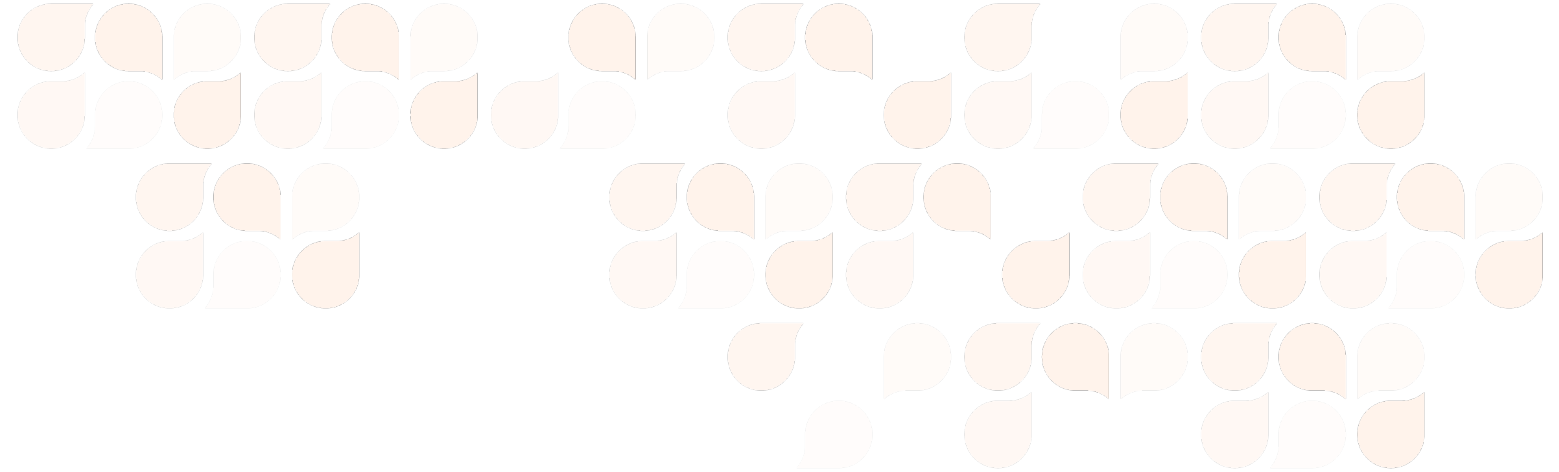




# Puzzel Conversational Intelligence

G-Cloud 15 Service Description

|                        |                     |
|------------------------|---------------------|
| <b>Version</b>         | <b>1.0</b>          |
| <b>Date of version</b> | <b>January 2026</b> |

## Table of Contents

|                                                      |           |
|------------------------------------------------------|-----------|
| Service Description.....                             | 3         |
| Key Features of Virtual Agent.....                   | 3         |
| Integrations.....                                    | 4         |
| Support .....                                        | 4         |
| <b>Help Site</b> .....                               | <b>4</b>  |
| <b>Incident Management</b> .....                     | <b>5</b>  |
| Additional Service Details .....                     | 6         |
| <b>Data Backup, Restore, Disaster Recovery</b> ..... | <b>6</b>  |
| Technical and Organisational Measures .....          | 6         |
| Systems.....                                         | 13        |
| Infrastructure and Resilience .....                  | 13        |
| <b>Onboarding Support</b> .....                      | <b>14</b> |
| Delivery Staff.....                                  | 15        |
| Training and Adoption .....                          | 15        |
| <b>Offboarding Support incl access to data</b> ..... | <b>15</b> |
| <b>Service Constraints</b> .....                     | <b>15</b> |
| <b>Service Levels</b> .....                          | <b>15</b> |
| <b>Technical Requirements</b> .....                  | <b>15</b> |

# Service Description

## Conversational Intelligence

Puzzel Conversational Intelligence is a cloud-hosted analytics and quality platform for recorded customer interactions and written channels. It provides Quality Assurance, insight generation, reporting and automation of manual post-contact tasks such as wrap-up and disposition, in a user-friendly web application designed for agents, team leaders, QA coaches and administrators.

### How does Conversational Intelligence transform service operations?

- Quality Assurance and coaching – Evaluate conversations consistently using configurable scorecards and coaching workflows.
- Insights and reporting – Analyse trends across topics, sentiment and outcomes to drive operational improvements.
- Automation – Reduce manual after-call work with automatic summaries, topics and dispositions.
- Transparency by design – Drill from high-level insights down to the individual conversation with clear rationale for scores and categorizations.

## Key Features of Virtual Agent

### AI-powered transcription and analysis

Proprietary ASR for Nordic languages with support for additional languages via best-in-class models. Analyse what was said (not voice biometrics) to derive sentiment, topics and compliance signals.

### Generative AI (summaries and assistance)

On-demand, configurable summaries using Azure OpenAI under EU data boundary with no training on customer data and time-limited retention.

### QA and Coaching

Configurable scorecards, randomized/manual sampling, self-evaluations, coaching notes and goals, with dashboards for progression.

### Trackers and Segments

Create keyword/phrase-based trackers and audience segments to monitor initiatives and surface emerging themes.

### Library of audio clips

Maintain curated clips for learning; governed by retention rules and redaction to minimise personal data exposure.

### Role-based access

Owner, Administrator, Team Leader and User roles with least-privilege defaults; audit logging across critical actions.

NOTE: Hosting and data residency are EU-only (Denmark and Germany), with Azure OpenAI used within the EU boundary and strict no-training commitments. Default retention settings support GDPR-compliant deletion policies and can be adjusted per customer policy.

## Integrations

Conversational Intelligence integrates with recording and email/ticket systems for ingestion via API or SFTP and exposes REST APIs and webhooks for data export. Puzzel CallID/SessionID enable linkage to external CX metrics. All integrations are scoped during onboarding and limited to those documented by Puzzel.

- Recording ingestion via provider API or secure SFTP
- Open REST API and webhooks for export (JSON, text for transcripts)
- Linkage using Puzzel CallID/SessionID to external BI/VoC systems

## Support

Basic support is given to all Puzzel customers through written requests only. Customers can chat with our support engineers via web chat or by raising a ticket through [help.puzzel.com](https://help.puzzel.com) and clicking on the Support tab on the right. Support is only available during business hours.

Customers can request further support however by subscribing to paid for packages. Please see our pricing file for details.

## Help Site

We will provide all customers access to our online help portal where you can view constantly updated useful information regarding your chosen products and features. This includes:

- Knowledgebase and Documentation of your software
- Maintenance Schedule
- Software Status and Incident Notifications
- Release Notes
- Announcements
- Ability to Raise Tickets
- Support Webchat

## Incident Management

When your issue is harder to solve, the Help portal is the centralised point where you can create incident tickets.

When your issue requires our support team, once triaged, we give you direct access to our technically proficient, in-region support engineers for rapid resolution of your ticket.

Tickets are triaged and assigned a P1 to P5 rating based upon the following matrix which measures Impact of incident versus the required Urgency.

| Impact / Urgency | High         | Medium      | Low         |
|------------------|--------------|-------------|-------------|
| High             | P1 – Highest | P2 – High   | P3 – Normal |
| Medium           | P2 – High    | P3 – Normal | P4 – Low    |
| Low              | P3 – Normal  | P4 – Low    | P5 – Lowest |

Puzzel's committed initial response times to you are based upon the assigned incident rating;

- P5 – Respond within 8 business hours
- P4 – Respond within 4 business hours
- P3 – Respond within 2 business hours
- P1 or P2 – Respond within 1 hour

For our customers, your ability to self-support and take ownership of the software is matched with a responsive, technical support team based in-region and able to support you quickly and efficiently by connecting you with a proficient support engineer immediately.

Our full Service Level Agreement can be reviewed via [this Help Page](#).

## Additional Service Details

### Data Backup, Restore, Disaster Recovery

The Puzzel Cloud Services are built on secure best of breed components. All services are produced and delivered from Data Centres fully managed and operated by Puzzel. Data processing takes place in Europe (UK and EU/EEA) and follows all regulations and requirements regarding data protection and data privacy.

- Only well recognized co-location partners are used.
- All Puzzel infrastructure is isolated in separate rooms or cages with access only for personnel controlled by Puzzel.
- All Data Centres are locked and alarmed with 24/7/365 surveillance.
- External and internal video monitoring and traceability of access to the premises.
- Redundant climate control with environmental monitoring of gas, moisture, heat and water.
- Fire alarm with automatic firefighting equipment.
- Uninterruptible power supplies regularly tested against fictional power outages.

### Technical and Organisational Measures

#### Organisation of Information Security

Puzzel has a security organisation that covers all relevant areas of the business. Puzzel has appointed one or more security officers responsible for coordinating and monitoring the security policies and procedures. Puzzel ensures that its Personnel are competent in information security.

- Puzzel employs Personnel with full-time responsibility for information security.
- Puzzel's CISO is assigned the Data Protection Officer role and is responsible for managing Puzzel's Information Security Management System (including Data Privacy) and is reporting directly to BoM independent to operational management.
- Puzzel has a comprehensive set of information security policies, approved by BoM and disseminated to all Personnel.
- Puzzel security policies are reviewed at least annually and updated whenever needed.
- All Puzzel Personnel have signed legally reviewed confidentiality agreements that apply during and post-engagement.
- Failure of Personnel to follow information security policies can be treated as a disciplinary matter and lead to sanctions, including dismissal.
- All Puzzel Personnel are given training in information security with focus on data protection.

- Data Protection by design and default is a basic principle for the Puzzel Contact Centre Services.
- Puzzel is committed to continual improvement of its security.

### Information Security Management System

Puzzel has an ISMS (Information Security Management System) in place to evaluate risks to the security of Personal Data, to manage the assessment and treatment of these risks and to continually improve its information security.



Puzzel has deployed an Information Security Management System (ISMS) to manage security professionally and to support Puzzel's business objectives. The Information Security Policy is the foundation of Puzzel's ISMS and is supported by underlying policies and procedures detailing security related activities and controls. The Information Security Policy is revised and improved annually.

Puzzel and its ISMS has been and continues to be audited by an independent, external auditor and certified under ISO/IEC 27001:2013. We are also certified ISO/IEC 27701:2019 (Extension to ISO/IEC 27001 for privacy information management) and by Cyber Essentials.

### Statement of Applicability

The applicability of all controls in ISO/IEC 27001:2013 Annex A have been evaluated against requirements from all interested parties. All controls listed in Annex A have been mapped to requirements and marked as applicable in the Statement of Applicability. This means that Puzzel must adhere to, and be audited towards, all parts of ISO/IEC 27001:2013.

### Physical Access

Physical access to Personal Data is protected.

- Puzzel runs the Puzzel Contact Centre Services from professional, third-party Data Centres with a defined and protected physical perimeter, strong physical controls including access control mechanisms, controlled delivery and loading areas, surveillance and 24x7x365 guards. Only authorized representatives have access to the data centre premises.
- Power and telecommunications cabling carrying Personal Data or supporting information services at the production data centre are protected from unauthorized access and damage.
- The production data centre and its equipment are physically protected against natural disasters, malicious attacks, and accidents.

- Equipment at the production data centre is protected from power failures and other disruptions caused by failures in supporting utilities and is correctly maintained.
- Equipment or disk media containing Personal Data (including faulty or end of life disks) are not physically removed from the production data centre unless securely erased prior to such removal or being transferred securely for destruction at a third-party site.
- When Personal Data is copied electronically by Puzzel outside the production data centre, appropriate physical security is maintained, and the data is encrypted at all times.

### System Access

Puzzel data processing systems are used only by approved, authenticated users.

- Access to Puzzel internal systems is granted only to Puzzel Personnel and/or to permitted employees of Puzzel's Sub-Processors and access is strictly limited as required for those persons to fulfil their function.
- All users access Puzzel systems with a unique identifier (user ID).
- Puzzel has established a password policy that prohibits the sharing of passwords and requires passwords to be changed on a regular basis and default passwords to be altered. All passwords must fulfil defined minimum. Each computer has a password-protected screensaver.
- A second factor of authentication is required for access to online systems containing Personal Data.
- Only secure protocols are in use for remote administration (e.g., SSH v2, RDP and HTTPS).
- Remote administration of Puzzel systems use industry standard VPN technology.
- Puzzel has a thorough offboarding process to deactivate users, their access, and data when a user leaves the company or a function.
- An Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) is deployed at the production data centre to help identify potential inappropriate access.
- For Customer access to the system, Puzzel provides a wide range of authentication capabilities including the ability for Customers to set their own password policies and support for two-factor authentication.
- Puzzel maintains a responsibility matrix linking assets and technology to responsibility owners.
- Puzzel maintains an asset register containing all parts of the Puzzel Contact Centre Services.

### Data Access

Persons entitled to use data processing systems gain access only to the Personal Data that they are authorized to access.



- Puzzel restricts Personnel access to files and programs on a “need-to-know” basis.
- Personnel training covers access rights to and general guidelines on definition and use of Personal Data.
- Where appropriate and practical, Puzzel employs data minimization and pseudonymizing to reduce the likelihood of inappropriate access to Personal Data.
- The production environment for the Puzzel Contact Centre Services is separate from the development and testing environment, and development Personnel do not access to the production environment other than under troubleshooting scenarios.
- Puzzel uses up-to-date anti-malware software on all appropriate computers and servers.
- Puzzel uses well-configured firewalls for the Puzzel Contact Centre Services.
- The Puzzel Contact Centre Services contains versatile capabilities to set roles and permissions to let Customers manage authorizations so that Personal Data is only made available to appropriate users when needed.
- Puzzel ensures that appropriate Personnel receive alerts and notifications from system software vendors and other sources of security advisories and installs system software patches regularly and efficiently.

### Data Transmission

Prevent Personal Data from being read, copied, altered, or deleted by unauthorized parties during transfer.

- Customer access to the Puzzel Contact Centre Services is protected by encrypted protocols.
- Puzzel configures TLS for security, for an up-to-date report on our configuration, see <https://www.ssllabs.com/ssldb/analyze.html?d=client.puzzel.com>.
- Puzzel uses encryptions for all other transmissions of Personal Data outside the production data centre.
- Puzzel web servers only use certificates issued from recognized 3rd party certificate vendors.
- Any Personal Data stored outside the production data centre is protected by encryption at rest.
- The Customer is responsible for the security of Personal Data once it has been transmitted from Puzzel to the Customer including when downloaded or accessed by Customer users.

### Confidentiality and Integrity

Personal Data remains confidential throughout processing and remains intact, complete, and current during processing activities.

Puzzel has a defence in depth approach to ensuring confidentiality and integrity and many of the measures in other sections of this document safeguard confidentiality and integrity. Some other measures that contribute include:

- Puzzel has a formal background check procedure and carries out background checks on all new Personnel with access to Personal Data.
- All Puzzel Personnel are obligated to sign confidentiality agreements and must adhere to business & ethics conduct policies.
- Puzzel trains and tests its software engineers and quality assurance Personnel in application security practices and secure coding practices.
- Puzzel has a central, secured repository of product source code, which is accessible only to authorized Personnel.
- Puzzel has a formal product development security policy and uses a Secure Development Lifecycle (SDLC) that includes a wide range of security testing, flaw reporting, measures, and management procedures.
- Security testing includes code review and employing static code analysis tools on a periodic basis to identify flaws.
- All changes to software on the Puzzel Contact Centre Services are via a controlled, approved release mechanism within a formal change control program that tracks, documents, tests, and approves change requests prior to implementation (ITIL standard).
- Puzzel do not use Customer Data in training.
- Puzzel has a procedure for vulnerability management to ensure confidentiality, integrity, and availability.

### Availability

Personal Data is protected from accidental destruction or loss, and there is timely access, restoration, or availability to Personal Data in the event of an incident.

- IT Operations On-call duty arrangement available 24x7x365.
- Puzzel uses a high level of redundancy at the production Data Centres so that an availability failure of a single system or component is unlikely to impact general availability.
- The production Data Centres has multiple power supplies, generators on-site and with battery backup to safeguard power availability to the Data Centres.
- The production Data Centres have multiple access points to the Internet to safeguard connectivity.
- The production Data Centres is monitored 24x7x365 for power, network, environmental and technical issues.
- Puzzel uses commercially reasonable efforts to create frequent backup copies of Personal Data, and these are duplicated (cross-site) between the production Data Centres.
- Puzzel has a system in place to ensure that any failures of backup to operate correctly are flagged and dealt with.
- Puzzel performs restore tests from those backups at least quarterly.

- Puzzel has a business continuity plan in place which is regularly updated.
- Puzzel tests elements of its business continuity plan regularly and learns from the results of such tests.
- DDoS protections are installed and protecting internet perimeters. DDoS protection from ISP's are in place to mitigate high-volume attacks and in the Puzzel perimeters to mitigate more advanced attacks.
- Patching, security upgrades, equipment replacements, capacity add-ons and other infrastructure changes are carefully planned and executed in regularly announced maintenance windows. Standard maintenance work will normally not disturb Puzzel Contact Centre Services.
- Current availability of the Puzzel Contact Centre Services can be seen at <https://status.puzzel.com>.

### Job Control

Personal Data processed on a customer's behalf is processed solely in accordance with the relevant agreement and related instructions of the Customer including the use of Sub-Processors.

- Puzzel acts as a Processor with respect to Personal Data and stores and processes Personal Data to operate the Puzzel Contact Centre Services under the instructions of the Customer, who is the Controller.
- Puzzel does not access Customer Personal Data, except to provide services to the Customer which Puzzel is obligated to perform in support of the Customer experience including for general operation and monitoring of the Puzzel Contact Centre Services, troubleshooting and maintenance purposes, for security reasons, as required by law, or on request by the Customer.
- In some specific Customer setups Puzzel will use a limited number of Sub-Processors to help it provide the Puzzel Contact Centre Services. In this case this will be specified in the data processing agreement between the Customer and Puzzel.
- External parties such as Subcontractors and others with access to any of Puzzel's assets are required to sign Non-Disclosure Agreements.
- Puzzel has data protection agreements in place directly or via affiliates with all Sub-Processors that process Personal Data. Personal Data are not processed outside of the European Economic Area (EEA) other than if requested by a customer.

### Data Separation

Personal Data collected for different purposes is processed separately.

- Puzzel uses a multi-tenant architecture to achieve logical separation of Personal Data originating from multiple Customers.
- In each step of the processing, Personal Data received from different Customers can be identified so data is always physically or logically separated.

- Customers have access only to their own Personal Data.
- Puzzel networks are segregated according to system use and data sensitivity.
- Production systems are physically and logically separated from development and test systems.
- Voice and data networks are physically or logically separated to ensure the best quality and security.

### Incident Management

In the event of a security incident or Personal Data breach, the effect of the breach is minimized, and the Customer is promptly informed

- Puzzel maintains an up-to-date incident response plan that includes responsibilities, how information security events are assessed and classified, and response plans and procedures.
- Puzzel logs administrator and user activities at the production Data Centres to provide evidence in the event of an incident.
- The clocks of all systems at the production Data Centres are synchronized to a single reference time source to aid investigation in the event of an incident.
- System administrator activities, exceptions, faults, and information security events are logged in a central monitoring tool 24/7/365.
- Puzzel regularly tests its incident response plan with “table-top” exercises and learns from tests and potential incidents to improve the plan.
- In the event of a security incident or data breach, Puzzel will notify Customers without undue delay after becoming aware of the security incident or data breach. Puzzel’s Data Protection Officer will be included in the event of a data breach to secure correct handling of the data breach.
- Puzzel maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, to whom the breach was reported and the procedure for recovering data.

### Compliance

Puzzel tests, assesses, and evaluates the effectiveness of these technical and organizational measures. Puzzel is compliant with legal and contractual requirements.

- Puzzel has appointed a CISO to work with compliance fulltime and to ensure that Puzzel complies with relevant laws and regulations.
- Puzzel conducts regular internal and external audits of its security.
- Puzzel performs risk assessments to protect services and Customer Data.
- Puzzel has a formal policy for managing suppliers who have access to Personal Data, and this includes criteria for reviewing and approving suppliers and procedures for monitoring and reviewing their performance.

- Puzzel takes reasonable steps to ensure that Personnel are aware of and comply with the technical and organizational measures set forth in this document.
- Puzzel conducts at least annual 3rd party network and application vulnerability scanning's and or penetration tests on the Puzzel Contact Centre Services to identify vulnerabilities and to demonstrate security compliance.
- Puzzel uses industry standard processes to delete Customer Data when it is no longer needed.
- Audit rights given to Customers always exclude the right or ability to look at the data of other Puzzel Customers.
- Puzzel maintains a register of all Personal Data processing activities in the organization.

## Systems

- **Carrier interconnections & Internet connections:** Operator connections and internet connections are redundant, and traffic are either load balanced or run in active/passive mode from ISPs or Carriers.
- **Network, Firewalls & Backbone:** Internal networks (core switches, firewalls, routers, MUX'es, panels, intercompany connections) are redundant by design
- **Operator Switches and Session Border Controllers:** Soft-switches and Session Border Controllers (SBC's) have component resilience and are redundant across the Data Centres. They connect to operator networks, enabling Puzzel's services to switch voice traffic to and from callers and agents.
- **Traffic modules:** Traffic modules hold the contact centre functionality (IVR, ACD, menus, queues etc). They are stacked and scale by adding more modules (servers).
- **Application and Web servers:** Application Servers provide the services and functionality for the Puzzel Contact Centre such as user management, configuration, SMS services, email channel, social media channel, billing, statistics etc. Application servers are load balanced and redundant across the Data Centres.
- **Database servers & File Storage:** The databases are the primary storage of the Application- and Customer Data. Examples of data are CDR information, users, statistics, configurations, billing information, recordings, and chat dialogues. Databases are either redundant across the Data Centres or run Active/Passive configurations with synchronous synchronization of data between the Data Centres.

## Infrastructure and Resilience

All components in Puzzel's infrastructure are redundant by design. There are three levels of redundancy built into the infrastructure;

- **Component resilience:** Every component in the infrastructure has built in resilience within the unit. This might be redundant power adaptors, network cards, mirrored disks etc.
- **Load balancing & redundancy:** All critical infrastructure such as web servers and application servers are load balanced allowing operational systems even if components/ servers fail completely. For components not suited for load-balancing such as databases advanced synchronization mechanism is used between the active server and passive servers. This prevents data loss and minimal disruption during failover.
- **Geo redundancy:** All services are built so they can run with full capacity in all Data Centres that the services are hosted, allowing a full outage of either of the Data Centres.
- **Backup:** Separate backup systems do cross-site backup of Data Centres and are duplicated.

## Onboarding Support

Puzzel has extensive experience in delivering implementation projects for all contact centres of all sizes and we ensure a safe and thorough implementation process for all our customers.

We employ a mature and professionally accredited project methodology, which closely follows PRINCE2 and ITIL project best practice. Our approach has been engineered to foster close working relationships between you and your dedicated Puzzel project team who will be responsible for the delivery and onboarding of your new services.

At the start of the project, we will work closely with you to ensure we understand exactly how to complete a smooth, transparent, and truly collaborative partnership. A Project Manager and Key Account Manager will be provided during the implementation of the project. All parties will decide when the deployment is passed over to Puzzel support.

Quality assurance processes are embedded throughout the delivery lifecycle, underpinned by our ISO 9001 and 27001 certifications, and the process is supported by Puzzel's Services team which includes Project Managers, Implementation Engineers, and Solution Architects. Our project methodology is based on six core phases. Each phase provides the rigour of structured documentation and reporting, underpinned by robust delivery processes, all of which are managed from start to finish by our team.

## Delivery Staff

Puzzel provides a Project Manager, Key Account Manager, Solution Architect, System Engineer for all implementation projects.

## Training and Adoption

During the Training phase Puzzel will schedule all enablement activities including in-person or virtual training sessions for your Administrators and Users to learn intimately the solution. Each customer will supply the names and email addresses of all attendees. Once conducted, further training sessions can be purchased at any time.

## Offboarding Support incl access to data

The Customer shall be entitled to require the orderly transition of the Services from Puzzel to the Customer and/or any third-party supplier appointed by the Customer by sending Puzzel a notice to that effect (“Exit Assistance Notice”) at any time prior to termination.

The migration process will then commence where the customer and Puzzel will agree and define all items, data, and material that the customer may wish to transfer prior to deletion. Once agreed and actioned, the deletion process will occur to ensure the customer instance is deleted, in-line with data protection agreements such as GDPR.

## Service Constraints

Scheduled maintenance may result in downtime; however, no downtime is ever expected during these periods.

## Service Levels

Puzzel Digital Engagement has an Availability target of 99.9%.

## Technical Requirements

For agents: Chrome, Firefox and Edge is supported. For mixed http/https content web sites a risk for limited functionality may occur in certain browsers.

For such web sites currently Firefox or Edge is recommended.