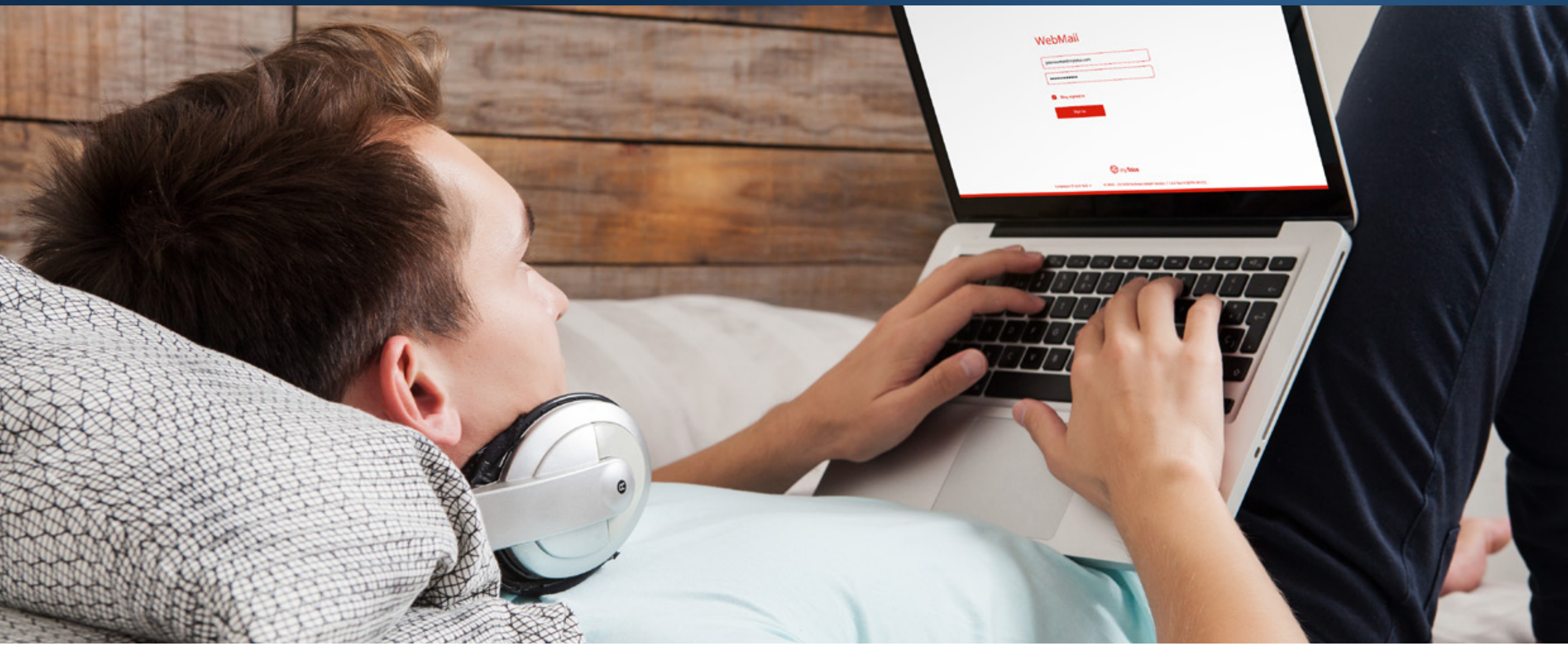
Stay Open.



DATASHEET

OX Abuse Shield

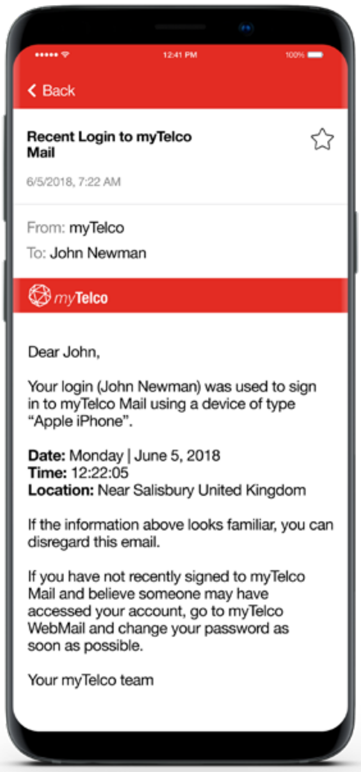
Protect your subscribers

Abuse protection meets WebMail
Most ISPs and mail providers have protection in place for SMTP abuse, but very few have the same protection for web applications such as WebMail, POP and IMAP. OX Abuse Shield solves this problem by providing a single system for handling abuse. It integrates with both OX App Suite and Dovecot Pro to protect against login and authentication abuse, brute force attacks and also to enforce common authentication and authorization policies across the platform. Additionally OX Abuse Shield detects suspicious logins, and flags potentially compromised accounts and abusing IP addresses.

OX Abuse Shield can be integrated with the authentication flow of any application, using a well-documented REST API.

Customization is the key
The abuse daemon ships with default policies to protect against brute force attacks. For even more sophisticated protection, Open-Xchange can provide customized Lua scripts that handle a wide variety of abuse scenarios as well as implementing customer-specific features and policies.

Comprehensive feature set
OX Abuse Shield features include DNS lookup, native GeoIP support, rate limiting and tarpitting, a flexible in-memory statistics database to provide abuse statistics and integration with customer authentication/authorization systems using the open HTTP REST API.



Recent Login to myTelco Mail

6/5/2018, 7:22 AM

From: myTelco
To: John Newman

Dear John,

Your login (John Newman) was used to sign in to myTelco Mail using a device of type "Apple iPhone".

Date: Monday | June 5, 2018
Time: 12:22:05
Location: Near Salisbury United Kingdom

If the information above looks familiar, you can disregard this email.

If you have not recently signed to myTelco Mail and believe someone may have accessed your account, go to myTelco WebMail and change your password as soon as possible.

Your myTelco team

The magic behind the security

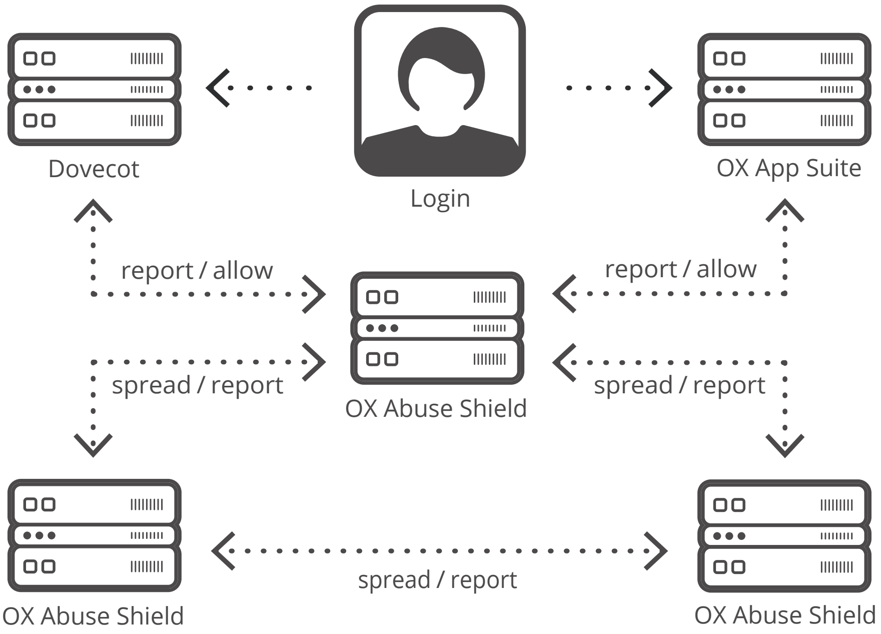
Clustering
OX Abuse Shield can be configured to run in a clustered environment, with multiple servers sharing data to achieve a unified view of abusive behavior. Clustering uses the UDP protocol and all information is encrypted over the wire using symmetric encryption and a shared secret between all servers. Clustering is achieved by configuring each Anti-Abuse Shield server to replicate the in-memory DB to a configured set of servers. Typically, those other servers would be configured to also replicate their DB to the same set of servers, thus creating a "mesh". In this way, OX Abuse Shield can be configured to create a highly available cluster, where all servers in the cluster have all the information relating to abuse and can thus be accessed in the same way by clients (the diagram below visualizes this approach). Alternative clustering arrangements can be configured, for example creating a set of "report-only" servers, which receive reports from clients and "spread" those reports to a set of "allow-only" servers, which contain all the abuse statistics and are queried by clients to decide whether to allow or refuse logins.

Sophisticated suspicious login detection
The login data and all login reports are now stored long-term in Elasticsearch. This functionality helps with sophisticated anomaly features such as detecting suspicious logins.

Real-time alerts about suspicious logins
When a suspicious login is detected, for example due to anomalies from previous logins, the system sends a real-time email alert to end-users or via webhooks to abuse and operation teams.

Advanced reporting
Periodic reports about potentially compromised users and IP addresses abusing the system based on long-term data stored in Elasticsearch are available. Pre-configured Kibana dashboards help identifying abusive IP addresses and compromised users.

How OX Abuse Shield works



OX Abuse Shield at a glance:

Replicated/clustered architecture
Login reports are shared between all the servers in the cluster so there is a single view of abuse.

Scriptable policy language
Using the Lua language, the functionality of the daemon can be extended to record and protect against a large variety of abusive behavior.

DNS lookup
For looking up IP addresses and domains in blacklists.

GeoIP lookup
GeoIP lookups can be made and incorporated into policy decisions.

Ratelimiting and tarpitting
Both can be enabled and enforced based on IP address, login name, GeoIP location, time windows, etc.

Flexible in-memory statistics database
A versatile and extensible in-memory data-base is used to store statistic information about abuse over time periods from a few minutes to many hours.

Integration with customer authentication/authorization systems
Customers can use the open HTTP REST API to benefit from the protection of the anti-abuse daemon in their own authentication and authorization systems.

Admin console
The admin console can be used for introspection, debugging and retrieving statistical information.

Suspicious login detection
Anomalies in logins are detected and real time alerts are sent to operators or end-users.

Reporting
Reports on potentially compromised accounts and abusing IP addresses are sent periodically to operations teams.

Stay Open. OX

www.open-xchange.com | info@open-xchange.com