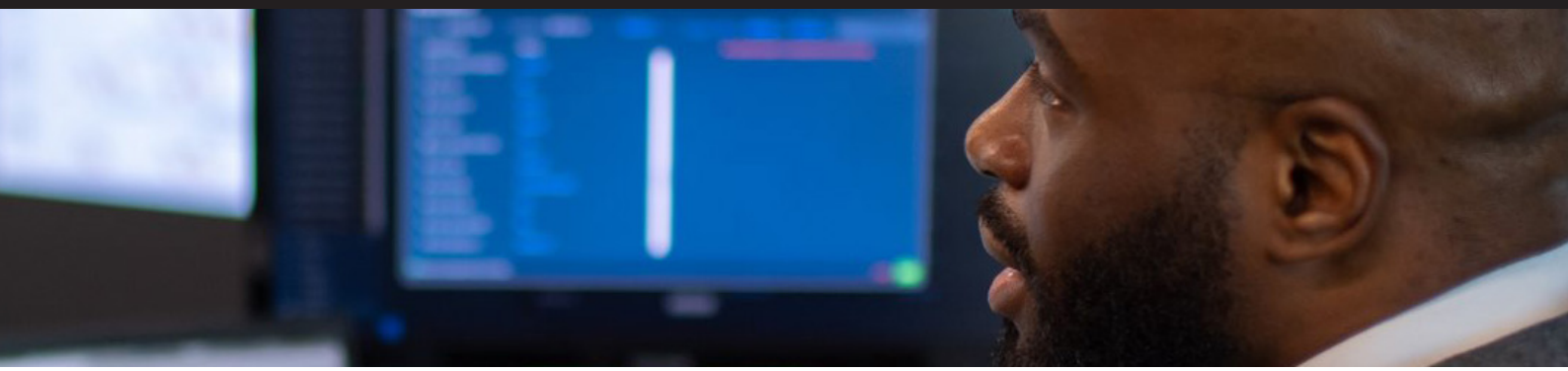
Orange
Cyberdefense



Service overview

Managed Application Delivery, Security and Access

Key benefits

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

Proactive monitoring
24x7x365 pro-active monitoring of key device metrics.

Help desk support
24x7x365 help desk 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 assessment
Assessment of risk to business-as-usual by requested changes.

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

Business continuity
Weekly backups of device policies and hardware configuration.

Service description

Applications, both web and discreet, are the life blood of most organisations, serving customers, third parties, partners and internal users on a 24x7x365 basis. It is therefore business-critical that they are able to be delivered on-demand.

Applications are also a primary source of risk for organisations, with hackers targeting applications in increasingly sophisticated ways.

Application availability and load balancing solutions judge routing decisions based on the content of the application, availability of the application's host servers, where the requests originate from, network conditions and several additional factors. This reduces response times, maximises throughput and makes optimal use of available resources.

Application Security goes beyond traditional network firewalling providing control at the application layer. This security is brought about by configuring rules based on applications such as: -

- Which users should have access from which devices
- Rules based on application behaviour and structure
- Geolocation rules allowing or restricting access by country or region
- DoS and DDoS rules preventing applications from being taken offline
- SSL traffic inspection

Application Access refers to creating and maintaining granular controls to ensure that only permitted users have access to discreet applications. These applications may be internal to the organisation or public-facing, such as Outlook Web Access, but need to have tight access restrictions imposed on their use.

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

Application delivery management components

- Application and on-going management of separate client-server architecture(s) ensuring optimised application delivery
- Provision of application-server performance visibility displaying response times,network conditions and user context
- Implementation and on-going management of up to 39 monitors to detect application delivery latency or failure
- Creation and maintenance of custom scripts for bespoke application delivery (additional charges may apply)
- Application Traffic Management with intelligent static and dynamic loadbalancing to eliminate single points of failure
- Implementation and on-going management of up to 19 delivery methods ensuring reliable delivery and availability
- Ongoing monitoring of synchronisation status to ensure transparent failover through connection mirroring

Application security management components

- Implementation and management of attack signatures, including the OWASP Top Ten, as released by the vendor and in accordance with customer change-control processes
- Management of IP intelligence linked with IP shunning (accelerated blacklisting) protecting from malicious sources
- Implementation and management of application layer DoS and DDoS detections
- Implementation and management of 'virtualpatching' signatures to protect application servers' Operating Systems or web-server layers until patched as requested by the customer
- Ongoing application-policy tuning enabling rapid detection of and protection against emerging threats (additional charges may apply)
- Installation of SSL certificates and ongoing monitoring of certificate validity
- Implementation of SSL termination policies, allowing inspection and mitigation of concealed threats
- Ongoing application awareness, monitoring client connections and server responses to mitigate threats based on security and application parameters

Application access management components

- Provisioning and on-going management of secure remote and mobile access to corporate resources from all networks and devices
- Definition and management of multi-layered profiles allowing access to different resources for users depending on the device type, authentication mechanism, location or device security status
- Definition and on-going management of access policies for authentication and authorisation to enforce user compliance with corporate policies and industry regulations
- Host checking functionality that ensures connecting devices comply with defined requirements and blocks or limits access by at-risk devices
- Configuration of flexible single sign-on and identity federation support allowing authenticated users automatic sign-on to back-end applications and services
- Installation of SSL certificates and ongoing monitoring of certificate validity