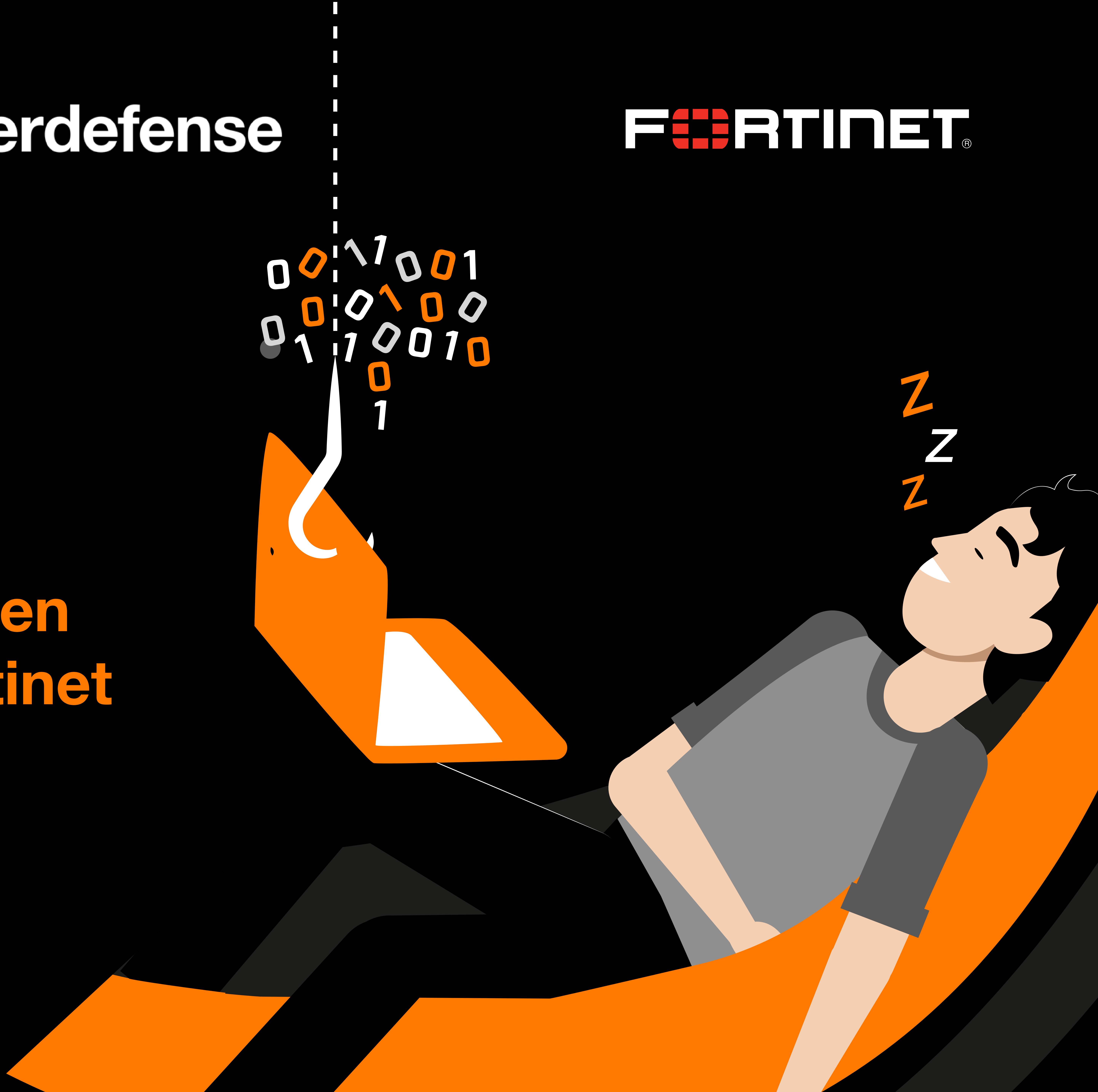
Business Cyberdefense FORTINET

Cybersecurity for the digital age

A strategic alliance between Orange Business and Fortinet



Market trends and working methods

Amid a surge in cybercrime, attackers are now targeting companies of all types and sizes. However, for reasons of competitiveness, they must continue their transformation towards the digital age. Attacks take a variety of forms, from ransomware to phishing, exploiting all kinds of technological and human vulnerabilities. They are evolving rapidly, and cybersecurity experts point out that the emergence of artificial intelligence is making the fight against cybercrime even more complex.

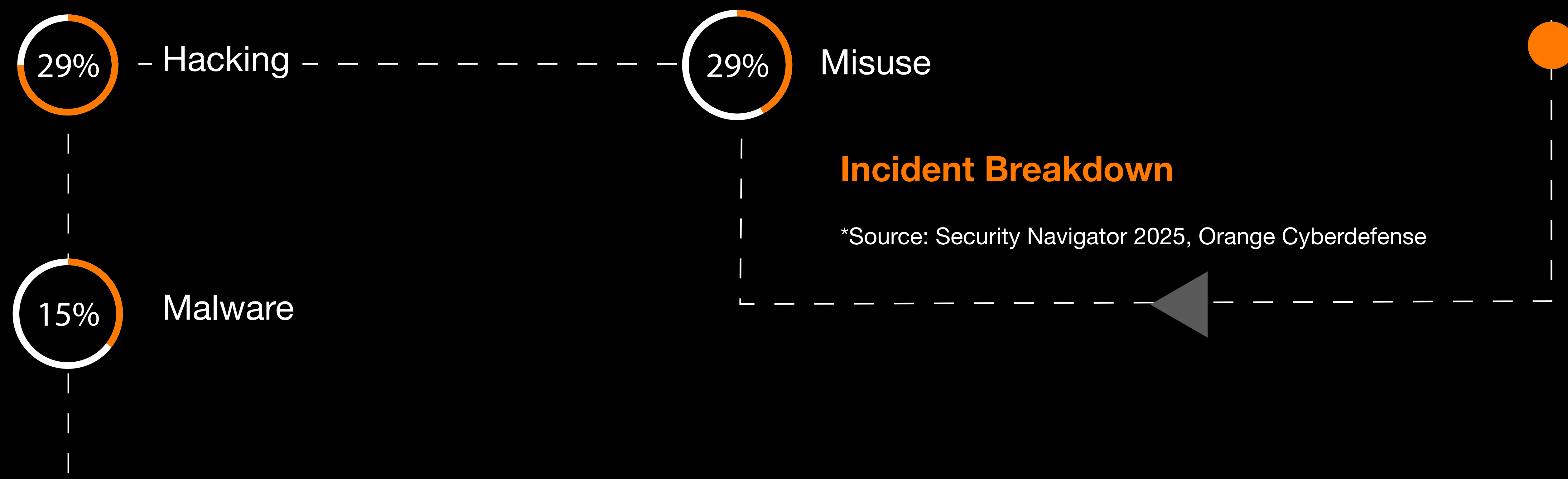
New ways of working, with massive adoption of remote working, more mobile employees, Wi-Fi becoming commonplace, as well as access to business data from a variety of devices, sanctioned and unsanctioned, all combined with massive adoption of the Cloud, mean that corporate networks have become much more complex to control and secure.

> «The cyber threat is one of the most serious economic and national security challenges we face.»
>
> Barack Obama - 44th President of the United States

135,225

Total incidents observed (October 2023 - September 2024)

*Source: Security Navigator 2025, Orange Cyberdefense



Incident Breakdown

*Source: Security Navigator 2025, Orange Cyberdefense

Digital transformation is driving growing demand for smart, flexible, high-performance grids, capable of absorbing massive use of energy. Cloud and the Internet, offer users a high degree of mobility, and support the explosion of data while guaranteeing a perfectly secure environment.

For all these reasons, security strategies need to evolve to ensure the protection of sensitive information in a heterogeneous and changing working environment.

Network management and security challenges

The spread of hybrid working and the constant evolution of the threats call for heightened vigilance from all companies of all sizes and varied sectors of activity.

Cybersecurity is strategic in guaranteeing business continuity, protecting data, employees and customers, while ensuring productivity and accessibility.

The challenges facing companies:

- protection against sophisticated attacks
- management of professional and personal equipment
- secure use of cloud applications
- regulatory compliance

In order to maintain effective protection, we need to find solutions and rely on competent partners.

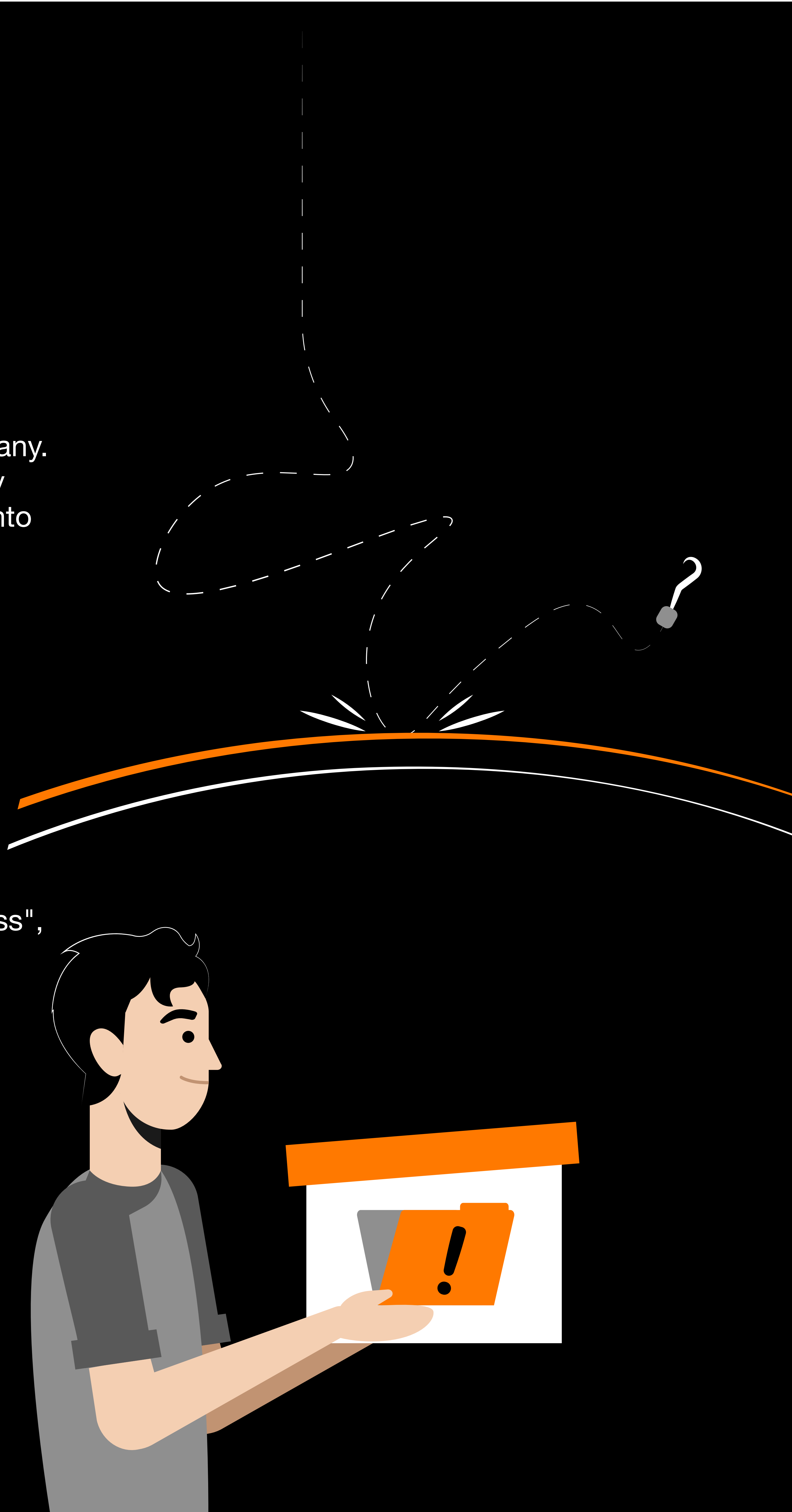
> “The level of cybersecurity says a lot about the future of a company. As with sustainability issues, organizations of all sizes, especially public ones, are integrating their cyber strategy and objectives into their reports.
> This transparency exercise, which is now mandatory in the USA, is a valuable indicator for stakeholders because it demonstrates: mastery of digital transformation, profitability and long-term investment, safeguarding the interests of customers and subcontractors, ability to attract, retain and engage talent.”

Laurent Célérier

Executive Vice-President "Central Europe & International Business", Orange Cyberdefense

Meeting these challenges requires an approach that systematically includes security in the choice of connectivity from the site to the remote user.

Advanced technological solutions need to be consolidated in order to apply unified, consistent security policies across all the use cases covered by a company's network architecture.



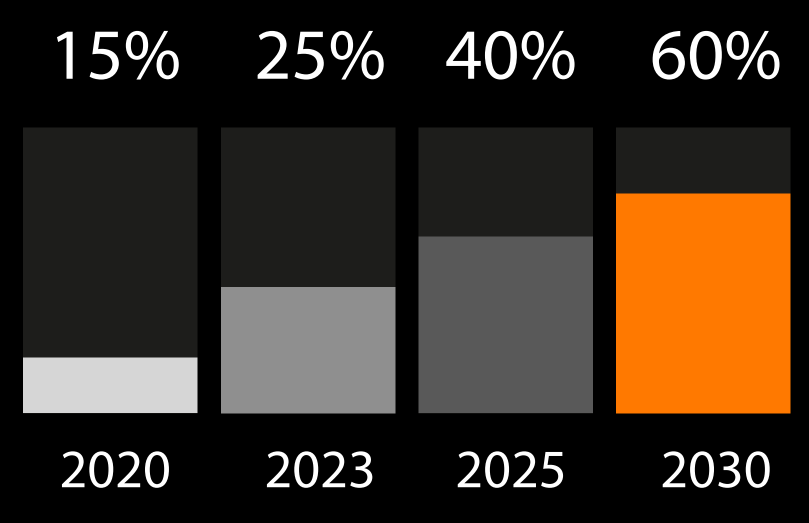
Strategies for combining improved connectivity and safety

Orange Business offers a seamless approach to support your infrastructure security strategy. Fortinet's Secure SD-Branch approach addresses both on-site security challenges and cyber-attacks. This solution helps secure the use of corporate information systems by integrating security and networking functions. Thanks to a single console, it enables centralized management of SD-Branch functions such as next-generation firewall, WAN link management, LAN and Wi-Fi network control, simplifying the protection of users, regardless of their location.

SD-Branch extends SD-WAN functionality to the entire branch network by consolidating services and converging management.

The SD-Branch market is booming in France **.

** : Source IDC SD-WAN & SASE: Market overview 2023 and outlook 2024



The advantages of an SD-Branch approach

Complete network visibility that enables the application of consistent security policies, preventing intrusions and malware, including ransomware.

A secure connection for all employees accessing company resources thanks to the advantages of the architecture.

Sensitive data remains protected while providing an optimal user experience, with enhanced network performance.

The partnership between Orange and Fortinet provides businesses with a robust, orchestrated solution for navigating a constantly changing environment.

An ultra-secure connection experience, regardless of the device used

Mark, sales representative for a company with numerous sites in UK and abroad

- Requirements: Rapid, agile deployment of new sites; ultra-permanent connection within the company or on the move; several devices for private and professional use; need to share large volumes of information.

- Threats: Targeted phishing attacks, malware, risks of device theft or loss, data breaches or losses, even business interruption.
  If a cybercriminal manages to compromise the security of Mark's devices, he could gain access to highly confidential company information as well as sensitive personal data.

- Thanks to the SD-Branch approach to securing the company's data and access flows, Mark can develop his new international branches with peace of mind, particularly in his brand-new premises in Prague. Here, he finds all his usual working environment, thanks to an SD-Branch architecture composed of switches and Wi-Fi + 5G access points to extend security as close as possible to the user. This prevents a threat from spreading to all other users, and to the strategic resources of the company and its partners.

- The company's secure converged solution for data access and sharing enables, Mark to share a highly confidential document. At first, Mark tries to use his personal storage account, which is not compliant with the company's security rules. Fortunately, thanks to its network visibility, the IT team immediately realizes this, and triggers an automated best practice action to Mark, informing him and blocking his action. This solution works for both cloud and private datacenters.
  For the enterprise, it guarantees a unified, real-time security policy, protecting users, data and applications.

30% of critical infrastructure organizations will suffer a security breach by 2025 ***.

*** Source: Gartner "Predicts 30 of critical infrastructure organization".

The advantage of a unified network and security ecosystem

The greatest challenges of digital transformation stem from its intrinsic complexity. Harmonizing business objectives with digital strategy, and managing the interdependencies between network, IT and cloud solutions while guaranteeing security, represent a real challenge for organizations.

With Evolution Platform, Orange brings together the latest connectivity and network security solutions from its ecosystem of partners in a service platform that can be customized and adjusted, in real-time, to your company's needs. Controllable from a self-service console or via APIs, Evolution Platform combines a secure digital infrastructure and service management aligned with cloud standards (instantaneous deployment and pay-per-use).
Relying on Orange's high-capillary and secure network, Evolution Platform promises enhanced network performance and security, as well as end-to-end service quality commitments.

On these foundations, Orange and Fortinet offer comprehensive network, cloud and cybersecurity solutions and services enabling:

1 Simplified management and automated control

Unified visibility extends to your entire infrastructure, including smart devices, connected objects and Operational Technology systems. This convergence of security and networks guarantees optimum protection for all devices, users, appliances and data.

For greater confidentiality, you can secure ports and restrict access to your networks to approved users and devices. Network segmentation and micro- segmentation allow you to apply granular access policies and monitor network traffic in detail.

2 Advanced, AI-enhanced security

You can strengthen security across your physical, virtual and cloud environments. FortiGuard Labs use advanced Artificial Intelligence and Machine Learning (ML) capabilities to generate shared, real-time threat intelligence to keep all parts of the security infrastructure informed of the latest attack variants for rapid detection and response.

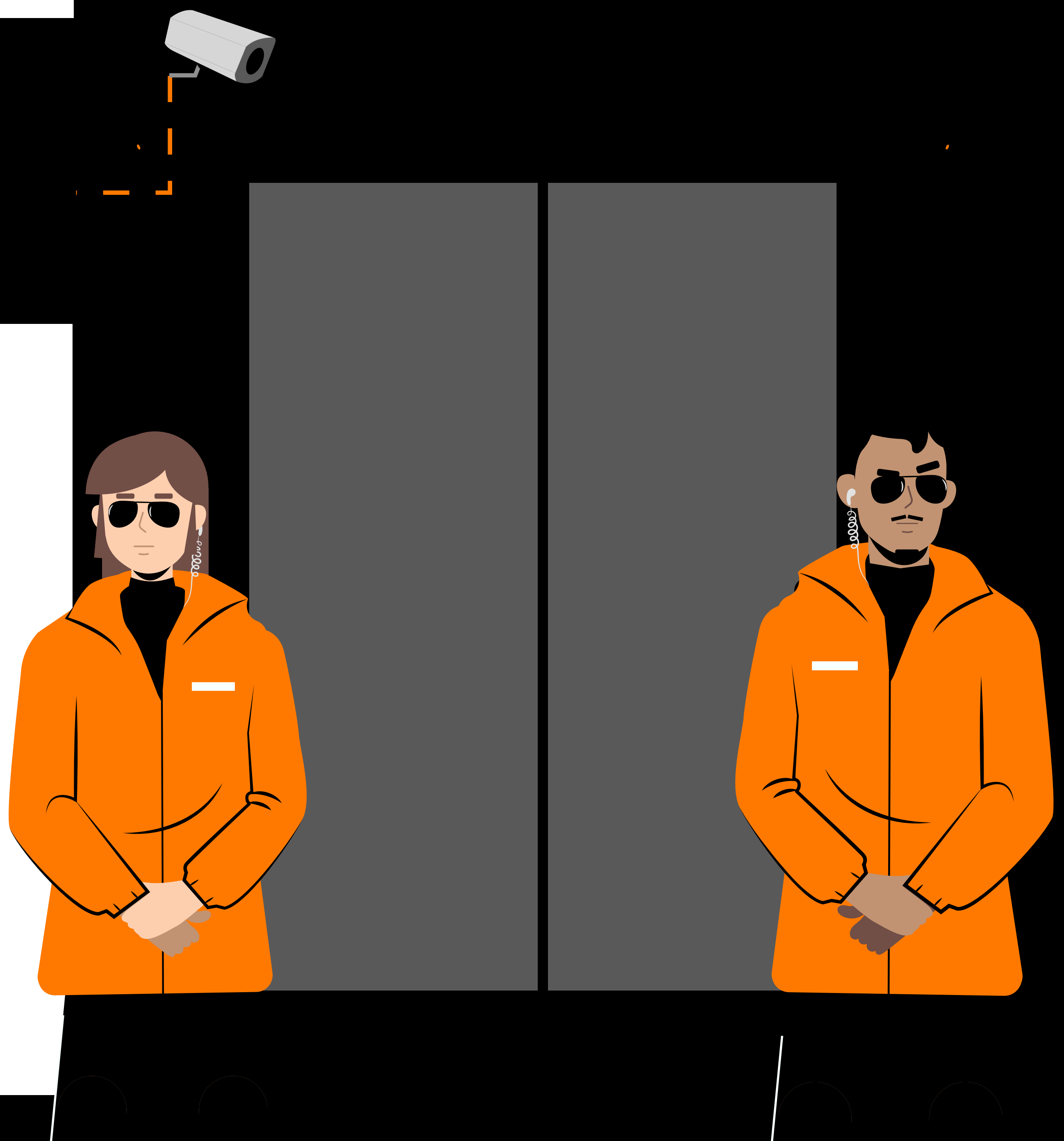
3 Enhanced user experience

Thanks to continuous optimization of network and application performance, when accessing and using your resources and applications. This is true wherever they're hosted and regardless of users' location.

4 Support

End-to-end support to understand your current and future needs, and the use cases specific to your business.

- Consulting and auditing
- Agile deployment
- Follow-up and solution lifecycle



Network users: who, when, what, how and from where?

Playful or inappropriate use of the network,
Identity theft and elevation of privileges by hackers or disgruntled employees,
Theft or loss of data and equipment,
Regulatory compliance and protection of users' privacy...

...There are many pitfalls for your network and security teams!

Identification + Authentification + User authorization = Smooth operation, traceability and integrity of your network

"The digitalization of companies is reaching the transformation stage. This means that after having accelerated the tasks as they were previously organized, digital technology allows the company to be rethought in depth, to make it more efficient and more responsive to a changing environment. But this same speed of adaptation can turn against the company if one of its many elementary processes thus optimized is diverted or distorted. It is then necessary to converge this expanding universe towards less complexity and more integration to prevent it from presenting an unmanageable risk. The security of tomorrow will not be obtained by addition, but by convergence. The question that then arises is: converge, yes, but towards what? Thousands of human years allow us to answer this question: converge at the lowest level, converge within the OS and natively integrate all these critical functions, network and security that will support future transformations."

Alain Sanchez - Fortinet EMEA CISO

A secure, connected experience for every use

Sylvie works internationally in places such as airports, hotels and cafés.

- Needs: Secure access to corporate resources and applications, and to cloud services (Microsoft 365 or Salesforce).

- Threats: Cyber-attacks, difficulties of secure connection to business applications from any location.

- On the move, with FortiSASE embedded in Evolution Platform, Sylvie benefits from secure, optimized connectivity. She connects to the Internet from a third-party location. Her traffic is automatically routed to the nearest Orange point-of-presence. There, it is inspected and secured thanks to the state-of-the-art technologies such as next-generation firewalling, intrusion prevention and content filtering. This SASE solution integrates identity management, access control to terminals, networks and applications. FortiSASE combines Fortinet's expertise in connectivity and security with the power of the Orange network and its know-how in terms of support (audit, design, build and run) and Orange Cyberdefense's expertise in terms of threat intelligence.

- In the office, security and optimum performance with Flexible SD-WAN mean Sylvie will always benefit from a seamless, secure experience. Indeed, Fortinet's Flexible SD-WAN service integrated with Evolution Platform optimizes traffic according to the network, guaranteeing better performance. In addition, endpoint security protects Sylvie's endpoints from threats, even on unsecured public Wi-Fi networks.

SASE is an approach that combines network security and wide area network (WAN) functions in a single cloud service.

82%* of French companies declare that security is the main decision factor when choosing a SASE solution ****

**** source: IDC Survey: Security Is the Top Driver for SASE Adoption in France oct 2023

Orange and Fortinet, a partnership focused on success

15 years
of partnership

650 Orange
Experts certified
by Fortinet

Strategic
partnership

Orange and Fortinet join forces to offer a solution which is complete, flexible, secure and scalable. We put our expertise in connectivity, cloud, security and integration at the service of your digital transformation project, to provide you with the right answers to your specific challenges and needs. By choosing Orange Business and Fortinet, you benefit from a holistic approach, recognized expertise and a comprehensive security solution to support your digital transformation project, and guarantee business continuity. All you need to think about is your core business.

About Orange Business and Fortinet

Orange Business, the business division of Orange, is a leading network and digital integrator. Orange Business draws on its expertise in next-generation connectivity, cloud and cybersecurity, its service platforms and partner ecosystem to offer trusted digital solutions to businesses worldwide. With 30,000 employees in 65 countries, Orange Business orchestrates end-to-end business transformation by focusing its value proposition on secure digital infrastructures, the customer experience, the employee experience and the operational experience. More than 2 million of professionals, businesses and local authorities in France and 3,000 multinationals trust Orange Business.

Orange is one of the world's leading telecommunications operators, with sales of 40.26 billion euros in 2024 and 292 million customers.
With Evolution Platform, Orange combines the expertise of its ecosystem of suppliers with the power of its network, through native integration of its partners' solutions on the latter, enabling your users to benefit from the latest updates, as well as improved network performance and security.

Fortinet (Nasdaq: FTNT) is a driving force in the evolution of cybersecurity and the convergence of networking and security. Our mission is to secure people, devices and data everywhere, and today we deliver cybersecurity everywhere our customers need it with the largest integrated portfolio of over 50 enterprise-grade products. Well over half a million customers trust Fortinet's solutions, which are among the most deployed, most patented and most validated in the industry.
The Fortinet Training Institute, one of the largest and broadest training programs in the industry, is dedicated to making cybersecurity training and new career opportunities available to everyone. Collaboration with esteemed organizations from both the public and private sectors, including Computer Emergency Response Teams ("CERTs"), government entities, and academia, is a fundamental aspect of Fortinet's commitment to enhance cyber resilience globally. **FortiGuard Labs**, Fortinet's elite threat intelligence and research organization, develops and utilizes leading-edge machine learning and AI technologies to provide customers with timely and consistently top-rated protection and actionable threat intelligence. Learn more at https://www.fortinet.com/, the **Fortinet Blog**, and FortiGuard Labs.

For more information:
https://www.orange-business.com/
LinkedIn: Orange Business
Twitter: @OrangeBusiness

Sources :

* Security Navigator 2025, Orange Cyberdefense ** IDC SD-WAN & SASE: Market overview 2023 and outlook 2024 *** Gartner "Predicts 30 of critical infrastructure organisation". **** IDC Survey: Security Is the Top Driver for SASE Adoption in France oct 2023

Business

FORTINET®