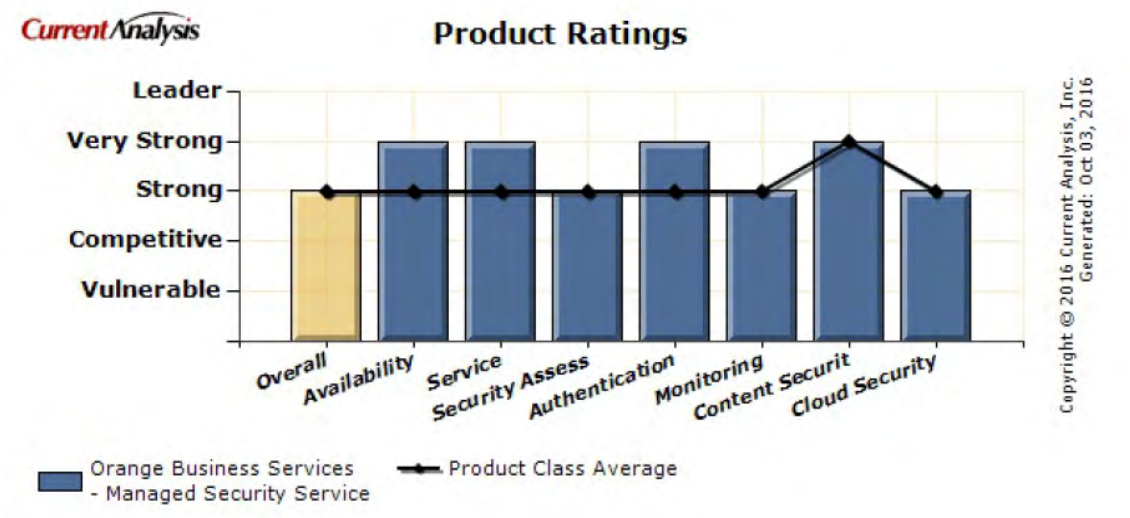
Orange Business Services - Managed Security Service

Marcus, John | September 28, 2016

Product Assessment - Managed Security

Marcus, John
Current Analysis
Principal Analyst,
Business Network and
IT Services

Summary



Competitive Strengths

- Hard-to-match mature global presence to support customer installations on the ground.
- Increasingly high-value services and flexible pricing and availability have helped generate organic revenue growth in the double digits.
- Well-established global security consulting, including GRC, security assessments, penetration testing and PCI DSS expertise, has built strong credibility as an advisory partner for enterprises.
- Orange is ahead of some peers in cloud security, having leveraged the cloud to evolve beyond the traditional managed security services approach, delivering security-as-aservice with pay-per-use options.
- Orange has a strong identity solution with three levels of multifactor authentication and identity federation for policy enforcement, and it is adding biometric technologies from partner Morpho.
- Orange can offer tailor-made managed security services through its CyberSOCs based in France and India.

Competitive Weaknesses

- Mobile security has proven to be a difficult nut to crack, but a recent partnerships with Atos/Bull could change that.
- Orange does not have a dedicated SOC in the Americas. It's not yet a priority region for Orange Cyberdefense, but weakens its otherwise robust geographic reach.

Current Perspective

Orange Business Services' managed security capabilities are strong, with services available in 160 countries supported by more than 1,000 security experts (including over 100 with CISSP certification) dedicated to client delivery and SOC operations located in six SOCs in France (2), Belgium (1), Mauritius (1), Egypt (1), and India (1) and two 'CyberSOCs' in France and India. The SOCs are populated by experts in security technologies who are in charge of managing the security infrastructure (e.g., equipment and applications), including operations and maintenance. CyberSOCs are staffed by security event experts who respond to and manage security events raised by IDS/IPS, APT protection, cyberwatch, vulnerability management, anti-DDoS and SIEM platforms. CyberSOCs alert customers, perform alert triage, analyze incidents, and advise and remediate when possible.

Orange was motivated at first to develop the CyberSOC approach to protect itself, including its brand image and its various compliance requirements. By adding intrusion detection systems, log analysis and anti-DDoS capabilities to existing security systems, it found it needed a new CyberSOC organization to handle ongoing management of new cyber threats against both itself and customers.

Orange Business Services rebranded its security business as Orange Cyberdefense in 2014, around the same time it announced the acquisition of security consultancy Atheos in France – adding to its stable of security consultants (and corporate clients). With the Atheos acquisition and that company's focus on consulting and governance, Orange put itself in a better position to win business from non-Orange clients. In April 2016, Orange acquired Lexsi, which provides services in the fields of audit, consultancy, incident response and cybersecurity training to more than 400 active customers in Europe and employs more than 170 experts.

Orange Cyberdefense articulates its strategy around four pillars, leveraging its consulting, integration services and security services skills: 1) design customers' cyber defense strategies; 2) strengthen, protect and control sensitive assets; 3) understand enterprise weaknesses and manage efficiency of cyber defense solutions; 4) monitor, alert, advise and remediate. Orange Business Services has strong competencies and experience in governance, risk and compliance (GRC) including penetration testing and in PCI DSS compliance, with a long list of clients in financial services. The company has been somewhat successful in targeting security opportunities outside of its typical global WAN clients, with global managed firewall services in particular, but the traditional installed base still accounts for up to 80% of security service revenues.

Orange offers automated vulnerability testing using Qualys, either in standard or sovereign mode, as well as manual penetration testing. Changes via the customer portal (My Service Space) are performed in a 'three eyes' (requester-SOC-requester's superior), ITIL-compliant and ISO 20000-certified manner in line with corporate security policies, and patches are applied based on real-time patch monitoring and the perceived threat to customer applications. Content security services include the network-based Web Protection Suite (the secure web cloud service powered by Zscaler), as well as appliancebased Managed Web Security solutions. Through its Security Manager portal, customers have a single, proactive point of contact.

Orange's secure authentication service leverages Gemalto solutions to authenticate individuals with soft tokens. Device authentication using web tokens is transparent to the end users and linked with the device in parallel. The service supports SAML v2 technology to provide secure authentication to cloud services, linking with a customer's corporate directory in real time. Multifactor authentication single sign-on and federated cloud identity capabilities comprise part of the Flexible Identity service launched in 2013. The approach to unified threat management runs from customer-managed, integrated security services to fully managed Orange Business Services offerings with highavailability SLAs managed via optional Spot Spare appliances. SIEM services using HPE ArcSight and IBM QRadar are tiered from Basic Services (with self-reporting) to Enhanced Services (with regular analysis of logs, etc.) to Expert Service (with real-time monitoring). Traction in SIEM is growing, with clients finding value in it based on the protection it provides business IP. Orange

has identified dozens of use cases supporting its SIEM clients, including a big focus on network protection (including DDoS) and compliance. DDoS protection delivers service levels of near real-time to 30 minutes from alert to intervention. The fully managed service protects any IP in a data center using scrubbing centers utilizing three types of anti-DDoS features: clean pipe, including blackhole, BGP flowspec and clean pipe technology on Arbor Networks and Juniper routers; web guardian, protecting web applications in CDN-based environments on Akamai or an Orange managed device; and site guardian, which protects any IP in a data center using an on-premises solution based on Arbor Networks technology. IPsec data encryption is enhanced with bespoke solutions for sensitive customers from Bull Group. Secure remote access solutions are offered jointly with Juniper both as managed service and in a SaaS model (Flexible SSL) based on Pulse Secure virtual appliances and a backend infrastructure fully developed by Orange. The Orange Web Protection Suite solution (based on Zscaler) provides both URL filtering and antivirus for mobile users when browsing the Internet.

Strengths and Weaknesses

Strengths	Weaknesses
• Orange has hard-to-match global presence (including partners) across 220 countries and six SOCs based in Europe, Africa and India plus two 'CyberSOCs' for threat intelligence – one in Europe and one in APAC (fully owned). As such, Orange Business Services has a very mature global presence to support customer installations on the ground. This regional and local field presence (166 countries directly operated by the Orange team, 220 with partners) ties into the global Orange follow-the-sun support capability complemented by a very strong security consulting team. • Orange Business Services has combined high-value services (managed, implemented, hosted) with increasingly flexible pricing and availability of its portfolio. New services across all areas of the portfolio, from security governance to identity-as-aservice and security operations, have been launched in the last two years, helping to win new customers and generate organic revenue growth in the double digits.	• Despite the acquisitions of Atheos and Lexsi, the Orange Cyberdefense business unit done limited marketing and announced few portfolio enhancements over the last year. • Mobile security has proven to be a difficult nut to crack, with many customers balking at paying separately for the security component of a mobile device management solution. As such, Orange Business Services has bundled security with MDM, relying on its MobileIron partnership. A Mobile Workspace solution with embedded content and device security has improved its value proposition, and a partnership with Atos/Bull now makes the latter's highly secure Hoox smartphone available. • Orange Business Services lacks a dedicated SOC in the Americas. The company says the region is not a key market in its current strategy, but the gap nevertheless weakens its otherwise strong position in terms of global presence.

• The provider has well-established global security consulting and security assessment capabilities and services, including GRC, threat assessments and penetration testing, and PCI DSS expertise, giving it strong credibility as an advisory partner for enterprises performing security audits, developing security policies and working through regulatory compliance issues. Coupled with its operational services and support, it can offer an end-to-end capability from advice to evaluation to implementation and control of security processes. • Orange Business Services is ahead of some of its peers in terms of cloud security. Its services have leveraged the cloud to evolve beyond the traditional managed security services approach, delivering Security-as-a- Service with pay-per-use options among other cloud-enabled consumption models. Flexible SSL, Flexible Identity, Security Event Intelligence services, and Cyber Risk & Compliance Intelligence are delivered via the Orange cloud, while Messaging Protection and Web Protection are delivered via external (public, partner) clouds. • Orange Business Services' Flexible Identity solution provides two levels of authentication and identity federation for policy enforcement. Its multi-factor authentication service leverages the customer's existing identity infrastructure, supports a wide range of apps and allows automatic end-user provisioning with access to cloud-based apps centrally managed. Identity federation also provides a central point of audit and compliance, which helps simplify the end-user experience. • Orange Business Services offers tailor-made managed security services through its SOCs based in France and Belgium. Employing only EU and NATOcleared personnel and being ISO27K certified, this SOC offers the flexibility and guarantees that very demanding customers expect. In particular, healthcare companies and other organization adhering to strict data privacy regulations can benefit from this offering.	

Metrics

Security Services Scope & Availability

Service geographic availability - global regions/number of countries and number of billable Security Professionals	All Orange Business Services managed security services available in 160 countries with over 1,000 security experts including over 100 CISSPcertified security consultants on five continents
Network Coverage for M2M	6 SOCs located in France (Rennes, Paris), Belgium (Brussels), India (Delhi), Egypt (Cairo) and Mauritius. 2 CyberSOCs located in France (Rennes) and India (Delhi).

Service Packages/Support Guarantees

Service geographic availability - global regions/number of countries and number of billable Security Professionals	All Orange Business Services managed security services available in 160 countries with over 1,000 security experts including over 100 CISSPcertified security consultants on five continents
Number and Location of SOCs	6 SOCs located in France (Rennes, Paris), Belgium (Brussels), India (Delhi), Egypt (Cairo) and Mauritius. 2 CyberSOCs located in France (Rennes) and India (Delhi).
SIM Options	Standard 2FF/3FF, Reinforced 2FF/3FF, MFF1, MFF2 (VQFN8-like) proposed in consumer, industrial, automotive versions. Embedded SIM (EUICC) includes GSMA standards for remote profile management.

Service Packages/Support Guarantees

Customer Service levels & features	Security Manager is a contractual allocation of a single proactive point of contact fully dedicated per client. OBS also has SLAs such as maximum time for recovery, maximum time for change (FW), time to alert (for security events) and time to mitigate (anti- DDoS).
Portal Features	The customer portal provides: usage reporting; policy configuration; change management for some services; realtime change management with remote access SaaS service (Flexible SSL); service configuration view; health reporting and feature provisioning for some services.

SLAs	Guaranteed max time of change (max 24 hours) for rules update, no limit of changes. For Managed UTM, high availability (on Spot Spare Appliance - as an option); for others, max time of action (granular), time to alert (for security events) and time to mitigate (anti-DDoS).

Security Assessment and Auditing Services

GRC	Orange Business Services provides GRC services through Security Consultants and its Security Manager resources. The provider offers Intelligence Threat Analysis based on government-grade experience. For compliance, Orange Business Services combines consulting for compliance process management + audit + pentesting.
Security Audits	Yes through Security Consultants addressing ISO9001, ISO20000, ISO27001/02, SAS 70, common criteria and NATO certification
Vulnerability Assessment Services	Yes, delivered through Security Consultants and Security Manager. A vulnerability scan service is available by OBS. It is based on a Qualys solution which is fully hosted in an Orange data center. Pentesters are dedicated to a manual or tailored approach. Orange also has also a vulnerability watch service called 'Vigil@nce.'

Authentication and Encryption Services

Identity and Access Management	The Orange Business Services secure authentication service has been extended to supporting both ActivIdentity and Cryptocard solutions. With these solutions, Orange Business Services can: 1) Authenticate individuals with various authenticators like software tokens (on PC or mobile devices), grid card or hardware tokens; 2) Authenticate devices with web tokens transparently for the end users and linked with the device itself (after an enrollment phase). In parallel, Orange Business Services extended its service to SAML v2 technology to provide secure authentication also to cloud services. The secure authentication service links with customer's corporate directory reflecting any change in the user account status (locked or disabled) in real time. Orange has also partnered with Morpho to access its digital identity and biometric solutions.
Encryption Services	Encryption services are provided in three ways: embedded in OBS' routers, dedicated boxes such as FW for IPsec, and dedicated services for SSL VPN (dedicated boxes or cloud based). In addition, OBS offers some bespoke solutions for sensitive customers based on Certes (Cipheroptics) or NetAsq technology

Monitoring and Event Management

Monitoring and Alert Services	Two kinds of monitoring and alerts are offered: health check and real time reporting, and security monitoring via IPS, SIEM, anti-DDoS, anti-APT and threat intelligence services. Alerting is delivered in near real time and reporting is included in the service.
Security Incident and Event Management (SIEM) solution	Services supported by the CyberSOCs include: IDS/IPS, SIEM, anti-DDoS, anti-APT and threat intelligence, with real-time, 24*7 monitoring and alerting. ArcSight and IBM QRadar are the current technologies used. In Belgium, Orange Business Services offers a SIEM monitoring service in a 'full flexible' mode based on HPE ArcSight technology, which monitors approximately dozens of customers, mainly in Europe. Orange is working to provide threat intelligence features to customers. The technology is still under evaluation and will be supported by the CyberSOC. Orange has developed a large threat intelligence database coming from more than 300 sources thanks to the Orange Labs (R&D). This database feeds SIEM services. Some other services may be used; it is still a work in progress. Orange provides an anti-APT (advanced persistent threat) service based on Trend Micro technology. This service may be proposed according to customer expectations: from an integrated delivery model to a full managed service model. Orange is working on providing an online sandbox that will be proposed for free to any Orange customers in order to let users test files. The sandbox is based on Orange Labs developments. Orange has its own epidemiological and signal intelligence laboratory in order to track malware, APT, AVT; this feeds the Orange threat intelligence database by providing new intelligence feeds (URL, domain, IPs), IOC and alerts about planned DDoS.

Threat Management and Content Security

Intrusion Detection/ Intrusion Protection	Juniper (SSL VPN), Check Point (nextgen FW), Fortinet (next-gen, UTM), Palo Alto (next-gen FW), Zscaler (web content filtering), BlueCoat (web content filtering), RSA (two-factor authentication), ArcSight (SIEM), and IBM QRadar (SIEM)
Managed Firewall Services	Yes, Orange Business Services can assist customers in defining the right policy driven by business requirements. For user groups, application control and web filtering are available using Check Point, while next-generation solutions are delivered with Fortinet and Palo Alto.
Unified Threat Management (UTM)	Yes, based on Fortinet, Cisco, NetAsq and Juniper.
Clean Pipes	Yes, network based service in partnership with Arbor Networks. This fully managed service proposes a complete clean pipes approach rather than only blackholing.

Distributed Denial of Service (DDoS) Mitigation	Orange Business Services' DDoS protection is articulated around three types of solutions to protect web applications only, global data centers using scrubbing centers, or through an on-premises device. Orange has developed an end-to-end approach for its DDoS Protection services from the business risks to complete mitigation of DDoS. DDoS Protection provides several levels of reactivity from 30 minutes after alert to near real time. The service is supported by the CyberSOC that is fed by an internal epidemiologic lab in order to prevent against some volumetric DDoS. Orange has also added a proactive mode to the reactive mode.
Endpoint Protection Services	Remote access solutions were launched jointly with Juniper both as managed service and in a SaaS model (Flexible SSL). The solutions are based on Pulse Secure virtual appliances and a backend infrastructure fully developed by Orange Business Services. The Orange Business Services Web Protection Suite solution (based on Zscaler) provides both URL filtering and antivirus solution for mobile users when browsing the Internet.
Data Leakage Protection	Yes, network based through Web Protection Suite (its secured web clouding service powered by Zscaler), or based on a bespoke solution through Managed Web Security, or using an appliance-based solution through Managed Firewall Check Point
Key Technology Vendor Partners	Juniper (FW, SSL VPN), McAfee (IPS), Check Point (FW), Fortinet (UTM), Zscaler (web content filtering), Sophos (mail content filtering), Qualys (vulnerability management), BlueCoat (web content filtering), SafeNet, Symantec (IAM), ArcSight (SIEM) and IBM QRadar (SIEM). Additional partners include TrendMicro (anti-APT), Arbor Networks (anti-DDoS), Akamai (anti-DDoS) and Orange Labs (innovations).

Cloud Security

Secure Access Cloud Services	Orange Business Services provides detailed answers to prospects and customer's regarding the security of its cloud services in order to detail what controls have been implemented. Orange Business Services accepts security audits from third parties only when performed by trusted third-party and when those audits don't jeopardize the security of the information or assets belonging to other's customers. Audit scope, content and involved parties are defined on a per-case basis and are subject to a formal agreement with the Chief Security Officer. In addition of providing clear answers to specific questions and security audits requests, Orange Business Services aims to include detailed statements regarding Information's security in all cloud computing services description. Vulnerability testing of the Orange Business Services cloud platforms is based on QualysGuard service, which provides high-level reports and requested by customers
Third party secure cloud access services	Orange Business Services can provide assistance to a customer wishing to interconnect to other cloud service providers. Orange Business Services provides both network-based firewall services with IAM and malware and URL filtering service. Via the Business- VPN Galerie service, Orange Business Services can provide private, direct and secure network interconnection with some public cloud providers.
Cloud Audit Trail Information	All end-users' actions on management systems are logged, analyzed and stored in a safe and secure way; the same applies for OBS administrators on systems and network equipment.
Cloud Security Standards Body Participation	CSA, DMTF, ETSI, ITU-T