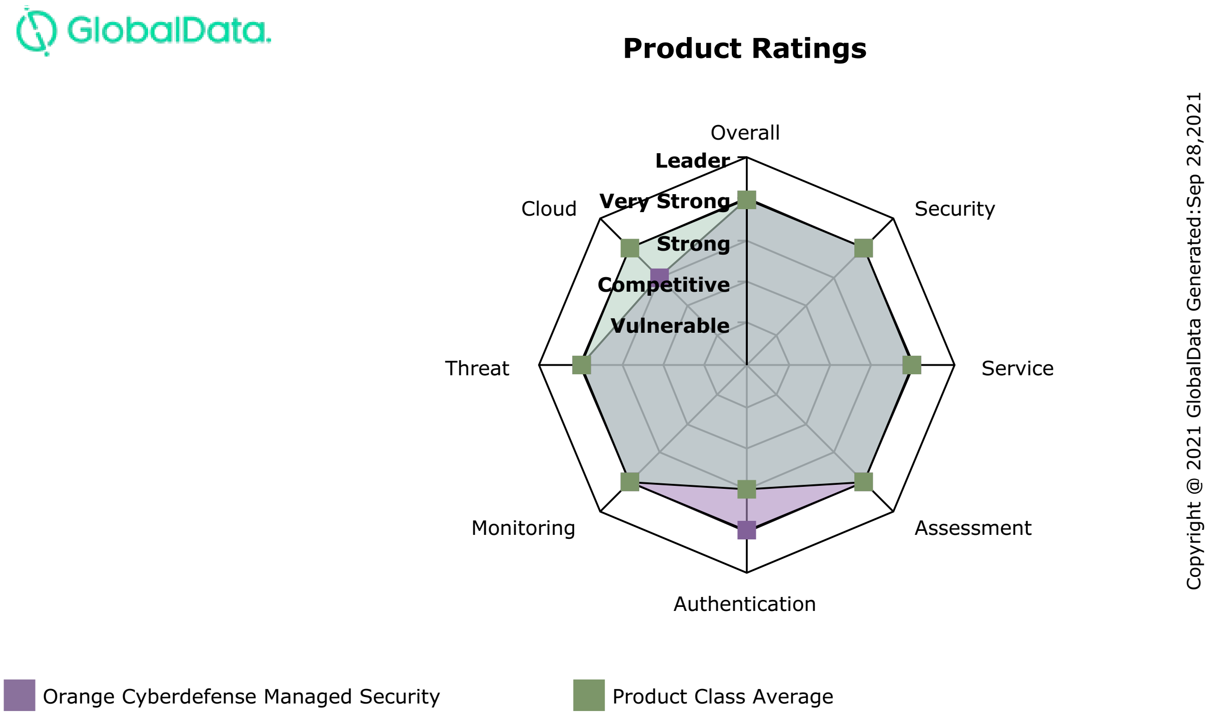
GlobalData.

Orange Cyberdefense Managed Security

Amy Larsen DeCarlo | September 28, 2021

Summary



What's New

- July 2021: During a conference, Orange laid out its strategic growth plans, during which it highlighted the work it is doing to expand its cyber defense business. Orange is looking to achieve double-digital revenue growth for Orange Cyberdefense.

- July 2021: Orange selected Palo Alto Networks' Prisma Cloud security platform as its cloud security solution. Orange will use Prisma Cloud's Cloud Security Posture Management (CSPM) features for multi-cloud compliance and governance. The operator will also tap Prisma Cloud's Cloud Workload Protection (CWP) features for securing hosts and containerized applications.

- June 2021: At MWC 2021, Orange demonstrated a couple of new offerings including IoT SAFE (SIM Applet For Secure End-2-End Communication), a new standard specified by the GSMA and Trusted Connectivity Alliance (TCA). IoT SAFE uses the eSIM as a key store to hold cryptographic keys and services to protect against physical attacks. Other offerings include: Cyberfiltre, to protect all kind of devices that are using the Orange network from diverse cyber threats; and Malware Cleaner, a solution proposed in different form factors that analyze with eight anti-virus USB devices, computers, and mobile devices.

Product Overview

Product Name	Orange Cyberdefense

Description	Orange Cyberdefense is a business unit responsible for delivering a portfolio of IT and cybersecurity services for the Orange group, including for business and enterprise customers.
Components	• Managed Security Services/Managed Vulnerability Intelligence – Watch, Identify, Protect • MSS/Threat Intelligence Services (World Watch, Managed Threat Intelligence) – Detect, Protect, Discover • PSS/Consulting, Advisory, Compliance Services (Strategy, Audit, Technology, IT, and OT) • PSS/Ethical Hacking Services (including Penetration Testing) • MSS/Secure Infrastructure Services (including: Managed NG Firewall, Managed Secure Web Gateway, Managed Email Protection, Managed DDoS Protection) • Endpoint and Mobile Security • Identity and Access Management • OT and IoT Security • MSS/MDR/Managed Detection & Response Services • Managed Threat Detection (Endpoint, Network, Log/SIEM) • Managed Monitored Cybercrime Services • Managed Threat Response (Isolation, Takedown) • Incident Response Services (Retainer and Emergency) • Compromise Assessment • Incident Response Consulting • Digital Forensics • Malware Cleaner
Key Customers	• AkzoNobel Packaging and Coatings • Belgium Federal Public Service • CERT NZ • Siemens • Luka • Mars
Key Rivals	• AT&T • Atos • BT • Computacenter • Fujitsu • IBM • Secureworks • T-Systems • Thales • Verizon

Essential Analysis

Strengths

• Orange has one of the more extensive security services portfolios in the world and a deep bench of other resources from which to draw. Among these is one of the world's largest ethical hacking teams

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.

with more than 150 experts.

- Based on revenues and resources, Orange Cyberdefense is the market leader in France, with the scale necessary to support clients far outside its home market. Orange has a CyberSOC in China that provides support for Western organizations with a presence in the country.

- Orange Cyberdefense takes an intelligence-led approach, embedding proprietary intellectual property and links to external intelligence sources into all solutions. Multi-security services capability, especially MSS+MDR, offers customers the ability to consolidate outsourcing under a single provider, resulting in better value and security outcomes.

- 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.

- 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.

- Some services are limited to certain geographies. For example, Orange announced the launch of a malware cleaner in France and South Africa that will add a layer of reassurance preventing malware traversing from USB devices and Android mobile phones into internal networks, but the solution is only being released in those countries and ad hoc in the rest of Europe.

Current Perspective

VERY STRONG

Orange Cyberdefense is very strong in cybersecurity, 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 rollout for key SIEM/SOC/machine learning-based solutions. All of its CyberSOCs now use a combination of ML/AI-based solutions in conjunction with internally developed tools and techniques such as pattern-based analysis and further qualification and targeted remediation supported through proprietary intelligence. The business has capitalized on board-level commitment to gain investment in security solutions, and it was restructured to report directly to the group level rather than to Orange Business Services. 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 11 CyberSOCs, 17 SOCs, four CERTs, and four scrubbing centers to mitigate DDoS attacks.

Prior to 2017, most security services revenue was tied to network and infrastructure 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 managed detection and response services leveraging SIEM, endpoint [mEDR], and network [mNDR/mXDR]) independent of network contracts. The company says this is not only 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 8,000 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 are contributing to the current healthy growth rate.

Bringing the portfolio to new segments is also underway, with Orange Cyberdefense reporting significant growth in key areas. For example, the mEDR solution, which is targeted to the midmarket in France, posted 5x growth in 2020. With Orange Cyberdefense now a group-level business, more investment in its brand in France should also enhance its position outside France and – in the future – B2C segments. Internationally, additional SOCs are being considered in new regions around the world (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 presents service providers with new business opportunities. GDPR implementation requires security-specific advice, but Orange Cyberdefense should expand its range of 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 market 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.

Buyers

- Global Reach: MNCs should note that Orange Cyberdefense's global delivery capabilities far outreach its brand awareness; 17 SOCs and more than 2,500 professionals bring a uniform portfolio to more than 160 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 160 countries and territories with over 2,500 security experts including over 100 CISSP-certified security consultants on five continents. Sites in Malaysia and the U.S. have enabled 24x7x365 Layer 2/3 support for global customers and an expansion of service management offerings.
Number and Location of SOCs	Seventeen SOCs located in France, Belgium (Brussels), Denmark, the 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). Eleven CyberSOCs located in France (Rennes, Paris), Poland, India (Gurgaon), Sweden (x2), China, Germany, the UK, Russia, and the 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. A new portal is being launched in Q2 2021, featuring a one-stop shop for all cybersecurity services, more dynamic and proactive capabilities, and integration with the SOAR platform.
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. Orange Cyberdefense has one of the largest pentesting teams with 150 experts. These are the same experts that are widely recognized and present at DEFCON and BlackHat. Services now available worldwide, enhancing the previous portfolio.
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, based on a Qualys solution, is fully hosted in an Orange data center. The service is going through a new evolution this year combining 'watch, identify, and protect' for faster, more targeted patch management based on threats and vulnerabilities relevant to each customer's context.

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; and 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 the 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	Very 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, Splunk, and ELK. Orange also offers xDR monitoring services backed by the CyberSOC. Vendors for these services include Palo Alto (XDR Cortex), 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. This database uses a patented correlation engine and feeds SIEM services. Orange provides an anti-advanced persistent threat (APT) 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 Epidemology Lab and Security Research Center for tracking malware, APT, and 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), Thales (multi-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 and Juniper-based offers are being replaced by Orange Cyberdefense'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	Orange offers Mobile Threat Protection, an endpoint managed security services for mobile devices based on Check Point SandBlast technology. Other notable managed EPP services: protection (based on Cylance) and EDR (based on Cybereason).
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	McAfee (IPS), Check Point (firewall and mobile protection), Fortinet (FW, UTM), Zscaler (web content filtering), Proofpoint (email filtering); Vade (email filtering), Qualys (vulnerability management), BlueCoat (web content filtering), SafeNet, IBM QRadar, Splunk, and ELK (SIEM). Additional partners include TrendMicro (anti-APT), Arbor Networks (anti-DDoS), Akamai (anti-DDoS), SEC-BI (a startup 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). Other key vendors include F5, Cybereason, and Vectra.

Cloud Security

Rating	Strong
Secure Access Cloud Services	Orange Cyberdefense’s approach has evolved to focus on zero-trust architecture and a SASE methodology. This approach allows organizations to route traffic securely to the cloud from any location rather sending it back to the data center. Orange offers consultative and managed services to support client security transformations.
Third party secure cloud access services	Orange Cyberdefense can provide secure cloud connectivity and security management to AWS, Microsoft Azure, and Google through its Managed Cloud Security Infrastructure (MCSI) solution. MCSI incorporates advanced threat detection, compliance checking, proactive monitoring for configuration vulnerabilities, and ongoing monitoring.
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