Press Kit
Orange Business Services

Orange Business Services helps companies solve their most pressing e-security challenges

Press Contact:
Gwenaëlle Martin-Delfosse, gwenaelle.martindelfosse@orange.com
Ghislain Garesse, Ghislain.Garesse@bm.com
Contents

Introduction

I. Emerging Security & IT Challenges

II. Orange Business Services: a 360° Market Approach

III. A Unique Portfolio

Links & Graphics
**introduction**

Security has become a **major business challenge** for corporations. In an increasingly competitive environment, customer data and identities are a vital asset for enterprises and deserve advanced protection. "Traditional" threats (intrusions, data loss, etc.) remained simple, pervasive, and identified; companies face today a new type of highly sophisticated, focused, and silent threat - not only targeting IT infrastructures, but also users’ mobile devices and terminals.

With the emergence of new types of applications and working environments, a more complex regulatory environment, and the accelerated development of cloud technologies, CIOs face new challenges to secure an **extended and opened perimeter**.

Recognized as a key player on the market of security services, Orange Business Services provides companies expert security services to develop security policies aligned with these new threats and challenges.

With a growth rate of its security revenues above market in 2012, Orange Business Services confirms its growth expectations on this market - a major pillar of its Conquests 2015 Strategic Growth Plan.

Orange Business Services’ unique expertise in the field of security is supported by robust network infrastructures, dedicated teams of security experts, Security Operations Centers (SOC), a CyberSOC and the know-how of its partners. Orange Business Services has a **comprehensive and integrated security approach** and provides a full range of solutions covering networks, infrastructures, terminals, and data in 220 countries and territories. To prevent and monitor emerging risks and e-crime attempts, Orange Business Services implemented an active innovation and partnership strategy to reinforce its portfolio of managed services with consulting, monitoring, and governance solutions and services.

---

1 Gartner - Marketscope for managed security services in Europe Gartner October 2012
2 Pierre Audoin Consultants « Survey on IT Security in France » 2013
Facts & Figures

unequaled dedicated resources
- 15 Orange Labs on four continents
- 1 Cyber Security Operation Center (CyberSOC) and 8 SOCs around the world
- More than 1,000 security experts including 350 dedicated corporate consultants
- The widest seamless IP network in the world, with more than 30,000 km
- Managed security services available in 220 countries and territories

proven expertise
- 600 international organizations rely on Orange Business Services to manage dedicated security services
- 400,000 end-users of our remote access solutions
- More than 300,000 end-users of strong authentication solutions
- 10,000 dedicated security devices managed by Orange
I. Emerging Security & IT Challenges

Over the last decade, new types of technologies, devices, uses, and threats deeply impacted the IT security landscape. Today, security is a critical business challenge for most companies.

1 - The new paradigm of IT security

Over the last decade, corporate security challenges have radically evolved. While focused in the early 2000s around simple, viral or DoS (Denial of Service) attacks that could slow down their activities, IT security is now considered a major business requirement. Intrusions, data thefts, and advanced persistent threats (APT) are more sophisticated, targeted, and silent than ever and can cause direct losses of millions of dollars and irreparable damage to corporate reputation.

Furthermore, exchange globalization, pervasive open access channels (for customers, partners, suppliers, etc.), and infrastructure convergence require securing extended perimeters. Data are no longer an internal siloed resource but a shared asset -- increasing their vulnerability to thefts or attacks.

The "coverage perimeter" in itself has become more and more complex to master due to the increasing mobility of users. Mobile devices (smartphones, tablets, etc.) are now ubiquitous in corporate environments; connected to open networks, and storing sensitive corporate data, they represent a new challenge for data security experts. The emergence of BYOD (Bring Your Own Device) - mixing personal and professional uses - makes it even more difficult to prevent data leaks. According to a 2012 Gartner Survey, 60% of employees equipped with corporate smartphones also use it for personal purposes.

The exponential growth of data (Big Data) is also a challenge to protect corporate information. It is even more complex since such data is now shared on social platforms (social networks, collaboration tools, cloud). Monitoring data in motion has never been so challenging...

2 - CIO: at the convergence of security issues

The roles and responsibilities of CIOs and security experts have been deeply altered by the new positioning of IT security at the center of corporate strategies. According to a 2012 survey by Opinion Way, 81% of security managers believe that security policies will gain strategic

---

3 Corporate Security Managers & Cyberthreats / for CDSE CDSE (Club des Directeurs de Sécurité des entreprises), Opinion Way, 12/07/2012
importance and 92% believe that digital risk management has positive effects on competitiveness.

While their role was mostly focused on team management, CIOs are now facing critical issues changing their scope of responsibilities.

According to Nicolas Furgé, Security Services Division Manager, Orange Business Services, a valid protection of information systems also improves productivity:

"All companies must protect their network environments for productivity purposes. They must ensure that their IT systems always remain safe and protect data privacy." However, according to the Opinion Way survey, 87% of respondents believe that French companies are not adequately equipped.

Among these new challenges, the "consumerization and commoditization of experience" plays a critical role. End-users can actually access any information system with any mobile device (tablet, smartphone, etc.) and any workstation. In this context, new questions arise: Who is this user? How can he/she be authenticated? How secure is the connection? Answers to such questions and implementation of relevant solutions are under the responsibility of a new generation of security managers and CIOs.

With the emergence of cloud computing, corporate security experts have to manage next-generation challenges. More specifically, cloud computing requires protecting data hosted outside the physical perimeter of enterprises. For Nicolas Furgé "Cloud and security are closely related; companies require efficient new generation security solutions." Once again, this new paradigm raises many questions: How do we secure cloud accesses and data exchanges? How do we validate users’ credentials and authorizations? In other words, cloud computing multiplies identities and data challenges, while the proliferation of digital media connected to enterprise data creates an even more complex landscape.

Finally, companies are increasingly subject to security standards and regulations requiring precise processes and workflows, including the ISO 27000 Standard on Information Security Management, PCI DSS for credit card payments and data privacy, etc. In this context of opened IT networks and emergent threats, compliance reporting can be quite challenging.
II. Orange Business Services: a 360° market approach

In this multi-risk market, Orange Business Services focuses on covering the full scope of corporate security requirements. For this purpose, Orange Business Services leverages its dual positioning as both an international carrier and a renowned system integrator.

A security vision based on five key development areas:

1. A unique 360° Security Approach to provide relevant solutions to the full scope of requirements of enterprises - irrespective of their size

2. Integration of security at the core of cloud offerings

3. A continuous innovation and strategic alliance program providing access to the most advanced technologies

4. Design of exclusive solutions covering two emerging, fast growth segments: identity federation and strong authentication

5. Extended consulting, management, and governance services to improve management of operational risks and e-crime

With this approach, Orange Business Services is able to deliver - on a global scale - a full range of services, ranging from infrastructure and mobile devices security, to network access control, provisioning of management tools, risk governance of data and workstations, etc.

Nicolas Furgé, Security Services Division Manager, Orange Business Services, added: "Our unique market positioning offers an exclusive competitive advantage to face the new threats of next generation environments. Each security service in our portfolio covers a range of specific needs for all types of companies, anywhere in the world. This approach is part of a broader strategy to create customer value."

A strategic deployment based on key assets

With more than 30 years of expertise in the development of professional networks and integration solutions for French companies and internationally, Orange Business Services provides its client a unique expertise of security on a global scale.
An end-to-end comprehensive know-how of the security chain

Orange Business Services federates a comprehensive expertise of key security domains:

Consulting to align business and technologies objectives:

Orange Business Services leverages a consulting business unit focused on security solutions within its Orange Consulting Division. The services provided are based on proven risk analysis methodologies and new generation tools collecting information on the level of protection of systems, computer networks, organization and processes.

Orange Business Services consulting services include:

- understanding corporate specific risk exposure and requirements

  Orange Business Services initially identifies the major corporate technical risks and the actual impact of emerging technologies and new communication channels (organization, processes, etc.) to provide tailored solutions covering risk analysis, vulnerability of legacy environments, financial analysis, etc.

- designing a global security agenda

  Based on this initial assessment, Orange Business Services helps companies to develop a comprehensive security program including a complete protection architecture, security program (risk management, continuity and disaster recovery), alerts, and incidents management.

Solution integration:

Orange Business Services has the global capacity to integrate end-to-end solutions for its clients all around the world - without contracting with external local third parties. Its integration services cover implementation, initial set-up, knowledge transfer and training on all the solutions within Orange Business Services’ extended solution portfolio.

Project management: support corporate change management through an optimized implementation timeline

In the deployment phase, the company can rely on its Orange-designated project lead managing the deployment of the solution. All potential issues related to implementation (deployment time, cost, quality, etc.) are assessed upstream through collaboration with Orange Business Services network and integration teams in order to reduce risk exposure during transitional phase and to develop, if required, a training plan for end-users.

This project phase is intended to meet corporate schedules, technical, and budgetary requirements to optimize the final solution. Orange Business Services also provides change
management services to support and improve end-user understanding and ownership of the
new security strategy.

**service management**, providing the highest levels of security

After implementation, Orange Business Services organizes the management and monitoring of
communication devices in order to provide global and customized support services (including
via monitoring and reporting technologies) and to anticipate further evolutions. This proactive
approach is aligned with corporate expectations - no longer related to technologies but focused
on improvement and performance.

**security solutions management**: manage and monitor the security system

For more simplicity and peace of mind, Orange Business Services can ensure the full
management of security solutions, support companies to define monitoring key indicators and
to implement technology watch.

Moreover, Orange Business Services provides its clients with a full range of operation and
maintenance services to ensure business continuity: a one-stop self-service platform to collect
service requests, view key operating indicators, manage incidents, control service and recovery
time, etc.

**CyberSOC, a major asset**

Beyond its eight SOCs, operating all installed
or managed security equipment, Orange
Business Services also implemented a Global
CyberSOC managing all equipment installed
on customer premises, regardless of their
manufacturer.

As a global and vendor-independent platform,
Orange Business Services’ CyberSoc
provides advanced analysis of security events
and assesses the vulnerability of client
systems, potential threats and potential
impact of attacks.

Leveraging its global carrier expertise in
monitoring and operating its own security infrastructures, Orange Business Services offers
through its CyberSOC, high value security services to improve protection of client data.
Proven Certifications

- France: ISO 20000 since 2008
- International: EAL 2 + Common Criteria
- UHP Administration platforms ISO-27001 Certified
- IP VPN service certified for the DCSSI (Direction Centrale de la Sécurité des Systèmes d’Information) "Common Criteria" since 2002
- First Global Operator to receive the ISO 15408 Certification for the security of its international IP VPN
- SAS-70 Type 2 (ISAE 3402) Certified Datacenters
- The Customer Services Centers supporting Orange Business Services security services are ISO 27001 certified

Orange Business Services is an active member of the "Liberty Alliance" and a founder of CERT IST.

A strong commitment to the security ecosystem

A partnership with ENSIBS

Orange Business Services partners with ENSIBS (Ecole Nationale Supérieure d’Ingénieurs de Bretagne Sud) to provide students an apprenticeship and professional training; the first session began in September 2013.


---

4 Liberty Alliance is an international consortium of more than 180 companies collaborating on the definition of standards for identity management.

5 Cert-IST is an alert and response center for cyber attacks for French companies
Security blog, "expertise hub"

Orange Business Services has developed the first expert blog dedicated to security professionals sharing information and innovations. This team, including Orange Business Services security experts (engineers, consultants, marketers, etc.) regularly post new experiences and different perspectives on major issues, challenges, solutions, and perspectives. http://blogs.orange-business.com/securite For more information, please refer to the "links and graphics" section at the end of this document.
a recognized security leader

Recognized in 2013 as the French leader of security solutions and services by Pierre Audoin Consultants and a major player in the field of Managed Security Services in Europe by Gartner, \(^6\) Orange Business Services has been recognized by CAP, a consulting and market research leader, \(^7\) for the second consecutive year as the N°1 provider of security services in France.

*These successive awards recognize the efforts made by our expert team to improve our offerings and security solutions and the excellence of our global vision and approach of security as a whole. These awards validate our development strategy focused on providing end-to-end support and consulting e-security services,* concluded Nicolas Furgè.

---

\(^6\) Marketscope for managed security services in Europe, Gartner, October 2012

\(^7\) Pierre Audoin Consultants « Survey on IT Security in France » 2013
III. A Unique Portfolio

Orange Business Services’ portfolio of security services is based on a comprehensive and integrated approach providing a full range of 360° business services covering the needs of all businesses around the world: risk management and compliance monitoring, data and transport protection, etc. Orange Business Services also provides cloud computing environments and solutions.

customized solutions for French and international markets

Orange Business Services offers a full range of 360° services addressing all corporate needs: simple and packaged solutions for SMBs up to 20 employees, "all-in-one" easy to manage and multi-site solutions for SMBs up to 500 employees, industry-specific and custom solutions for large companies. Through this extended portfolio, Orange Business Services provides: basic solutions to secure workstations, "Unified Defense" platforms ("my local network"), protection against Denial of Service (DoS), compliance with standards and safety regulations, etc.
a global and integrated approach

To meet all the security needs of its customers, Orange Business Services offers multilevel offerings and services as well as high value consulting and support services.

Orange Business Services offers three models of service delivery aligned with corporate operating principles:

- integrated services
  Orange Business Services helps companies choose the most valuable devices according to their specific needs. In that case, Orange Business Services will be responsible for the delivery, configuration, and operation of devices.

- managed services
  Orange Business Services provides subscription-based services to manage and operate security devices - hosted within Orange Business Services datacenters or on the premises of corporate customers.

- cloud-based services
  In this case, public or private infrastructures are available on-demand and are fully managed by Orange Business Services. Such infrastructures are invoiced on a pay-per-use basis according to custom metrics related to each offer (users, bandwidth, etc.). These service models can be tailored based on Capex and Opex budgets.
A comprehensive portfolio

Orange Business Services has developed a portfolio of end-to-end reliable solutions offering advanced security within three families of products:

- **Securing infrastructures**: **Trusted Infrastructure**

  These solutions isolate IT infrastructure (extranets, partner networks, etc.), control incoming and outgoing flows, and provide availability and resilience services. They also help to detect and prevent abnormal activities or suspicious behaviors (malware, data leakage etc.).

- **Securing work environments (tools, identities and accesses, terminals)**: **Trusted Work Environment**

  These solutions manage users’ authentication and credentials and validate their identity via basic or strong authentication methods (tokens, certificates, grids, etc.). These solutions also monitor access to resources and secure data, equipments and users’ communications with various third parties (telephony, messaging, collaborative applications, video, etc.). They provide a confidential environment and adapt connectivities according to user profile (employee, partner, etc.) and type of equipment (PC, personal versus professional mobile devices).

---

Focus on **Security Integration Services** deployment of security services on a global scale

The Trusted Infrastructure portfolio includes **Security Integration Services**, a unique offer providing integrated security solutions (infrastructure and access) in 220 countries and territories. This customized service allows companies to choose the service modules they need.
Focus on **Flexible Identity**
*a cloud solution to federate user identities*

This offer provides a centralized and seamless connection to business and personal applications - irrespective of physical location (cloud, on-site, etc.) and access device (PC, tablet, etc.).

Provided as a cloud service, this highly flexible and easy to use solution is invoiced on a pay-per-use basis.
monitoring corporate security parameters to anticipate, analyse, and manage security threats and attacks: management and governance

Orange Business Services provides companies with dashboards and reporting tools required to monitor and optimize IT security parameters and improve efficiency. Moreover, software and hardware inventory solutions implemented with this platform validate the compliance of workstations and IT infrastructure with applicable regulations. Dedicated tools store and manage log files in order to comply with legal mandates applicable to data retention and network monitoring.

Focus on CyberRisk and Compliance Intelligence
assessment of the risk exposure of IT infrastructures and customized action plans

This offer provides a detailed assessment of the level of security of corporate IT environments in any type of infrastructure (i.e. devices, OS, information systems, application services, etc.) in order to implement appropriate solutions to mitigate risks. As a full audit and consulting service, this offer relies on a set of information sources and technology watch carried out by Orange Security Experts in order to define the custom risk exposure landscape of each corporate environment. This service provides a precise assessment of the overall security exposure and rates the level of compliance with applicable regulatory requirements.
Focus on **Security Event Intelligence**

**ex-post analysis and implementation of improvement corrections**

Security Event Intelligence is a security information and event management solution based on the collection of log data generated by IT teams to trace activities. This solution also implements an effective post-attack analysis (forensics, optimizes IT and network operations, and streamlines compliance initiatives.

Security Event Intelligence addresses emerging threats to ensure business continuity.
- **Cloud-based** security offers

Orange Business Services portfolio of SecaaS (Security as a Service) covers 4 major corporate requirements:

- Securing all accesses with Business VPN End User
- Content filtering with Web Protection Suite
- Managing credentials and identities with Flexible Identity
- Managing and governing with Security Events Intelligence and CyberRisk and Compliance Intelligence.

Each of these services is provided on a pay-per-use basis and relies on secured infrastructures deployed and operated by Orange Business Services and its technology partners.
Links and graphics

- discover: Orange Business Services security Web site
  http://www.orange-business.com/fr/nos-solutions-securite

and computer graphics "BYOD and emerging security risks"

and focus on Orange Cyberdefense

- discover: Orange Business Services expert security blog
  http://www.orange-business.com/fr/blogs/securite

News and events, best practices, mobility, desktop and cloud computing are among the many topics covered weekly on our security blog. A unique opportunity to update your knowledge on emerging IT and telecommunication security threats.

Inside....
Cyber security trends: Eric Domage evokes the proliferation of communication channels and associated risks, the requirement of dedicated cloud security solutions (authentication, etc.), and ROI challenges.

Security Information and Event Management (SIEM), covering technical and organizational measures required to address current threats to the information assets of an organization.

"Debriefing Orange Security Day 2013 # OSD13" by Jean-François Audenard, Cloud Security Advisor at Orange Business Services

- read our blog book "coffee time"
A digest of security blog posts in a series of small practical and thematic booklets:
VLAN Security
Password security
DoS attacks
BYOD and mobile security

- watch: webTV
Orange Business Services Web site “Security” vids on security and cloud computing, cybercrime, spam or DMZ.