Orange Cyberdefense Managed Security

May 14, 2020

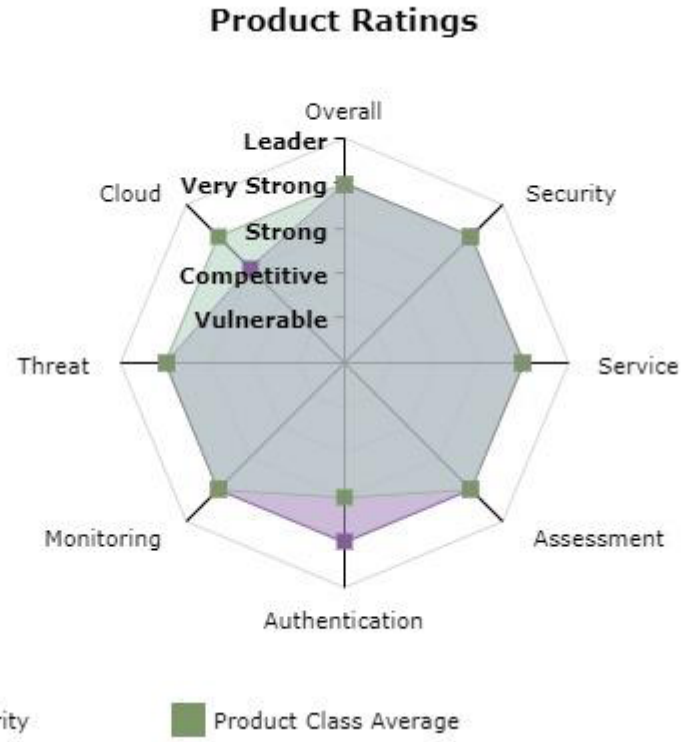
Larsen DeCarlo, Amy

PRODUCT ASSESSMENT REPORT - GLOBAL MANAGED SECURITY SERVICES

REPORT SUMMARY

Orange Cyberdefense is primed to support clients facing COVID-19 challenges across Europe and around the world. With the assets from its SecureData and SecureLink integrated into the fold, Orange has a deeper bench from which to draw.

SUMMARY



WHAT'S NEW

- **February 2020:** Orange announced EUR 1.5 billion for staff training in its five-year strategy plan to strengthen expertise in the areas of AI, cloud computing, code, and cybersecurity.
- **October 2019:** During European Cyber Security Month, Orange highlighted that thousands of Europeans fall victim to cyberattacks every year and the only way to fight cybercrime is by preventing it and aims to raise public and business awareness of cyber and phishing risks.
- **July 2019:** Orange Business Services has completed the acquisition of SecureLink, a leading independent cybersecurity player in Europe, for EUR 515 million.

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 the Orange group, including for business and enterprise customers.
Components	• Flexible Security Platform • DDoS Protection • Web Protection Suite • Flexible SSL • Mobile SSL • Secure Gateway • Threat Management Services • Flexible Identity • Consulting/Audit/Compliance Professional Services • Technical Audit/Penetrating Testing • Vulnerability Management • Security Incident and Event Management (SIEM) • Threat Intelligence Services • Incident response services • Email Protection Suite • Mobile Threat Protection

Key Customers	• AkzoNobel Packaging and Coatings • Belgium Federal Public Service • CERT NZ • Siemens	
Key Rivals	• AT&T • Atos • BT • Computacenter • Fujitsu	• IBM • SecureWorks • T-Systems • Thales • Verizon

ESSENTIAL ANALYSIS

Strengths

- Based on revenues and resources, Orange Cyberdefense is the market leader in France, with the scale necessary to compete for significant market shares beyond its home market.
- Orange Cyberdefense 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 Cyberdefense is a group-level business and has budget for 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' networks supporting MNCs (and increasing Asia business), it lacks strong brand awareness in key markets including North America.
- Mobile security has been limited, treated as an add-on to mobile device management; a mobile threat detection offer based on Check Point SandBlast has improved its position.

CURRENT PERSPECTIVE

VERY STRONG

Orange Cyberdefense is very strong in managed security, proving adept at developing its portfolio of solutions and adding the resources that drive them. For example, it has been fast in moving from proof of concept to roll out for key SIEM/SOC/machine learning-based solutions, due to the agile approach its Paris CyberSOC team is taking when integrating new technology. The business has capitalized on board-level commitment to gain investment in security solutions, and recently was restructured to report directly to the group level rather to Orange Business Services. With aggressive plans underway in acquisitions, adding a thousand more security professionals, in training, and in research and development, the business is growing at a rapid rate annually and has opportunities to extend its market leadership beyond France. Two security academies and a new headquarters in Paris have been added to assets that include ten CyberSOCs, 16 SOCs, and four CERTs.

Prior to 2017, most security services revenue was tied to network services contracts, including managed firewall, as well as cloud/application and mobile security. Since the formation of Orange Cyberdefense, revenue growth has been accompanied by a shift in the mix to include an equal amount of “pure play” security services sales (including threat monitoring, SIEM, and DDoS mitigation) independent of network contracts. The company says this is not due to increased marketing investment, but rather growing customer demand and its sales team’s ability to demonstrate value across the portfolio. As a result, the number of CyberSOC customers continues to grow rapidly.

With 3,700 MNC and UK and France-based enterprise customers, Orange Cyberdefense’s service revenues are among the largest for European telco operators competing in security. To keep growing faster than the market, it will need to continue investing in people and, potentially, more acquisitions. It will also have to end up on the positive side of the trend toward enterprises consolidating the number security suppliers they use, but for now, recent reports of winning customers away from competitors is contributing to the current healthy growth rate.

Bringing the portfolio to new segments is also underway. For example, the CyberSOC in Poland enables base-level services to a broader set of business customers, including SMEs and other enterprises that aren’t very advanced and don’t need high end solutions, but increasingly need to be compliant and have visibility over their security posture. With Orange Cyberdefense now a group-level business, more investment in its brand in France should also enhance its position in SOHO and--in the future--B2C segments. Internationally, additional SOCs are being considered in new regions around the world (a new SOC in Atlanta has opened, as well as a new security hub in Morocco to support customers in French-speaking countries), while increased marketing efforts are being put in place to provide visibility of Orange Cyberdefense’s security capabilities beyond the network.

COMPETITIVE RECOMMENDATIONS

Provider

- **Regulated Opportunity:** The introduction of regulations often present service providers with new business opportunities. GDPR implementation requires security specific advice, but Orange Cyberdefense should expand its range solutions that support ongoing regulatory compliance controls beyond consulting.
- **Computer Emergency Response Team (CERT) Strength:** Not all managed security service providers can demonstrate the assets and experience of Orange Cyberdefense as a CERT in terms of breach mitigation, especially when it comes to international scope with CERTS in France, Singapore, and Canada. It should position them as marketing leading, highlighting especially the capabilities of its proprietary tools.

- **Network Advantage:** Due to its network ownership, Orange Cyberdefense 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 Artificial Intelligence/Machine Learning (AI/ML). The company should demonstrate how AI/ML can be integrated into its own threat database to detect unknown threats, and into its multiple supported SIEM platforms. Plans to industrialize this and offer it as an embedded service should be clarified with customers.

Competitors

- **Multinational Mindshare:** While Orange is expanding its international presence and revenues, competitors with global brands (e.g., IBM, etc.) can take advantage of the provider's more limited cybersecurity brand recognition outside of Europe.
- **Checkbook Development:** While acknowledging its integration strengths, competitors can nonetheless characterize Orange Cyberdefense as reliant on third-party acquisitions to grow its portfolio and pipeline.

Competitors

- **Multinational Mindshare:** While Orange is expanding its international presence and revenues, competitors with global brands (e.g., IBM, etc.) can take advantage of the provider's more limited cybersecurity brand recognition outside of Europe.
- **Checkbook Development:** While acknowledging its integration strengths, competitors can nonetheless characterize Orange Cyberdefense as reliant on third-party acquisitions to grow its portfolio and pipeline.

Buyers

- **Global Reach:** MNCs should note that Orange Cyberdefense's global delivery capabilities far outreach its brand awareness; 16 SOCs, and more than 2,100 professionals bring a uniform portfolio to more than 220 countries and territories.
- **Value on Top:** In addition to being present around the world, Orange Cyberdefense has proven its ability to do much more than operate and maintain installed security platforms on the customer's behalf; by fine-tuning tools and adding value through CyberSOC analysis, it has succeeded in taking global customers away from established leaders.

Metrics

SECURITY SERVICES SCOPE & AVAILABILITY

Rating:	Very Strong
Service geographic availability - global regions/number of countries and number of billable Security Professionals:	Most Orange Cyberdefense managed security services available in 220 countries and territories with over 2,100 security experts including over 100 CISSP-certified security consultants on five continents. Sites in Malaysia and USA have enabled 24x7x365 Layer 2/3 support for global customers and an expansion of service management offerings.
Number and Location of SOCs:	Sixteen SOCs located in France, Belgium (Brussels), U.S., India, Egypt, the UK, the Netherlands, Germany, Sweden, Norway, China, Malaysia, Mauritius, and Poland. Four CyberSOCs located in France (Rennes, Paris), Poland, and India (Delhi). Ten CyberSOCs located in France (Rennes, Paris), Poland, and India (Gurgaon), Sweden (x2), China, Germany, UK, Netherlands.

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 Cyberdefense 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:	A single portal “My Service Space” undertakes all ITIL functions of ordering, change management, billing etc. and access to service-specific modules (e.g., Security Event Intelligence, the SIEM-based detection service powered by Orange’s CyberSOC, Flexible Security Platform, etc. to manage alerts, reporting, and related functions). 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. Mobile Threat Protection (MTP) solution (additional feature on top of Orange’s Mobile Device Management services) is also administered via a customer portal.
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 Cyberdefense 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 Cyberdefense 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 Cyberdefense. 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 a vulnerability service called 'Vulnerability Intelligence Watch' which is actually a threat intelligence service focused on vulnerability feeds customizable according to each customer's systems/OS/applications and other bespoke parameters. A re-launch is planned in Q1 2019.

AUTHENTICATION AND ENCRYPTION SERVICES

Rating:	Very Strong
Encryption Services:	Encryption services are provided in three ways: embedded in Orange Cyberdefense's routers, dedicated boxes such as FW for IPsec, and dedicated services for SSL VPN (dedicated boxes or cloud based). In addition, Orange Cyberdefense offers some bespoke solutions for sensitive customers based on Certes (Cipheroptics) or NetAsq technology. It also offers services for mobile voice and data encryption for the government sector, based on Android and iOS called Mobile Security Intense. Orange Cyberdefense is also developing a solution for blind IPS for https: detection of malware in encrypted web traffic.
Identity and Access Management:	The Orange Cyberdefense secure authentication service has been extended to supporting both ActivIdentity and Cryptocard solutions. With these solutions, Orange Cyberdefense 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 Cyberdefense 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. Orange also offers xDR monitoring services backed by the CyberSOC. Vendors for these services include Cybereason and Vectra.
Security Incident and Event Management (SIEM) solution:	Services supported by CyberSOCs include: IDS/IPS, SIEM, anti-DDoS, anti-APT and threat intelligence, with real-time, 24*7 monitoring and alerting. HPE ArcSight is being phased out, while IBM QRadar, Splunk, and ELK platforms are now fully supported. SIEM is available “as a service” or through a dedicated or sovereign platform. Orange Labs has developed a large threat intelligence database coming from more than 600 sources, public and private (and some exclusive to Orange such as signal intelligence and malware analysis from its lab and CERT, from its global backbone, and from threats to the Orange Group and affiliates). A recent agreement with Europol is a proof point of the quality and uniqueness of the database, which Orange CyberDefense is launching as an XaaS offering from Q1 this year. 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 provides an online sandbox, based on Orange Labs developments, which customers can use to 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:	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), Splunk, ELK, and IBM QRadar (SIEM)
Managed Firewall Services:	Yes, Orange Cyberdefense 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 fully-managed next-generation solutions are delivered with Check Point, Fortinet, or 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):	Fortinet, Cisco, NetAsq, and Juniper-based offers are being replaced by Orange Cybderdefense's Flexible Security Platform and Secure Gateway solutions.
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 Cyberdefense' 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 Cyberdefense. The Orange Cyberdefense Web Protection Suite solution (based on Zscaler) provides both URL filtering and antivirus solution for mobile users when browsing the Internet. Orange also offers Mobile Threat Protection, an endpoint managed security services for mobile devices based on Checkpoint Sandblast technology.
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 (firewall and mobile protection), Fortinet (FW, UTM), Zscaler (web content filtering), Sophos (mail content filtering), Qualys (vulnerability management), BlueCoat (web content filtering), SafeNet, Symantec (IAM), IBM QRadar, Splunk, and ELK (SIEM). Additional partners include TrendMicro (anti-APT), Arbor Networks (anti-DDoS), Akamai (anti-DDoS), SEC-BI (a start-up Orange invested in) which provides AI/ML based detection to power its Cyber SOC as well as integrated solutions, Vectra Networks and Alsid (active directory security), and Orange Labs (innovations).

CLOUD SECURITY

Rating:	Strong
Secure Access Cloud Services:	Orange Cyberdefense 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 Cyberdefense 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 Cyberdefense aims to include detailed statements regarding Information's security in all cloud computing services description. Vulnerability testing of the Orange Cyberdefense cloud platforms is based on QualysGuard service, which provides high-level reports and requested by customers.
Third party secure cloud access services:	Orange Cyberdefense can provide assistance to a customer wishing to interconnect to other cloud service providers. Orange Cyberdefense provides both network-based firewall services with IAM and malware and URL filtering service. Via the Business-VPN Galerie service, Orange Cyberdefense 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 Cyberdefense administrators on systems and network equipment.
Cloud Security Standards Body Participation:	CSA, DMTF, ETSI, ITU-T

© GlobalData 2020. John Carpenter House, 7 Carmelite Street, London EC4 0BS.