GlobalData.

Orange Business Services Managed Security

September 29, 2017

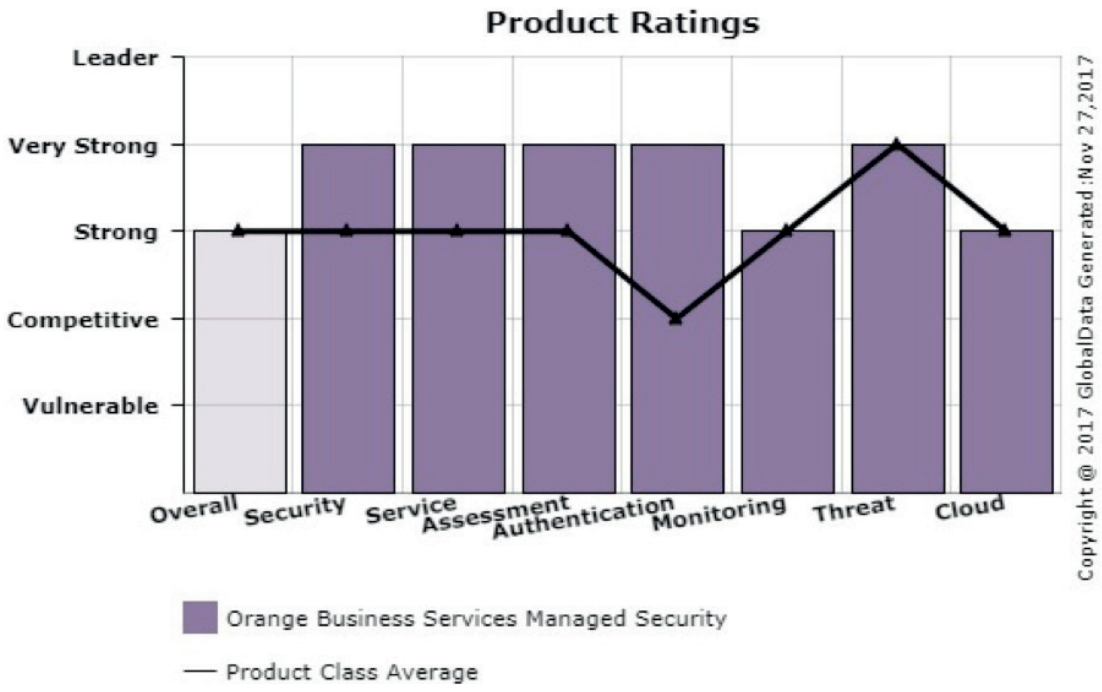
John Marcus

PRODUCT ASSESSMENT REPORT - MANAGED SECURITY SERVICES

REPORT SUMMARY

Orange Business Services has made its Flexible Security Platform available, while at the same time adding hundreds of additional dedicated human resources to its security practice.

SUMMARY



WHAT'S NEW

- **July 2017** - Added 150 security professionals in H1 2017, following the increase of 200 in 2016; part of plans to add 1,000 new dedicated personnel by 2020.
- **July 2017** - Flexible Security Platform available, providing all-in-one Internet gateway based on Fortinet next generation firewall running on a virtualized architecture in Orange data centers.
- **July 2017** - Ramp up of consulting-based solution portfolio for industrial control system security.

PRODUCT OVERVIEW

Product Name	Orange Cyberdefense
Description	Orange Cyberdefense is a business unit responsible for delivering a portfolio of IT and cyber security services for business and enterprise customers.
Components	• Flexible Security Platform • DDoS Protection • Web Protection Suite • Flexible SSL • Mobile SSL • Secure Gateway • Unified Defense • Threat Management Services
Key Customers	• AkzoNobel Packaging and Coatings • Belgium Federal Public Service • Siemens
Key Rivals	• AT&T • Atos • BT • Computacenter • Fujitsu • IBM • NTT • SecureWorks • T-Systems • Verizon

ESSENTIAL ANALYSIS

Strengths	• Based on revenues and resources, Orange Business Services is the market leader in France, with the scale necessary to compete for significant market shares beyond its home market. • Orange Business Services is not dependent on legacy resale; its partner-based solutions are integrated into managed and cloud-based services that don't require customer-owned CPE and the associated business model. • Orange Business Services has budget for security investment: both tactical (regional acquisitions), and strategic (internal R&D), strengthening its hand and keeping it on the offensive competitively.
Limitations	• Despite the global reach of Orange Business Services's networks supporting MNCs (and increasing Asia business), it lacks market recognition outside of France when it comes to security. • Strong in threat management, Orange Business Services has previously relied on Arcsight for SIEM; with the uncertainty around that platform, migration to IBM's QRadar is underway, potentially slowing momentum in the near-term. • Mobile security has been limited, treated as an add-on to mobile device management; plans for new mobile threat detection capabilities should improve the offer.

CURRENT PERSPECTIVE

STRONG

Orange Cyberdefense is demonstrating strong momentum following board-level commitment to security solutions, reflected by key acquisitions in recent years, aggressive plans for adding hundreds of security professionals, and providing the training and research and development required to reach and maintain its goal of market leadership in Europe. Two security academies and a new headquarters in Paris are being added to assets that include two CyberSOCs, seven SOCs, three CERTs, and three scrubbing centers around the world.

Momentum (27% revenue growth in Q2 2017) is aided by Orange Business Services's priority on bundling and integration of security features and services throughout its general portfolio. Rather than treat security as a silo, it is relevant to all business functions from Internet access, to user devices, to corporate and customer data. To avoid becoming a technology reseller, there is a commitment to develop a security add-on for every Orange product and service (i.e., communications or applications), and to include a managed/monitoring aspect with every core security offering. In doing so, Orange Business Services can demonstrate the value add that a service provider can offer, increasing customer stickiness and wallet share.

Looking ahead, Orange Business Services has a solid roadmap for its core network security offering-Flexible Security Platform based on Fortinet. Available now in France, future enhancements include appliance-based firewalls, as well as support for other regions and other vendor platforms in the delivery of universal CPE for any virtual network functions. Internally, Orange is developing new solutions for SMBs in France, and new technology around IPS for encrypted traffic. While its threat management and CyberSOC solutions are extensive, with multiple delivery models (SIEM as a service, dedicated SIEM, "sovereign" SIEM, etc.) and service levels, migration from Arcsight to QRadar as its core SIEM technology could impact short-term momentum. With the 2016 acquisition of Lexsi, however, Orange Business Services's incident response capabilities are very strong, with hack prevention, fraud prevention, and data leak and cyber surveillance capabilities that have proven themselves repeatedly, most recently with its robust defense against the global Petya malware crisis.

COMPETITIVE RECOMMENDATIONS

Provider

- **Regulated Opportunity:** The introduction of new regulations often present service providers with new business opportunities. GDPR implementation requires security specific advice, but Orange Business Services should design solutions that go beyond consulting to include ongoing regulatory compliance controls.
- **Computer Emergency Response Team (CERT) Strength:** Not all managed security service providers can demonstrate the assets and experience of Orange Business Services as a CERT in terms of breach mitigation. It should position them as marketing leading, highlighting especially the capabilities of its proprietary tools.
- **Network Advantage:** Due to its network ownership, Orange Business Services is in a good position to build up security intelligence capabilities, which can also be enriched through third-party data sources and other technologies such as AI/Machine Learning.

Competitors

- **Multinational Mindshare:** Competitors with global brands (e.g., IBM, etc.) can take advantage of the Orange Business Services' lack of mindshare outside of France in cyber security.
- **Chequebook Development:** While acknowledging its integration strengths, competitors can nonetheless characterize Orange Business Services as reliant on third-party acquisitions to grown its portfolio and pipeline.

Buyers

- **SIEM Shift:** Enterprises evaluating SIEM solutions should consider providers with deeper experience with QRadar than Orange Business Services, given its history with HPE ArcSight, which it is only migrating away from now.
- **Global Reach:** MNCs should note that Orange Business Services's global delivery capabilities far outreach its brand awareness; seven SOCs and more than 1,000 professional bring a uniform portfolio to more than 160 countries.

Metrics

SECURITY SERVICES SCOPE & AVAILABILITY

Rating	Very Strong
Service geographic availability - global regions/number of countries and number of billable Security Professionals	Most Orange Business Services managed security services available in 160 countries with over 1,000 security experts including over 100 CISSP-certified security consultants on five continents
Number and Location of SOCs	7 SOCs located in France (Rennes, Paris), Belgium (Brussels), India (Delhi), Egypt (Cairo) Malaysia, and Mauritius. 2 CyberSOCs located in France (Rennes) and India (Delhi). 3 CERTs in France, Canada, and Singapore. 3 scrubbing centers in France and the U.S. (with satellite scrubbing centers in Spain, Russia, Poland, Egypt, Jordan, Morocco, Tunisia, Ivory Coast, and Senegal).

SERVICE PACKAGES/SUPPORT GUARANTEES

Rating	Very Strong
Customer Service levels & features	Security Manager is a contractual allocation of a single proactive point of contact fully dedicated per client. Orange Business Services 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; real-time change management with remote access SaaS service (Flexible SSL); service configuration view; health reporting and feature provisioning for some services. Portal access is provided for CERT customers (Threat Defense Center and Vulnerability Watch portal). Flexible Security Platform offers the option of a dedicated customer portal enabling service design and ordering, with co-management features (content filtering settings, etc.) for flexible service delivery with customer control.
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

Rating	Very Strong
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. New audits available for IoT security, industrial control system security, and due diligence audits as part of CERT digital forensics.
Vulnerability Assessment Services	Yes, delivered through Security Consultants and Security Manager. A vulnerability scan service is available by Orange Business Services. 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

Rating	Very Strong
Encryption Services	Encryption services are provided in three ways: embedded in Orange Business Services' routers, dedicated boxes such as FW for IPsec, and dedicated services for SSL VPN (dedicated boxes or cloud based). In addition, Orange Business Services offers some bespoke solutions for sensitive customers based on Certes (Cipheroptics) or NetAsq technology. New services are planned to address mobile voice and data encryption for government sector, based on Android. Orange Business Services is also developing a solution for blind IPS for https: detection of malware in encrypted web traffic.
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.

MONITORING AND EVENT MANAGEMENT

Rating	Strong
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. Key vendors include QRadar, RSA, Splunk and ELK.
	Services supported by 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; QRadar will be the platform for the future. SIEM is available "as a service" or through a dedicated or sovereign platform.

Security Incident and Event Management (SIEM) solution	Orange Labs has developed a large threat intelligence database coming from more than 400 sources. This database uses a patented correlation engine and feeds SIEM services. Orange provides an anti-APT (advanced persistent threat) service based on Trend Micro technology, ranging from an integrated delivery model to a full managed service model.Orange is working on providing an online sandbox, based on Orange Labs developments, available for free to any Orange customers in order to let users test files. Orange has its own epidemiological and signal intelligence laboratory for tracking malware, APT, AVT; this feeds the Orange threat intelligence database.

THREAT MANAGEMENT AND CONTENT SECURITY

Rating	Very Strong
Intrusion Detection/ Intrusion Protection	Juniper (SSL VPN), Check Point (next-gen 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.Flexible Security Platform is the Fortinet-based next generation firewall and all-in-one Internet gateway, delivering cloud-based firewall for inbound/outbound traffic and on-demand access to advanced security features. Usage-based pricing is offered according to bandwidth levels.
Unified Threat Management (UTM)	Yes, based on Fortinet, Cisco, NetAsq and Juniper.
Clean Pipes	Yes, SaaS 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. Orange has three major scrubbing centers around the world and nine satellite centers, with total DDoS mitigation capacity of 2.8 Tbps. Key vendors include Arbor and Akamai.

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 (FW, 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

Rating	Strong
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 Orange Business Services administrators on systems and network equipment.

Cloud Security Standards Body Participation	CSA, DMTF, ETSI, ITU-T

GlobalData PLC, John Carpenter House, 7 Carmelite Street, London, EC4Y 0AN,
+44 (0) 207 936 6400