Orange Belgium

IT Security Solutions

Network Security

As corporate networks are transforming and extending, more sophisticated attacks mean network security has to be redesigned.

Whilst organisations are rethinking the way in which they create and deliver value, the requirement for flexibility became crucial for launching new digital workflows. To benefit from such flexibility, increasing reliance on cloud services transformed network topologies. In the meantime, remote access to corporate data further amplified the change within historical network patterns.

More user work performed off the corporate network than on it

More workloads running in IaaS than in the enterprise datacenter

More applications consumed via SaaS than from corporate infrastructure

More sensitive data located outside of the enterprise datacenter than inside

More user traffic destined for public cloud service than to corporate data center

More traffic from branch offices heading to public clouds than to corporate data center

The transformation of network topology forces organisations to switch their network security strategy from datacenter-centric to identity-centric.

Traditional security architectures, which utilise datacenter firewalls as a central component, must be strengthened to secure users, devices, applications, and data moving outside the enterprise perimeter:

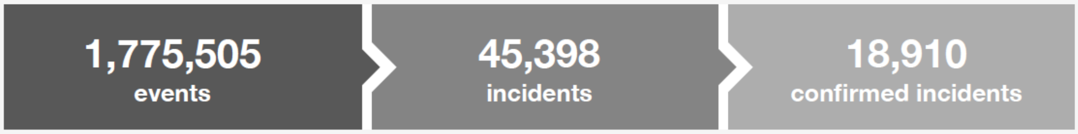
- Deploy **Next Generation Firewall** (NGFW) including advanced security features such as URL Filtering;
- Prevent attacks exploiting web application's vulnerabilities with a **Web Application Firewall** (WAF) inspecting HTTP traffic;
- Implement **Cloud Access Security Broker** (CASB) acting as an intermediary between users and cloud service providers with 4 major functionalities - Visibility, Compliance, Data Security and Threat Protection;
- Adopt **Zero Trust Network Access** (ZTNA) to control access to corporate data based on user identity. Include **Endpoint protection** as part of the ZTNA strategy to ensure device compliancy (sanitary check);
- Develop **Detection & Response** capacities such as Sandboxing and XDR to block more sophisticated attacks bypassing traditional prevention systems;

This trend is leading to new network security approach as described by Gartner in 2019: Secure Access Service Edge (SASE). This consists of an amalgamation of the functionality of modern networking with the protection provided by new security measures.

In a modern cloud-centric digital business, users, devices, and the network capabilities they require secure access to, are everywhere. As a result, secure access services need to be everywhere as well.

Network & Application anomalies still remain the most frequent incident type observed by Orange group, globally, last year.

As a European leader in security management services (MSSP), Orange analysed a large number of security events happened in 2020, making it possible to share unique statistics on events and incidents that were recorded in 2020. Orange SOCs (17) and CyberSOCs (11) located worldwide constantly analyse data, identify anomalies and help customers to update. In the data analysis performed between January and October 2020, more than 1.5 million security events that led to more than 18 thousand confirmed incidents were recognised. More detailed analysis available in our white paper

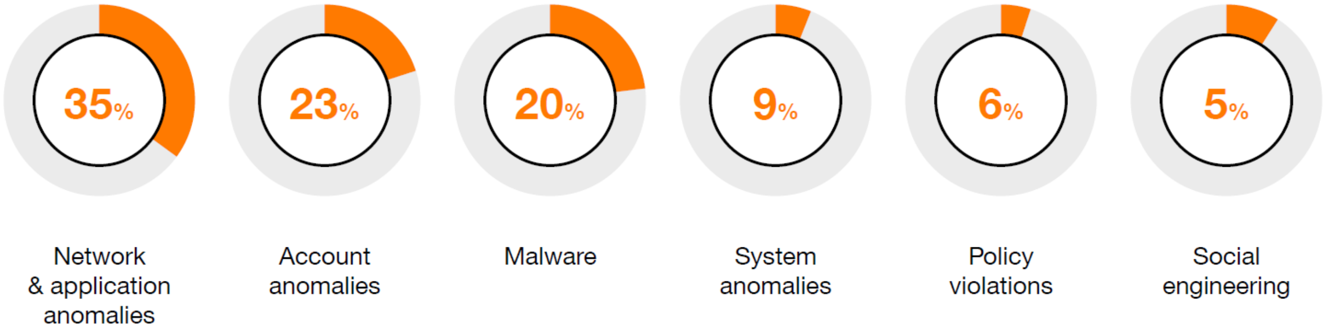


1,775,505 events

45,398 incidents

18,910 confirmed incidents

Confirmed incidents by category



While network security is becoming more complex, organisations need to balance their needs with their budgets and expertise. Building technological ecosystems will simplify your daily operations by embracing the concept of a “single glass of pane”.

To help its clients addressing network security challenges, Orange partners with technology leaders providing top-performing, end-to-end, cyber security platforms. Implementing integrated network security ecosystems consolidates visibility across infrastructures, reducing the tools and competences required in-house and shortening incident-response time.

Aware that security operations can be demanding, Orange offers a comprehensive range of managed services to support IT workloads.

Our security managed services support IT departments either by outsourcing tasks that can be performed in-house, but prove to be too demanding (by way of time or experience) or as a way to benefit from assets and expertise in a flexible way.

Maintenance

Hardware & License replacement with specific SLA

Equipment Management

Operating System updates & design authority for MACD

Security event monitoring

SOC analysts monitoring security events and alerting you to incidents

Emergency Response

Cyber Emergency Response Team supporting incident recovery

Where to start?

Network security is a large topic and possibly complex to address from scratch. As a first step, Orange suggests that prospective clients undergo an assessment. Different types of assessment can be performed depending on existing maturity:

- **<u>Infrastructure assessment:</u>** Gain visibility and keep control over your network & security set-up for easier decision making;
- **<u>Penetration testing:</u>** Adopt a proactive approach to identify and exploit vulnerabilities in your network security defense and detection systems; or
- **<u>Other types</u>** of assessment such as vulnerability scan or framework based (ISO27001).

More information
https://business.orange.be/en/it-solutions/security-solutions

Orange Belgium
Avenue du Bourget 3,
1140 Evere

Contact us
B2BSecurity@orange.be