

OK on the web *yes*



We can help you to keep an eye on web and social media usage by enabling you to filter or restrict access to particular websites and the content within them.

Highlights

- Gain access to skilled resources and best-of-breed technology and monitoring equipment to help enhance your security posture
- Increase protection from new emerging social media (Web 2.0) threats, backed by industry leading contractual Service Level Agreements.
- Continuous rapid web threat research helps to provide comprehensive protection against new threats.
- Use of hybrid on-premise and Cloud based filtering enables most malware filtering to be effected off premise in the Cloud and thereby increase the amount and availability of bandwidth for business use
- Can reduce the hardware or software required for email, web and data protection, helping you to reduce costs and complexity.

Web filtering has advanced from simply making use of white-and black-lists for websites and signature-based malware detection. It now includes site reputation and real-time analysis that looks for dynamic and scripted threats embedded in web content and code such as JavaScript and Flash. A web security suite can restrict access to web-based applications – such as online games, chat, or file-transfer – based on either the URL or unique protocols and client-side applications.

The Optus Managed Content and Gateway security service provides centralised single policy formulation for web usage together with a powerful unified management platform to enforce and report on these policies.

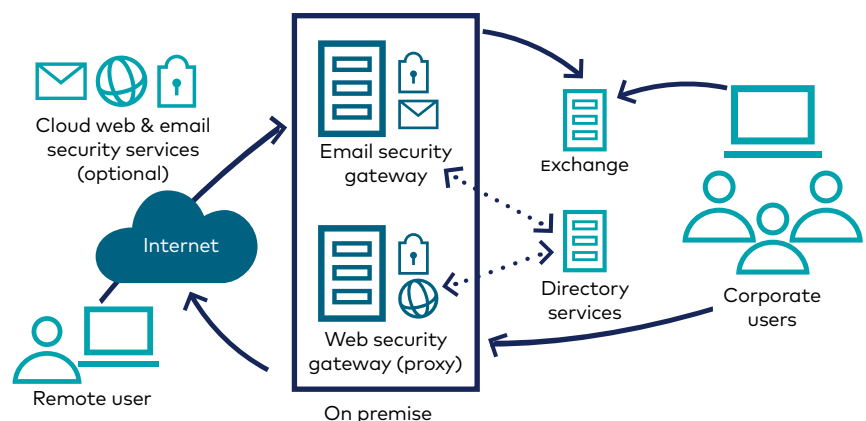
How it works

An Optus Managed Content and Gateway Security service can be deployed in a number of ways:

- **On-premise** – all components of the content filtering infrastructure are hosted on the customer premise
- **Cloud** – a content filtering gateway hosted in the cloud accessible via the Internet
- **Hybrid (on-premise and a cloud)** – some components are hosted in the cloud and some on-premise.

A web security suite typically consists of:

- An appliance to filter web traffic on one or more sites
- A management console to configure and report on users, groups and policies
- A database to store log and reporting data
- And optionally a cloud-based component to filter inbound traffic from the internet before it uses bandwidth and reaches your premises, as well as acting as failover option in the event of appliance failure.



Content and gateway security functions

Depending on the solution and services chosen the following functions can be provided:

Web security

A web proxy service for security, administration and caching as well as separating the corporate network from the outside network.

Real-time content classification

- Empowers social web controls and content classification of large, active social networks such as Facebook.
- Real-time data classification.
- Classifies structured and unstructured data, and includes parsing and decoding support to address outbound data theft.

Malware protection

Applies multiple anti-malware engines to identify both general and specialised malware, including infected PDF files.

Reputation analysis

Considers more than 20 characteristics to provide detailed assessment and reputation scoring that encompasses contextual awareness.

URL classification

Applies powerful machine learning to quickly identify a webpage based on its content – including images, multimedia and links.

High availability

Overall fault tolerance of your solution can be increased by providing a configuration that allows firewall devices to failover in the event of critical failure.

Directory integration

Integration with corporate directory services such as active directory, LDAP to provide more granular role based access control policy.

SSL inspection

Ability to inspect encrypted content by loading the digital certificate onto the content security gateways.

Advanced reporting

Customised agreed reports generated on a monthly basis by security specialists.

Feature availability

Optus works with industry leading vendors to provide best-of-breed technology solutions. The table below shows the service options available.

Standard Features
Web security
Real-time security classification
Real-time data classification
Malware protection
Reputation analysis
URL classification
Optional Features
High Availability
Directory Integration
SSL inspection
Advanced reporting

Let Optus manage your security



We want to help to reduce your exposure to security threats and incidents. Our aim is to assist you with protecting your valuable intellectual property and complying with legislative requirements.

We can help you to assess, design, implement and manage your security environment so you can move ahead with confidence knowing the confidentiality, integrity, availability and protection of your critical business data is in hand.

Through our managed services you have access to our experienced and skilled team to supplement your own resources.

Whether it is just one aspect of security such as Content and Gateway security or our whole suite of integrated security solutions, choose the peace of mind offered by Optus.