

Business Internet Security.

Confidentiality, integrity, and availability of the data being handled is paramount.

Alexandru Ionescu, Managing Security Solutions Consultant



Orange Romania security approach

Business Internet Security solution



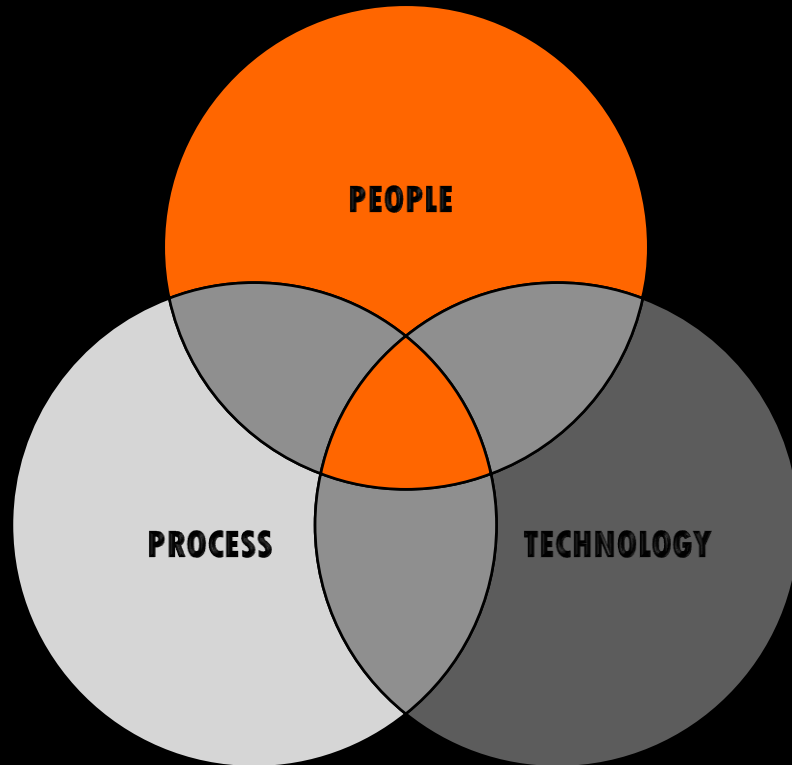
CIA triad

Confidentiality – access to information should be restricted to only those who need access to it

Integrity – assurance that information is accurate, and reliable – in other words, protected from unauthorized modification, destruction and loss

Availability – guarantee of access to information by authorized persons and when necessary

Pillars of cybersecurity



People

- Staff Training & Awareness
- Professional Skills and Qualification
- Competent Resources

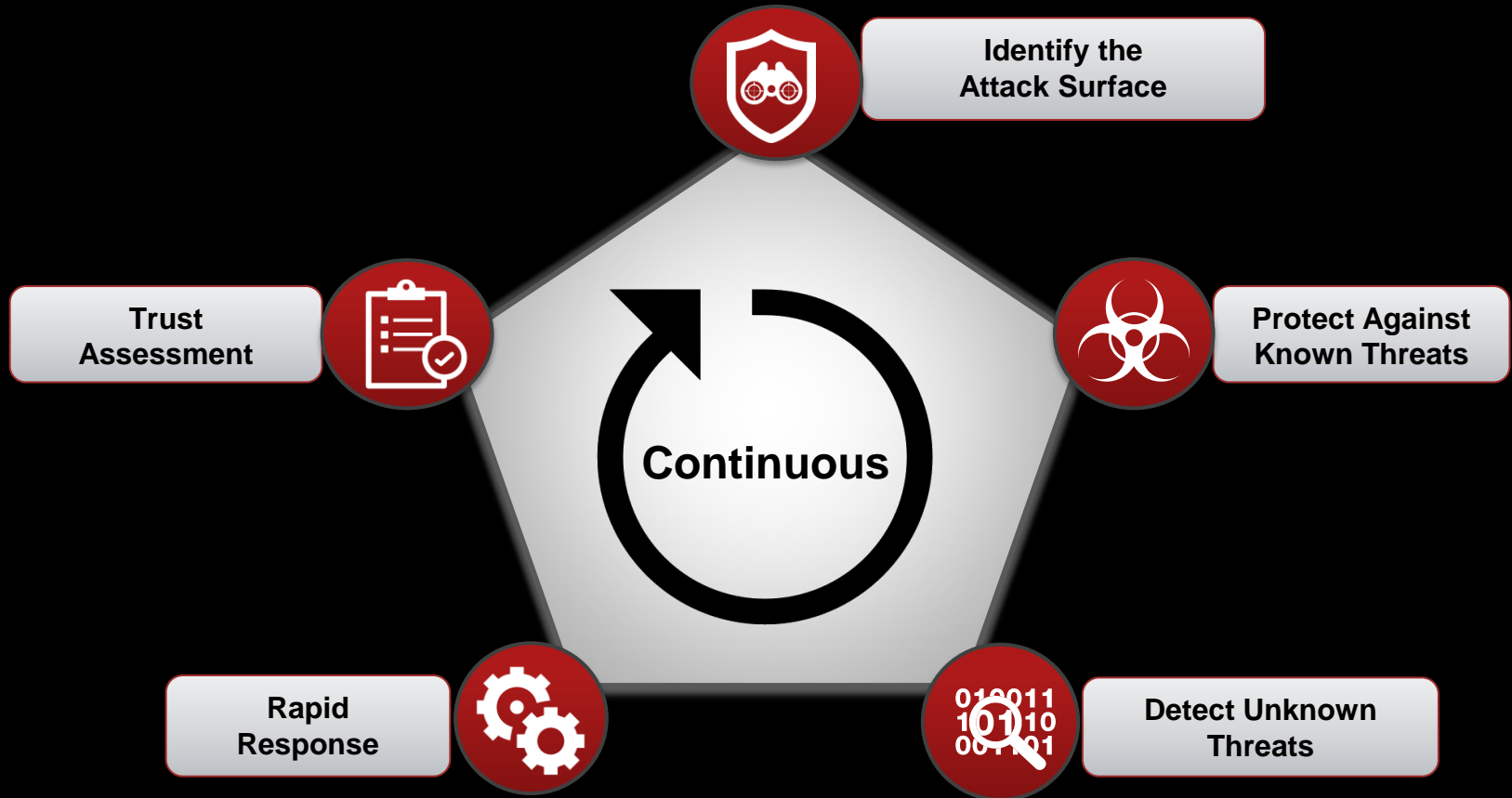
Process

- Management Systems
- Governance Framework
- Best Practices
- IT Audit

Technology

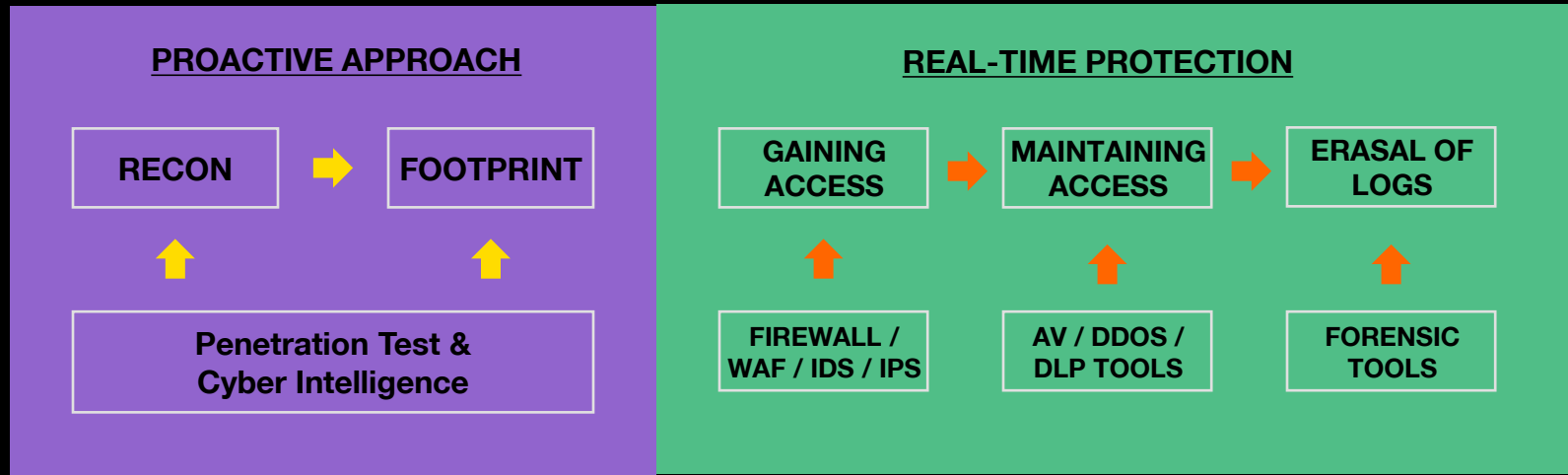
You can't deploy technology without competent people, support processes, or an overall plan

Security framework for digital security



Proposed Security framework

Professional services + MSSP

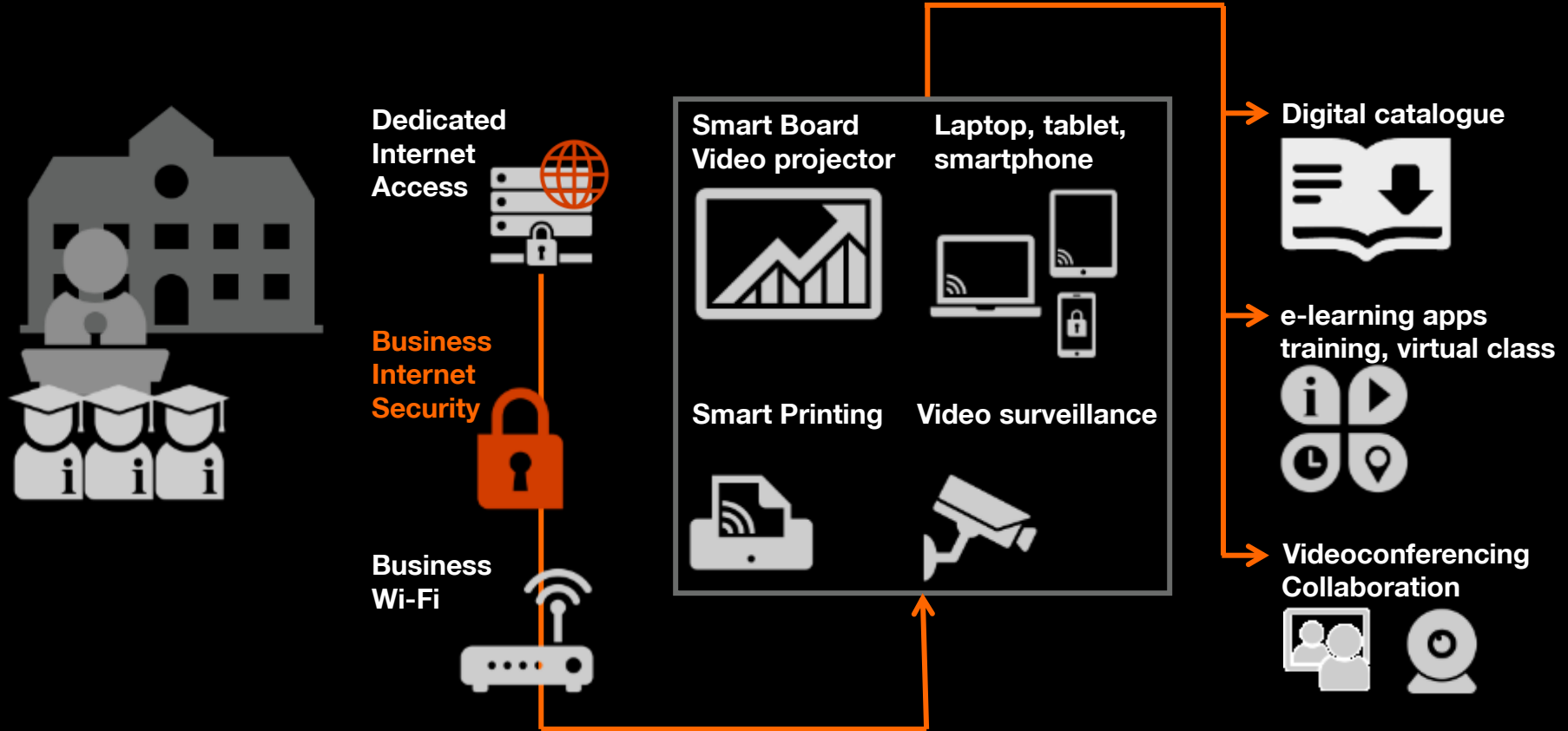


Professional Services
Partnerships



MSSP

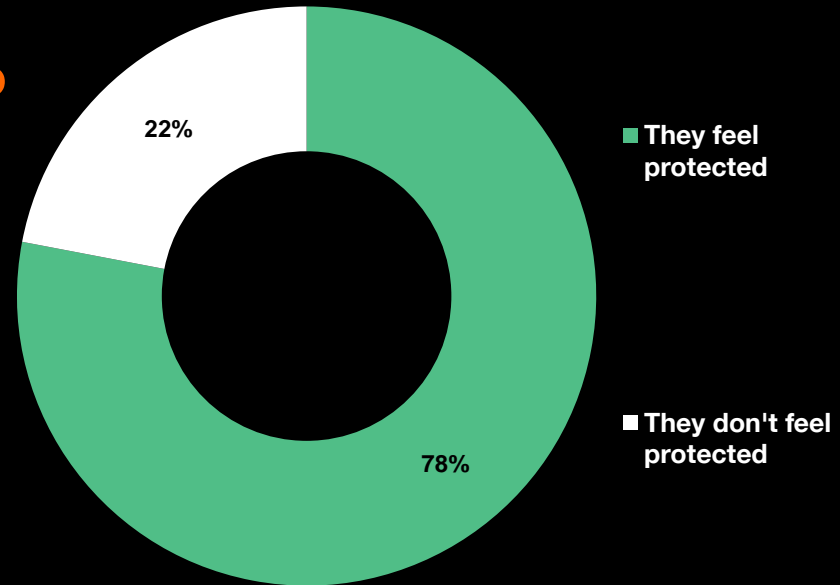
Integrated and secured solution design



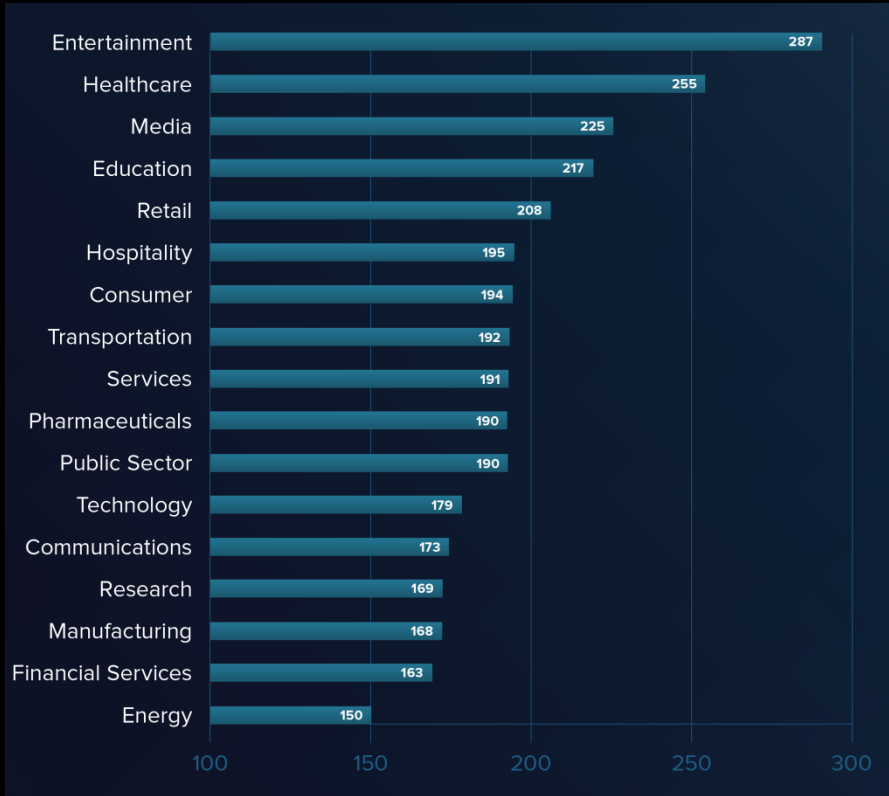
Romanian companies are very confident, but are they protected?

Less than a quarter of the interviewed companies believe they are exposed to cybersecurity risks

- 30% don't secure the Wi-Fi network
- 43% don't have anti-malware filtering
- 50% cannot control the Internet traffic
- 63% don't have anti-DDoS protection
- 83% don't have dual VPN authentication



Average Number of Days to Detect a Breach by Industry



67%

Of companies find out of the breach from external parties

197 days

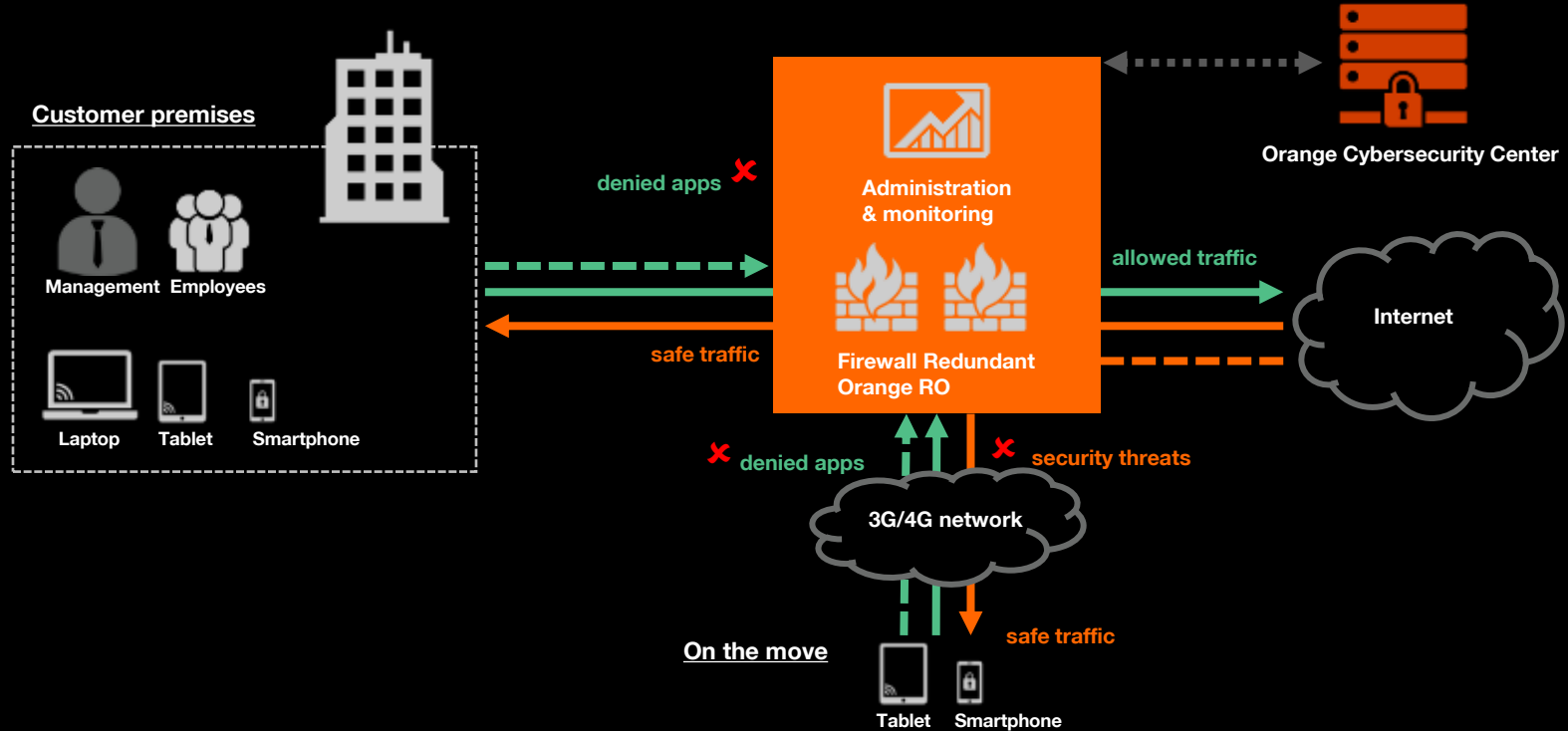
The world average for the time to detect an attack

Orange Romania security approach

Business Internet Security solution

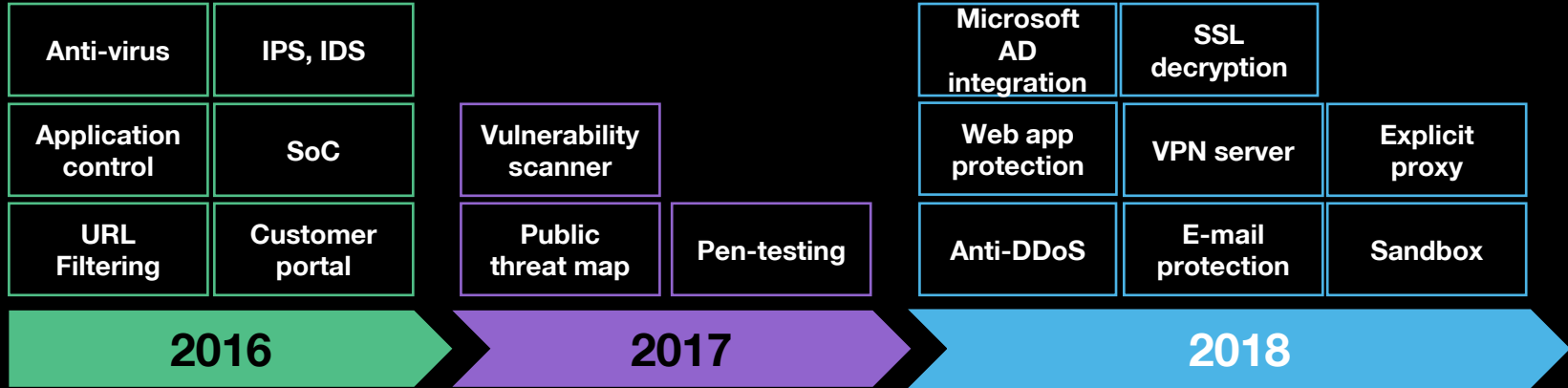
Business Internet Security

Managed security service architecture



Business Internet Security

Product evolution



Business Internet Security

More than security

ROUTING AND CONNECTIVITY

CONTROL

SECURITY

PROFESSIONAL SERVICES

Firewall

Allows new connections based only on a set of clear rules.

Example: to a web server from the customer network or just to the destinations that are required

- ✓ Small and medium businesses that do not have professional network equipment; (cloud based solution)
- ✓ The core network of large companies, where such systems already exist, but want a technology refresh to successfully respond to new threats (on-premise solutions)

ROUTING AND CONNECTIVITY



Network Address Translation

ROUTING AND CONNECTIVITY

Translating private IP addresses from the Customer network into one or more public IP addresses to facilitate Internet connectivity. Ensures visibility at the individual user level.

✓ Internet connectivity of multiple headquarters via a single secured point;
Large number of users (eg Wi-Fi for visitors, private APN)



APN Filtering

Filtering the traffic from the SIM cards that are part of a default private APN, depending on the IP assigned to each SIM.

- ✓ Reducing the cost of roaming
- ✓ Anti-phishing Filter
- ✓ IOT Solution

ROUTING AND CONNECTIVITY

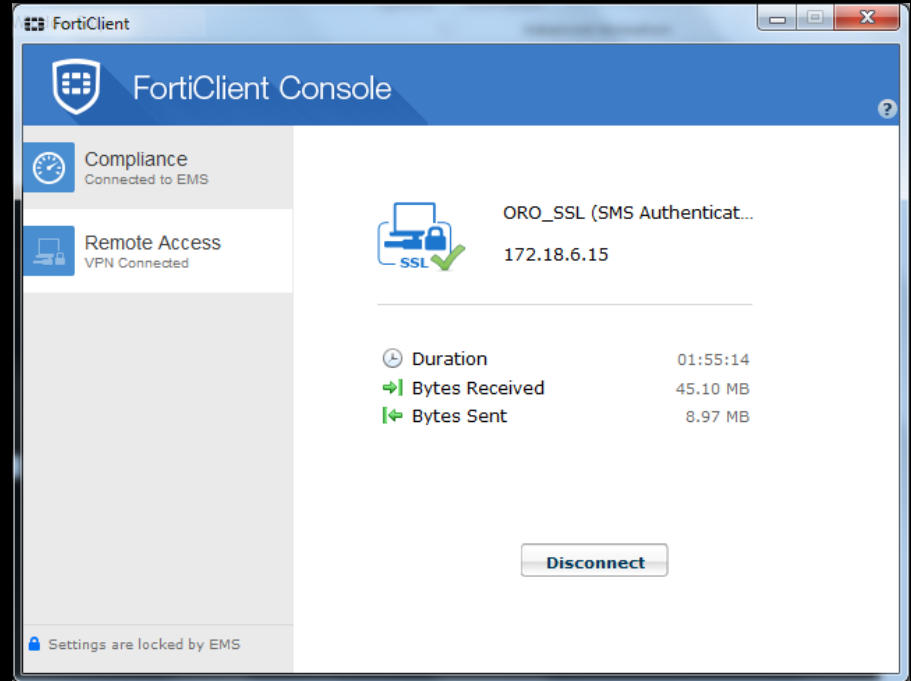


Remote Access VPN

Secured and encrypted remote access over the Internet to the customer's resources accessible from the Orange network, using an IPSec-compliant VPN client, based on user name and password.

- ✓ Remote workers
- ✓ Subcontractors
- ✓ Secured access to IaaS resources

ROUTING AND CONNECTIVITY



Site-to-Site VPN

Secured and encrypted connection over the Internet of one or more remote locations to ensure customer access to their own resources hosted in the Orange network.

- ✓ Connectivity with an office outside the Orange network or abroad
- ✓ Secure transfer of sensitive data over the Internet

ROUTING AND CONNECTIVITY



Load Balancer

ROUTING AND CONNECTIVITY

Balancing incoming connections from the Internet to two or more of the customer's similar servers. LB is available for the following services: HTTP, HTTPS, IMAPS, POP3S, SMTPS, SSL.

- ✓ Scalability
- ✓ Redundancy
- ✓ For companies offering online services



This website is **unavailable**.

If you are the website owner, please contact your website administrator for further details.

URL Filtering

CONTROL

Allows connection to websites according to a set of rules and based on their inclusion in the available categories, or one-off exceptions, in accordance with the Customer's security policy.



The site ahead contains harmful programs

Attackers on **thepiratebay.org** might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).

- ✓ Blocking access to malicious sites
- ✓ Blocking inappropriate content (ex. adult, gambling)
- ✓ Network bandwidth efficiency

Application Control

CONTROL

Recognizing the applications according to known/custom signatures and blocking, limiting or allowing access to those applications according to a set of rules.

- ✓ Blocking inappropriate or malicious applications (ex. torrents)
- ✓ Prioritizing business applications
- ✓ Avoiding security risks (e.g. data exfiltration)
- ✓ Increasing employee efficiency



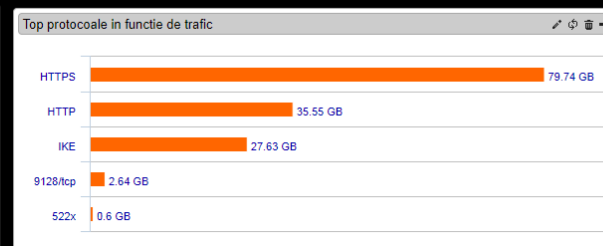
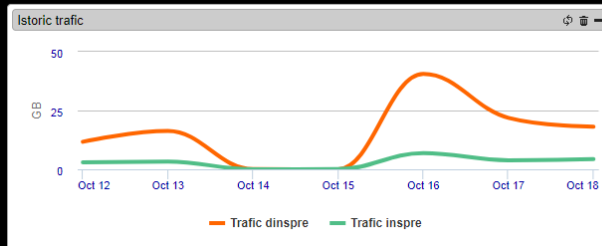
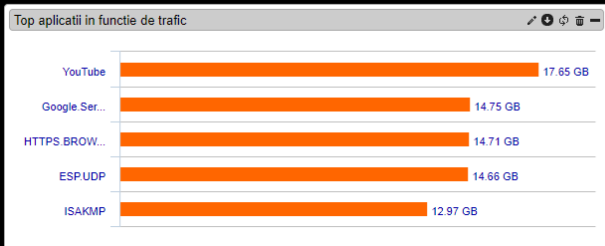
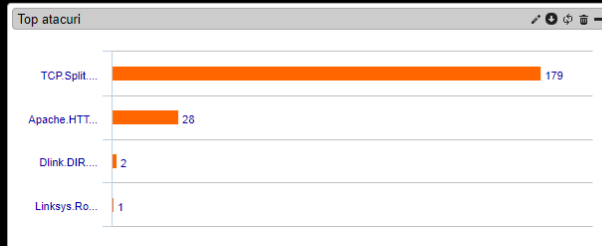
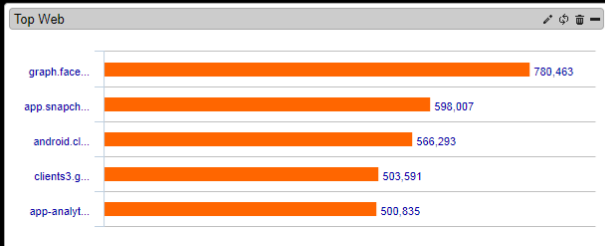
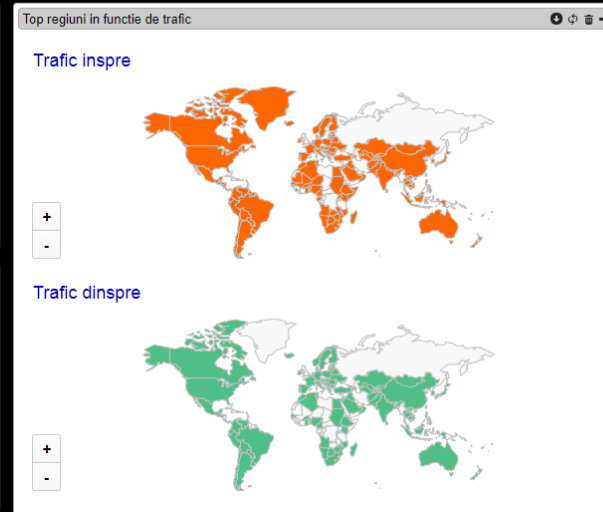
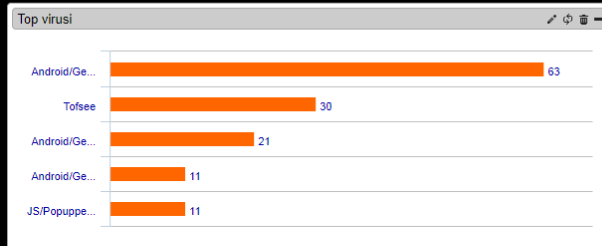
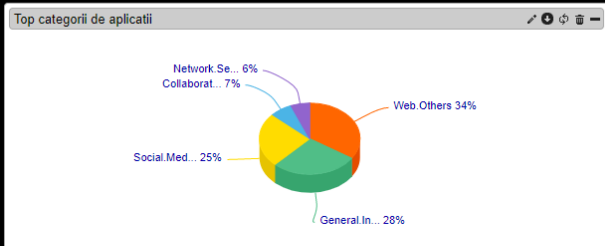
Management interface

CONTROL

Acasa | **Ecran principal** | Reguli si obiecte | Vizualizare | Rapoarte | Resurse suplimentare | Audit

+ Widget | Tot | Ultimele 7 zile

Actualizare

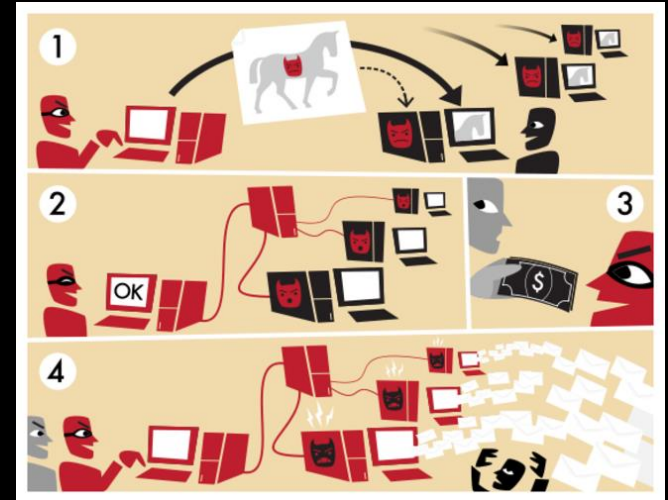


Antivirus

Inspection of transferred files within the 10MB limit and blocking of those containing viruses. Blocking communication with command and control servers of botnet networks according to known signatures.

- ✓ Malware download blocking (e.g. Ransomware)
- ✓ IP Reputation & Anti-Botnet Security Service

SECURITY





Advanced threat protection

SECURITY

Delivering sandboxing as an integrated feature of established security technologies already in place across network, email and web application inspection points.

- ✓ Discovering zero-day vulnerabilities
- ✓ Together with IPS technology, that includes multiple smart security feeds, the solution offers advanced protection against known or unknown threats.

 <h3>Meltdown</h3> <p>Meltdown breaks the most fundamental isolation between user applications and the operating system. This attack allows a program to access the memory, and thus also the secrets, of other programs and the operating system.</p> <p>If your computer has a vulnerable processor and runs an unpatched operating system, it is not safe to work with sensitive information without the chance of leaking the information. This applies both to personal computers as well as cloud infrastructure. Luckily, there are software patches against Meltdown.</p>	 <h3>Spectre</h3> <p>Spectre breaks the isolation between different applications. It allows an attacker to trick error-free programs, which follow best practices, into leaking their secrets. In fact, the safety checks of said best practices actually increase the attack surface and may make applications more susceptible to Spectre</p> <p>Spectre is harder to exploit than Meltdown, but it is also harder to mitigate. However, it is possible to prevent specific known exploits based on Spectre through software patches.</p>
--	--

DDoS Protection

DDoS protection is a premium service where customer traffic is constantly monitored, ensuring that, if attacked, it will be redirected to Orange Cleaning Center, thus ensuring the availability of Internet connectivity.

- ✓ For companies offering online services
- ✓ Can integrate other internet providers for on-premise solution

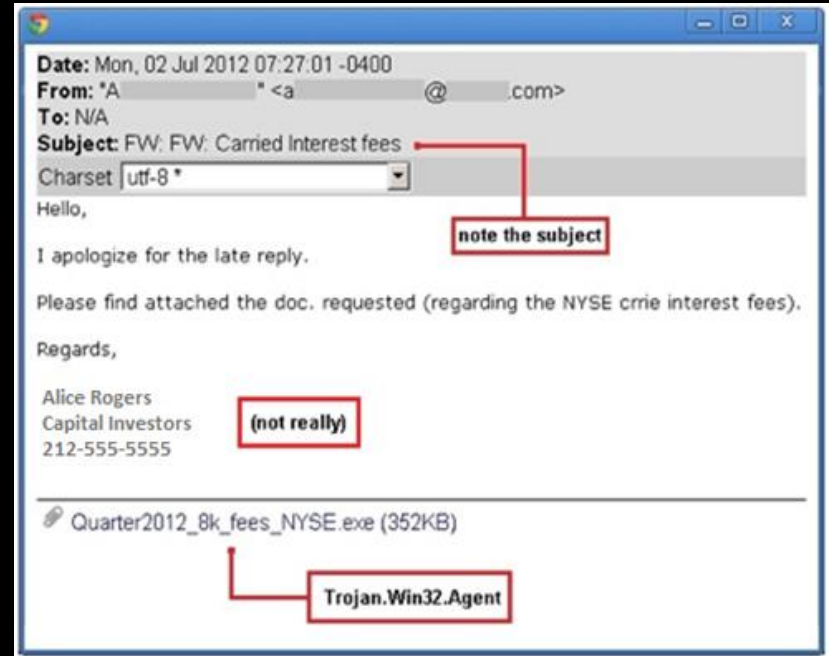


E-mail protection

Identifying "Spam" messages using known content recognition signatures and / or known malicious server lists, followed by proper tagging of messages by adding tags in the "Subject" field and / or blocking or deleting attachments that are identified as malware.

- ✓ Malware download blocking (e.g. Ransomware)
- ✓ Protect against socially-engineered phishing and business email compromise
- ✓ Blocking large volumes of unwanted spam
- ✓ Can be integrated with any customer's mail solution

SECURITY



Web Application Firewall

WAF's AI-enhanced and multi-layered approach protects web apps from the OWASP Top 10 and more. With dual machine learning detection engines customer applications are safe from sophisticated threats such as SQL injection, cross-site scripting, buffer overflows, cookie poisoning, malicious sources and DoS attacks.

- ✓ For companies offering online services
- ✓ Protect web-based applications from code-based vulnerabilities

SECURITY



Threat Map

<https://bis-threatmap.orange.ro>



Real Time Map

Statistics

Insights

Are you vulnerable?

About

Source of attack

	United States of America
	Romania
	Netherlands
	Sweden
	Canada

Number of attacks

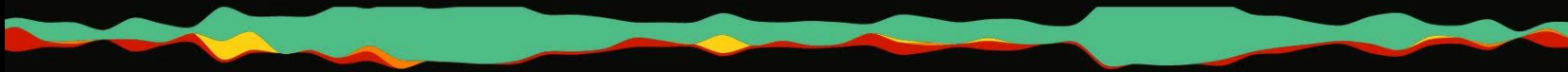
750
305
86
76
53



Time	Source	Threat
L4 29/10 0:0:6	United States of A...	HTTP Unknown Tunnelling
L4 29/10 0:0:6	United States of A...	SSH Client Request Mimicking
L1 29/10 0:0:4	United States of A...	ABNR Botnet
L4 29/10 0:0:3	United States of A...	SSH Client Request Mimicking
L4 29/10 0:0:2	United States of A...	SSH Client Request Mimicking

Real time threat analytics from data gathered from Orange Business Internet Security Agents deployed across Romania

● L1 Critical Risk ● L2 High Risk ● L3 Medium Risk ● L4 Low Risk





40%

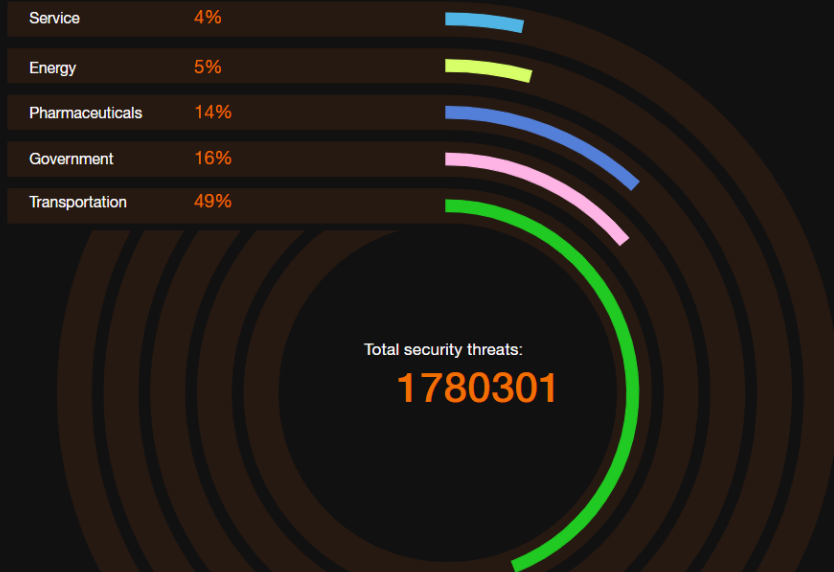
of all Corporate dedicated Internet access links protected

5.500.000

security events detected each month by
ORO Business Internet Security

[Last 7 days](#) | [Last 30 days](#)

Security Threats By Categories

[View all »](#)

<https://bis-threatmap.orange.ro>

Latest News

2019/04/17 [Windows Zero-Day Emerges in Active Exploits](#)

A just-patched vulnerability in the Windows operating system that was previously unknown up until last week is being actively exploited in the wild; it opens the door for full system takeover.

Discovered by Vasily Berdnikov and Boris Larin of Kaspersky Lab on St. Patrick's Day this year, the flaw (CVE-2019-0859) is a use-after-free issue in the Windows kernel that allows local privilege escalation (LPE). It's being used in advanced persistent threat (APT) campaigns, the researchers said, targeting 64-bit versions of Windows (from Windows 7 to older builds of Windows 10).

Read more: [threatpost.com](#)

2019/04/17 [Scranos, a new rootkit malware, steals passwords and pushes YouTube clicks](#)

Security researchers have discovered an unusual new malware that steals user passwords and account payment methods stored in a victim's browser — and also silently pushes up YouTube subscribers and revenue.

The malware, Scranos, infects with rootkit capabilities, burying deep into vulnerable Windows computers to gain persistent access — even after the computer restarts. Scranos only emerged in recent months, according to Bitdefender with new research out Tuesday, but the number of its infections has rocketed in the months since it was first identified in November.

Read more: [techorunch.com](#)

2019/04/16 [Trading Bots Are Running Wild on Crypto Exchanges](#)

"Flash Boys"-like trading manipulation is rampant on certain cryptocurrency exchanges, according to a paper from researchers at Cornell Tech and several other universities.

Special arbitrage bots are anticipating and profiting from ordinary users' trades on decentralized exchanges, which let them trade more directly, the authors said in a report released last week. The firms that deploy the autonomous trading programs manage to get priority ordering by paying higher fees, and use that advantage for

Are you vulnerable?

<https://bis-threatmap.orange.ro>

Find out if your website is vulnerable to cyber threats by using Threat Map's advanced security scanning engines:

- Web Security Scanner
- CMS Specific Scanner (for Drupal, Joomla, WordPress)
- APT Watering Hole Malware Detection Engine
- RO Hacked Database

Detailed Reports on found vulnerabilities, malware and remediation techniques

Are you vulnerable?

Most probably, yes. We found critical vulnerabilities for 84% of the companies we tested in 2018. Enter your details below to for an instant test of your company website. Contact us for an in-depth evaluation of your entire network.

Your Company Website

[https://](#) ▼

[www.company-website.com](#)

Your Name

Your e-mail address (required to send you the report)

Please choose the scan type

[Fast Scan & Non-Intrusive](#) ▼

<http://www.cybersecuritychallenge.ro>



Campionatul European de Securitate Cibernetică

April 11 · 🌐

Lotul preliminar al României pentru Campionatul European de Securitate Cibernetică (București, 2019) a fost definitivat în urma unei competiții naționale online, desfășurată pe 6 și 7 aprilie. Mulțumim tuturor pentru participare! Clasamentul final este disponibil aici: <https://ctf.cybersecuritychallenge.ro/scores> #ECSC2019



Thanks.

We are here for you.

We're listening.

