Stay Open.

OX Whitepaper

OX Protect

Version 2.0

January 2020

1 OX Protect Overview

OX Protect is the new end-user facing security solution from Open Xchange. It offers malware and Phishing protection, and Parental Control based on DNS filtering to consumers and allows for fine-tuning of settings per household as well as per device or per profile (of a household member).

OX Protect brings easy control over profiles that allow specific settings for each family member and for their connected devices. Profiles and settings can be changed using a web portal or by using either the OX Protect app, or a third-party app integrated with the OX Protect API.

OX Protect uses smart DNS filtering technology to provide an extremely efficient and cost-effective network filtering solution for malware and undesired content.

1.1 Features

1.1.1 General Features

OX Protect includes many features that provide an exceptional experience for protecting family members and smart devices, including:

- Flexible profiles for family members and devices – Define multiple profiles each with their own specific settings and assign devices to the relevant profiles. This provides the ultimate controllability and flexibility to provide a safe and tailored internet experience, whether that's for children or for IOT devices.
- Per Device Control – OX Protect can differentiate between various devices in the household. This allows assignment different filtering profiles for different devices in the household, so child's laptop can be treated differently from a parent's tablet, or the family TV.
- Global and per subscriber Black and Whitelists – Allows blocking or allowing of domains on a system-wide level as well as for households or individual profiles.
- Advanced timers – This allows for features such as 'bedtime', whereby all devices for a particular profile cannot access the internet during the night.

- Real-time alerts – Sending alerts to end-users when suspicious or malicious events take place. These alerts can be sent via the OX Protect app (using Push Notifications), Email, or SMS. For example, alerts when detecting access to a malware or phishing related domains.

- REST API providing access to the end-user settings – The API allows control of the per-subscriber settings stored in the OX Protect Middleware. It allows access to the profiles and devices associated with a specific account. In this way, the control interface can be easily integrated in existing web portals, the OX Protect Apps, or integrated into existing apps.

- Integration via OAuth2 – The REST API supports the OAUTH2 protocol for easy integration into existing mobile or web applications, without requiring separate authentication.

1.1.2 OX Protect for Families

OX Protect for Families offers content filtering and parental control with unique multi-level control for Safe Browsing per user and supports customizable categories for filtering, configurable time-windows such as bedtime and off time, per-profile whitelists and blacklists.

Features of Protect for Families include:

- Selective DNS filtering based on categorization of hundreds of millions of sites.

- Parental control – Enabling content filtering of the categories of content for the whole household, or for individual family members and devices. Each profile can have a completely tailored internet experience.

- Support for Categories - Block all domains related to a specific category, for example ‘news’, ‘social media’, or ‘dating’. Protect supports over 250 different categories for fine grained control.

- Platform Support – Allows fine-grained control for specific widely-used platforms such as Facebook or Instagram. For example, a parent can block Social Media as a category, but still enable Facebook to be used.

1.1.3 OX Protect for Malware

The filtering engine makes use of best in breed threat intelligence to provide protection from malware and phishing:

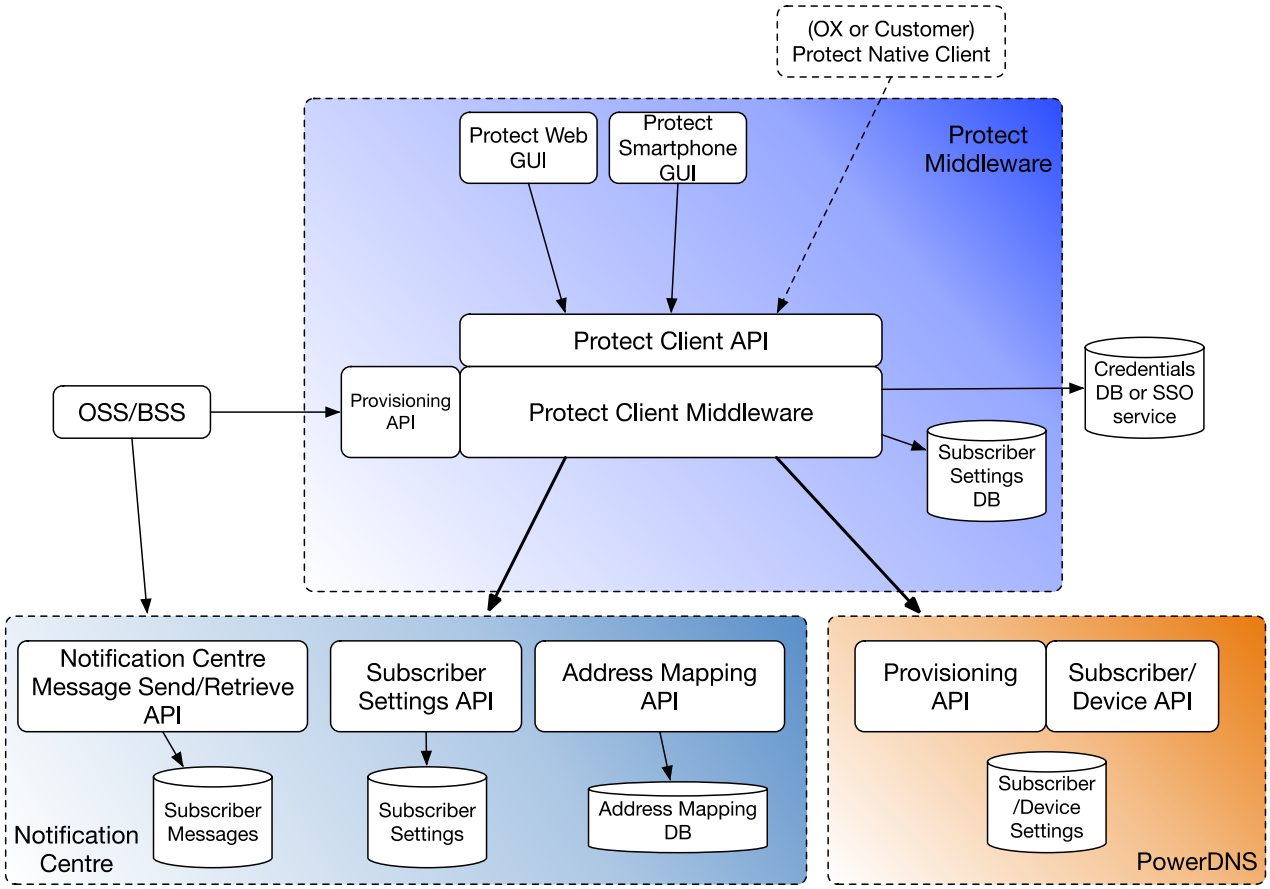
- Block access to known bad malware sites, including drive-by downloads, ransomware and hacked websites.
- Block access to known phishing sites, to prevent credential theft and exposure to malware.
- Block access to servers that correspond to known malware Command and Control (C2) endpoints, and thus detecting potentially infected devices, including IOT devices.

1.2 OX Protect Components and Architecture Overview

The diagram below shows the overall architecture of OX Protect and the interaction between the three main components:

- **OX Protect Middleware** contains the end-user settings, and facilitates interaction with the Apps, GUI's, provisioning from the Telco's side, etc.
- **PowerDNS** is part of the network's DNS infrastructure and performs the actual filtering and analysis of the DNS requests.
- The **Notification Center** takes care of translating and forwarding events in the network to the relevant users, based on specific subscriber settings.

OX Protect Architecture



2 OX Protect Middleware

2.1 Overview

The OX Protect Middleware contains the end-user settings. Through the customer facing API it facilitates interaction with the Protect App and GUI's. It also provides an operator-facing provisioning API.

2.2 Middleware Subscriber API

The middleware provides an HTTP API to modify the filter settings of users and devices. This API is used by end-user facing web applications and mobile applications (such as the included OX Protect app) and can also be used for customer applications and GUIs such as Self-care portal.

This API is end-user focused and includes support for end user configuration, and authentication/authorization, including OAUTH2 support. The APIs can used to integrate with customer OSS/BSS systems, existing mobile apps, self-care portals, and customer care systems.

This API is also used by Open-Xchange's own mobile apps and web UI.

2.3 Provisioning API

The Provisioning API allows the operator to create new subscribers/users in OX Protect.

3 Notification Centre

The Notification Centre provides a flexible and scalable solution to the problem of alerting users to events. It supports multiple notification methods including Push (Android and iOS), SMS and Email.

The Notification Centre provides a REST API to send new events, which is used by the PowerDNS component, but can also be used by third-party components to contact users via any of the supported notification methods.

4 PowerDNS

OX Protect uses the PowerDNS platform to analyze DNS requests and apply the relevant policies based on the subscriber and device making the request.

Applying policy at the DNS level avoids having to deploy expensive DPI equipment in the core network, saving money and increasing network performance.

Integration with a variety of network authentication sources is supported, including RADIUS for broadband networks, and the GX interface to the PCRF for mobile networks.