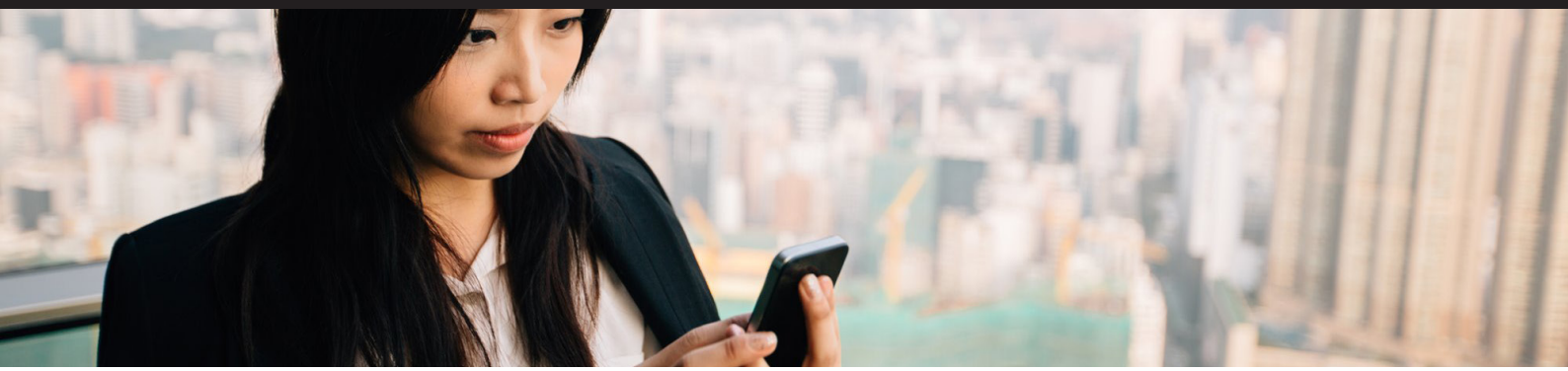
Orange
Cyberdefense



Service overview

Managed Content Filtering

Key benefits

Incident alert
Identification and notification of issues related to device availability.

Proactive monitoring
Subject to contract, 24x7x365 proactive monitoring of key device metrics.

Service-desk support
Subject to contract, 24x7x365 support to remediate issues in normal operation of scoped appliances.

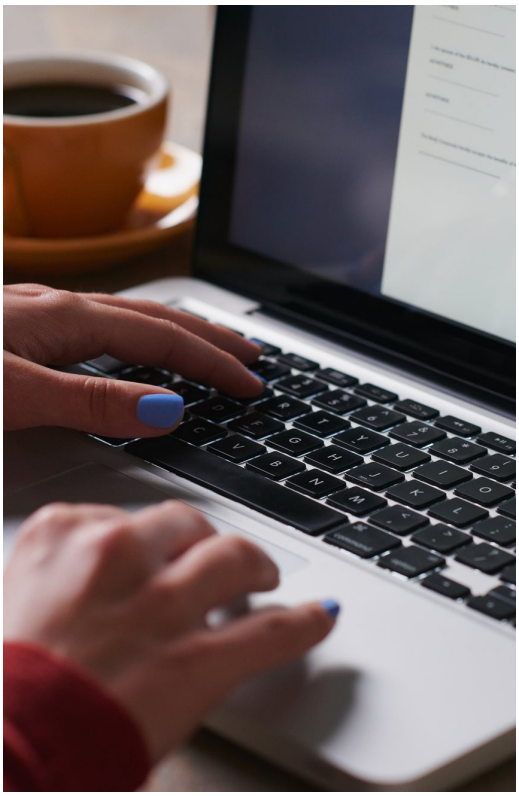
Patching, updates and upgrades
Where performed remotely, full deployment of patches, updates and upgrades to the device specific software.

Change management
a) In coordination with change processes and change windows specific to the customer business
b) Assistance with the creation and implementation of changes.

Service description

With the web browser and email reader the frequent target of hackers and social engineering, the rise of malicious web sites and emails has been exponential. Content security has traditionally been thought of in the context of protecting against HTTP and HTTPS web traffic, the lines between browser-delivered content and mail-client delivered content have blurred with HTML email just as much a target as HTML webpages.

Content filtering does not necessarily only apply to inbound web- or email traffic however. Outbound filtering, as part of a holistic approach to 'Content', mandates that documents and spreadsheets being sent to Software-as-a-Service (SaaS) applications, hosted Infrastructure-as-a-Service (IaaS), hosted Platforms-as-a-Service (PaaS) and third parties be filtered so that confidential information isn't published or shared in violation of regulatory compliance obligations or corporate policy.



Why Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries.

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Key service components

Email content filtering

- Ongoing addition, modification and removal of customer's filtered email domains
- Ongoing management of enforced email encryption**
- Policy management of email content filters governing: -
  - Unsolicited Bulk Email (UBE)
  - Spam detection policy controls and alerts
  - Anti-malware policy controls and alerts
  - Image controls (applies to images in email content)
  - Impersonation controls
  - URL filtering (applies to URLs in email content) controls
  - Sandbox delay controls
  - Geo-location controls
  - Data protection and compliance controls for vendor predefined templates (custom data-protection templates may be provided at additional Professional Services charges)
- Domain/Sender/Recipient/Destination whitelisting and blacklisting
- Auto-remediation and Clawback controls (applies to delayed removal of emails and attachments found to be malicious postdelivery)

Web content filtering

- Ongoing management of access- and URL filtering policies
- Custom Proxy Auto-Configuration (PAC) file creation and maintenance
- Custom Whitelist and Blacklist creation and ongoing maintenance
- Custom 'Block Page' creation and maintenance
- Ongoing management of antivirus/ antimalware policies
- Management of remote user's VPN content security policies
- Ongoing management of web isolation policies enforcing potentially hazardous websites to be opened in contained, cloud-based environments disabling active

Data loss prevention

- Management of vendor-provided compliance-based policies (custom policy creation and management may incur additional Professional Service charges)
- Whitelisting of false-positive blocked files