webmate

Platform Security

2021-01

by TESTFABRIK

webmate Secure Cloud Testing

- Compliance & Privacy
- Data Controls
- webmate Architecture
- Identity Management
- Network Integration
- webmate Connect
- Security Management

Compliance & Privacy

GDPR COMPLIANCE

- Testfabrik is a data processor of customer data in accordance with the EU General Data Protection Regulation (GDPR).
- Testfabrik has implemented a privacy compliance program to comply with GDPR requirements.
- All customer data is stored and workloads are processed in our data centers located in Germany.

ISO/IEC 27001 Data Center Certification

- webmate services are hosted in data centers compliant with the ISO/IEC 27001 information security management system.
- ISO/IEC 27001 covers information security organization, physical security, access control, communication security, incident management, use of cryptography, etc.

Data Controls

3rd Party Data Access

- Testfabrik does not share customer data in any form with 3rd parties nor do we provide access to production systems to 3rd parties.
- With partners providing support services to Testfabrik, e.g. hosting, contractual agreements are in place.

Device Security

- Android and iOS mobile devices are physical devices hosted in our data centers.
- Devices belonging to a customer's "dedicated cloud" are isolated from other customers' devices (WiFi, USB).
- Devices in the "public cloud" are automatically cleaned after every access.
- Virtual desktop devices are provisioned on demand for a specific customer and destroyed after use.
- All customer devices are grouped in an isolated "Customer Device Center".

Data Security

- Testing and customer data is stored on equipment dedicated to Testfabrik (no global cloud vendors).
- Data communication is secured with TLS 1.2+ or various VPN technologies (IPsec, OpenVPN, as requested by customers).
- Customer data is only accessed by Testfabrik engineers on a strict per-need basis for support and troubleshooting purposes.
- Note: We recommend to use only non-sensitive or synthesized data for testing.

Data Retention

- Data created during testing (e.g. logs, statistics) is retained at least 30 days. Customers that require longer retention periods may request individual retention configurations.

Identity Management and Organizational Structure

Individual User Accounts

- Every webmate user is assigned an individual user account. Users are identified by login email address, a password or an API key (non-SSO case).
- A user may be assigned the role of an "organization administrator" who has elevated permissions, e.g. to invite other users or modify their permissions.

Role-Based Access Control

- webmate defines a set of permissions that control access to resources or if certain use case can be executed.
- Organization administrators may create and configure organization roles that bundle sets of permissions.
- Roles may be assigned to users on a per-project basis.

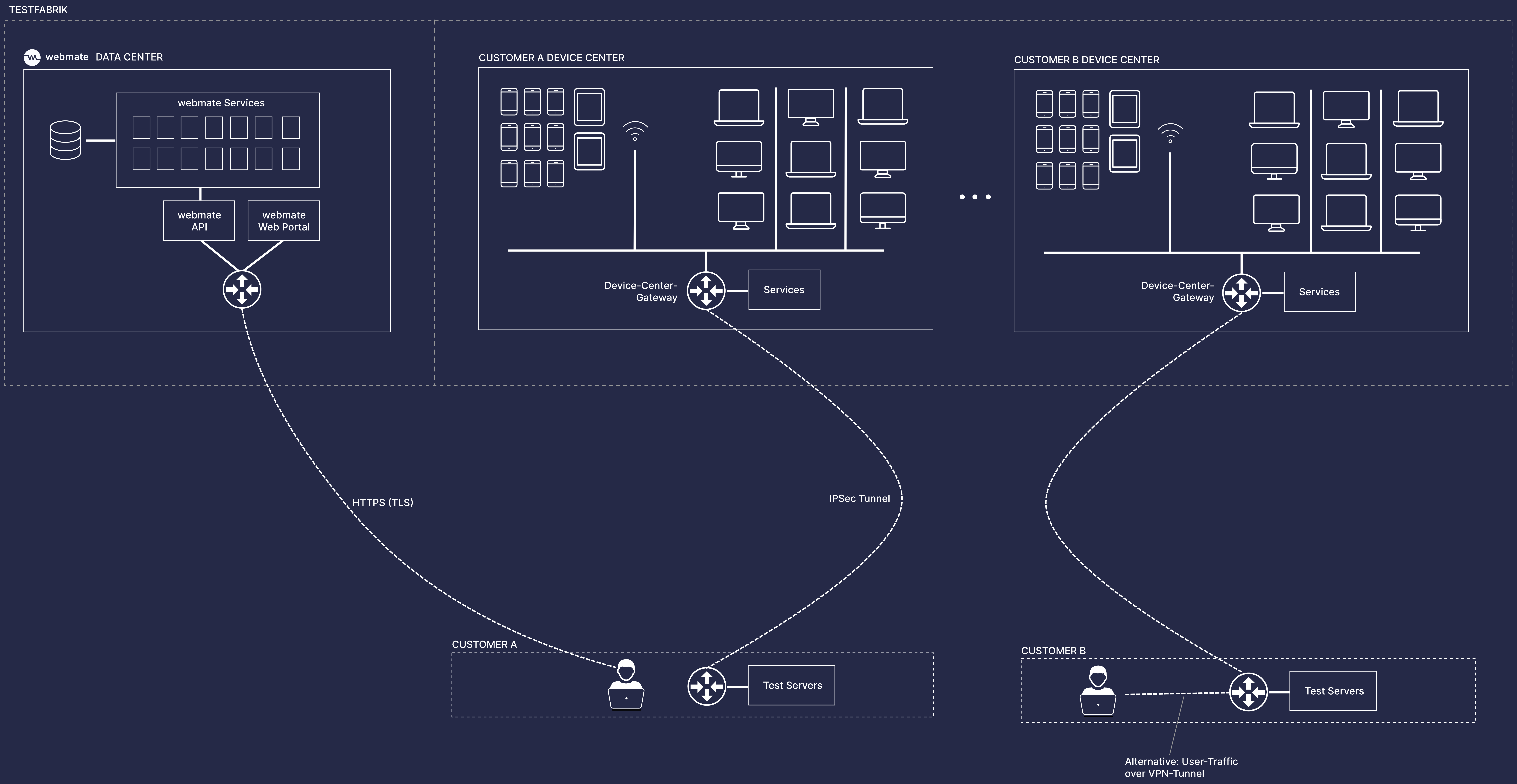
Organization Projects

- webmate resources can be assigned to "Projects".
- Test activities in webmate are isolated within projects.
- Organization administrators
  - manage projects of an organization,
  - assign resources to projects
  - configure, which users may access a project
  - assign roles (permissions) to users for a project

SSO

- webmate can be configured to use an OpenID Connect provider (e.g. Keycloak or Active Directory FS) for user authentication.
- Roles can be assigned dynamically to users by the OpenID Connect provider.

webmate Architecture



webmate Architecture

Customer Device Centers

- Every customer has an individual, isolated Device Center containing its (real and virtual) devices and other resources.
- Device Center access is restricted to
  - its customer (e.g. via VPN)
  - devices deployed / used by customer
  - webmate services
- Access to customer network is only possible through its associated Device Center.

webmate Data Center

- The webmate data center contains services and infrastructure required to run webmate.
- webmate is API first and webmate services are provided through an API gateway.
- webmate Data Center services are shared by customers. Authentication and authorization are implemented carefully.
- If required, Testfabrik offers running a dedicated data center for a customer.

Communication

- Communication to/from Customer Device Centers is secured using VPN technologies (IPsec, OpenVPN, Wireguard) and TLS 1.2+.
- Customer communication with a data center is secured with TLS.
- If required, customer communication may also be tunneled using the Customer - Device-Center connection.

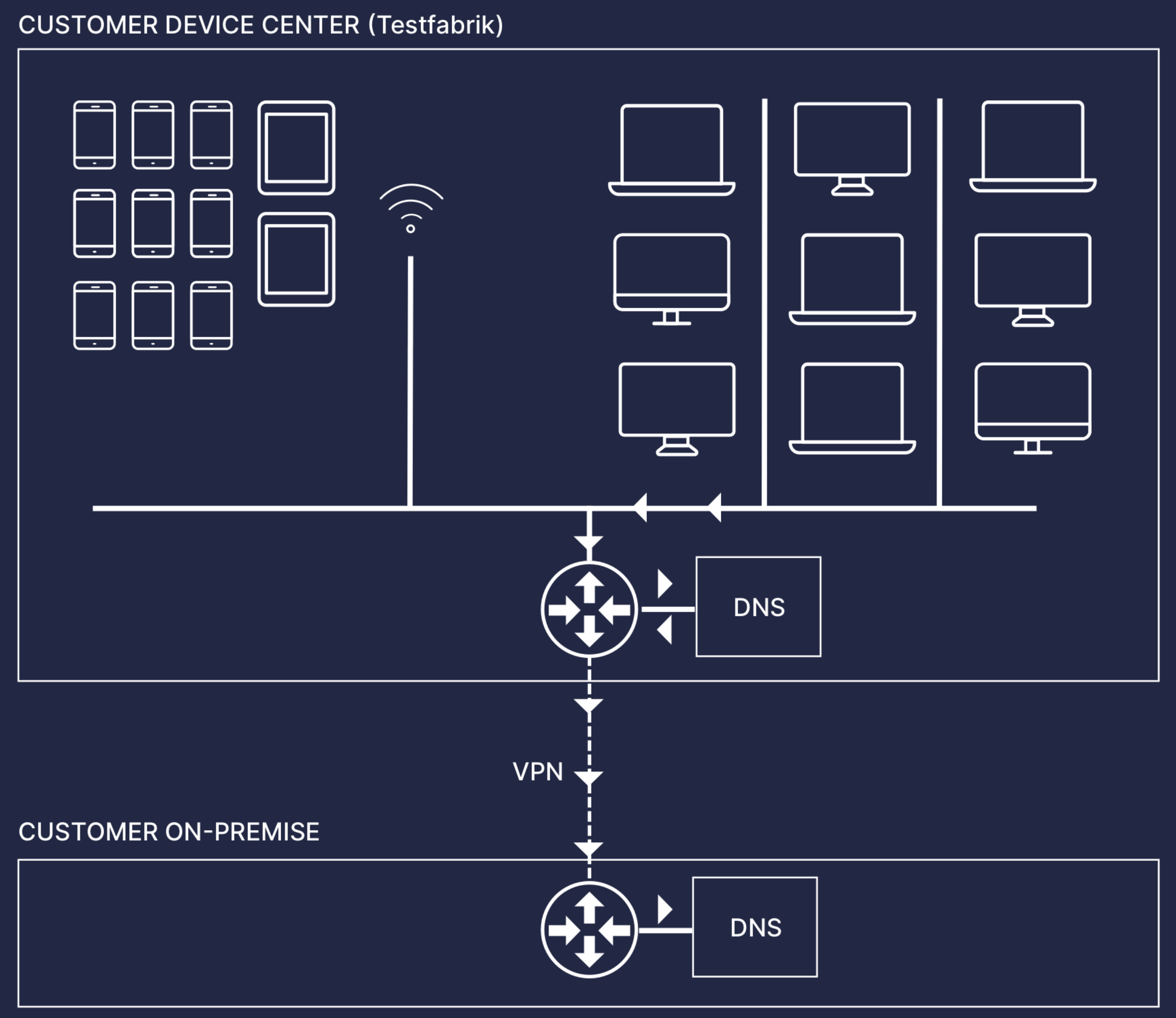
Network Integration

IPsec VPN / OpenVPN

- Communication between customer networks and a webmate Device Center may be secured using a VPN technology.
- After configuration, VPNs are permanently active.
- Devices in Device Center may use VPN connection to access customer application servers for testing.
- Services in Device Center may use VPN to access customer infrastructure, e.g. Microfocus ALM for issue reporting.

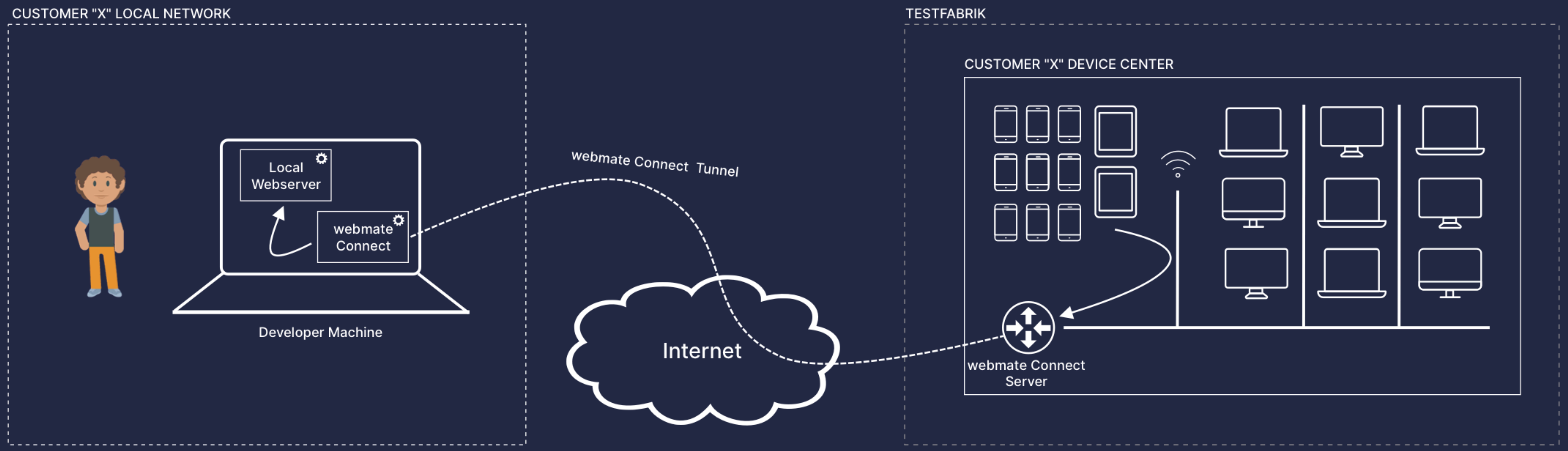
DNS / Name Lookups

- Device Center nodes and services may be configured to use customer DNS infrastructure.
- This allows using non-public host names.
- It is also possible to configure multiple upstream DNS servers or configure individual DNS records manually.



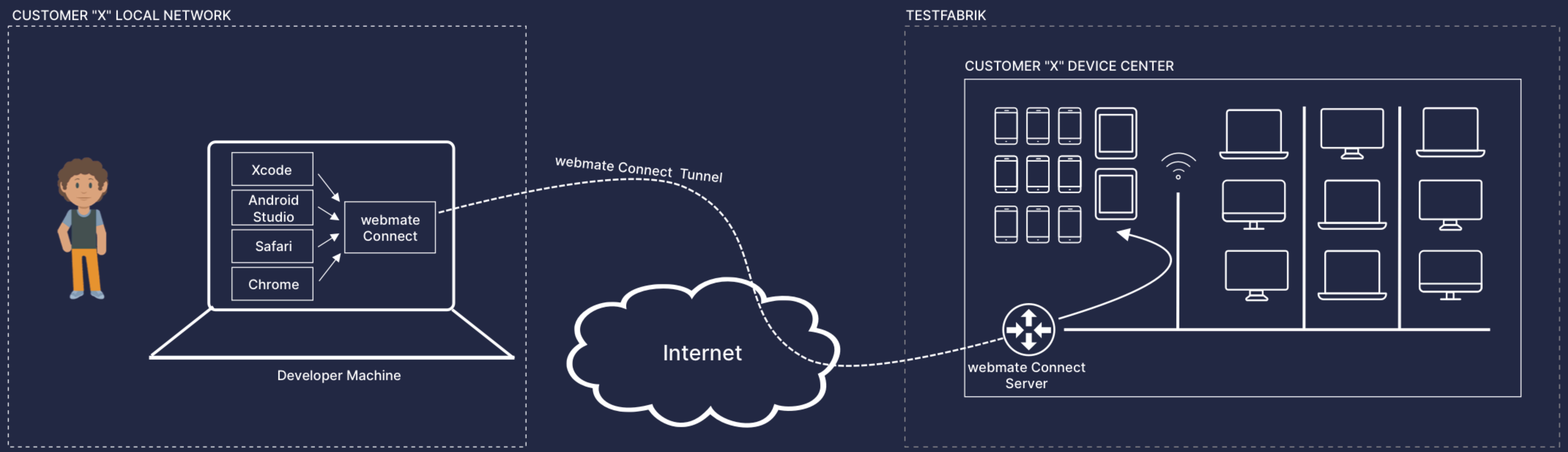
webmate Connect – Local Access

- webmate Connect is an optional offering that allows accessing local resources from Device Center devices.
- webmate Connect is a binary that can be downloaded to developer machines / CI services.
- It can be used to test applications on developer machines.
- Communication is tunneled over HTTPS / TLS 1.2.
- Communication is established from client computers and may use existing enterprise proxies (with WebSocket support).
- webmate Connect source code may be provided for analysis.



webmate Connect – Application Access to Device Center

- Some applications try to access resources on a local computer, e.g.
  - Xcode / Safari access mobile devices via local Unix Socket,
  - ADB / Android Studio / Google Chrome access mobile devices via local TCP socket,
  - CDP-based testing frameworks (Cypress, Puppeteer, Playwright) access CDP-TCP-Socket on local Chrome, Edge, or Firefox.
- webmate Connect can be started in a mode that redirects requests to these local resources (Unix Socket, local TCP sockets) to Device Center devices.



Security Management

Security Testing and Auditing

- Testfabrik performs tests of webmate infrastructure and the webmate web application.
- Internal tests are conducted by our security team.
- Regular external audits and penetration tests are conducted.
- In compliance to GDPR regulations, conformance of security processes and organization checked on a regular basis.

Incident Response

- Testfabrik operates an incidence response team for webmate.
- Incidents are classified and prioritized with regard to severity and impact.
- Incident Response team coordinates escalation and coordination in case of an incident.

Disaster Recovery / Business Continuity

- Recovery plans for vital core functions of Testfabrik's business are maintained.
- Risks are evaluated and appropriate controls and measures implemented to mitigate / reduce risks.
- Regular disaster exercises assess the effectiveness of controls and measures, e.g. backup procedures.

Change and Patch Management

- Changes and patches are deployed in accordance with defined SLAs.
- Major changes are communicated early.

TESTFABRIK

info@testfabrik.com

www.testfabrik.com