Knowledge and awareness key to meeting NIS2 requirements

axence®

97%

customers rate our technical support positively

+600,000
Agents worldwide

+4500
Active customers

+40
Countries (EMEA, Americas, APAC)

21
Years in IT management & cybersecurity

100%
European-owned and developed

They trusted us

KPRP
Kancelaria Prezydenta Rzeczypospolitej Polskiej

MODIVO

ZIKO APTEKA

WITTCHEN

DAX COSMETICS
RONTO Pharmaceuticals Group

KASA UNII LUBELSKIEJ

morele

X-KOM

PHOENIX CONTACT

eobuwie.pl

Mimo Wszystko
Fundacja Anny Dymnej

Ministerstwo Zdrowia

PM Bank

WARMIŃSKO-MAZURSKI
URZĄD WOJEWÓDZKI
W OLSZTYNIE

ROMET

EC ENGINEERING

NORTHWAY® BIOTECH

ILF CONSULTING ENGINEERS

BULGARIAN STOCK EXCHANGE

EUROINS
MEMBER OF EUROHOLD

Core Customer Segments

Government

Commerce

IT & Tech

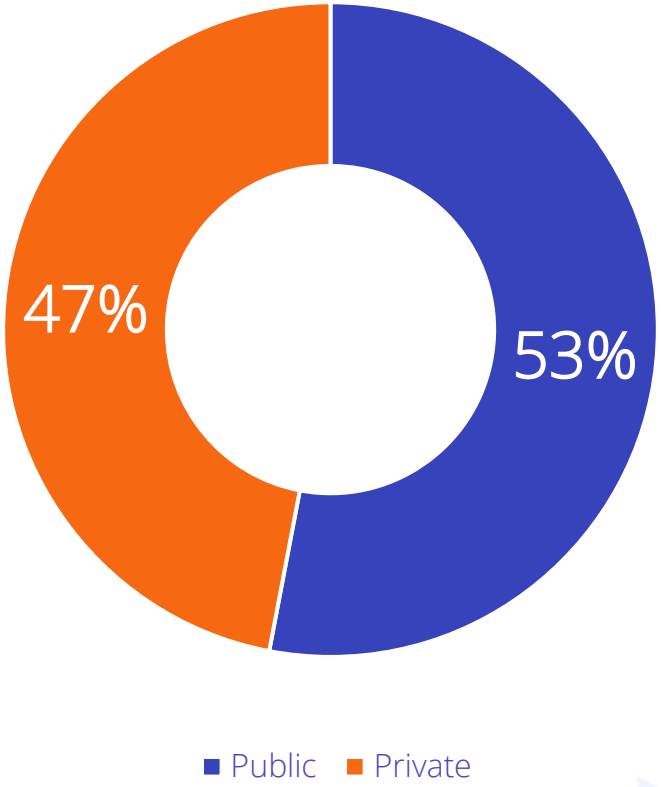
Education

Finance

Manufacturing

Logistics

Healthcare



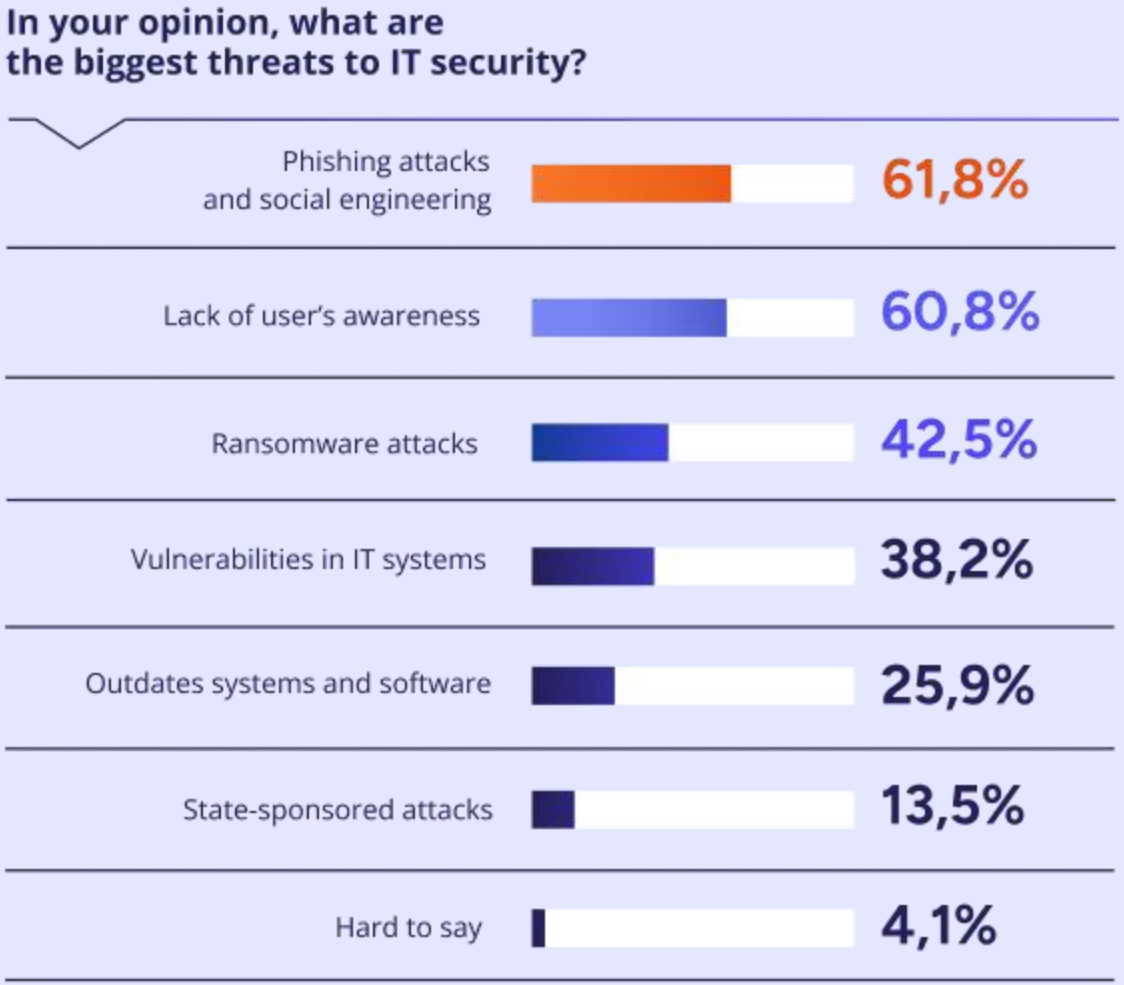
Main threats:

Phishing and social engineering

61,8%

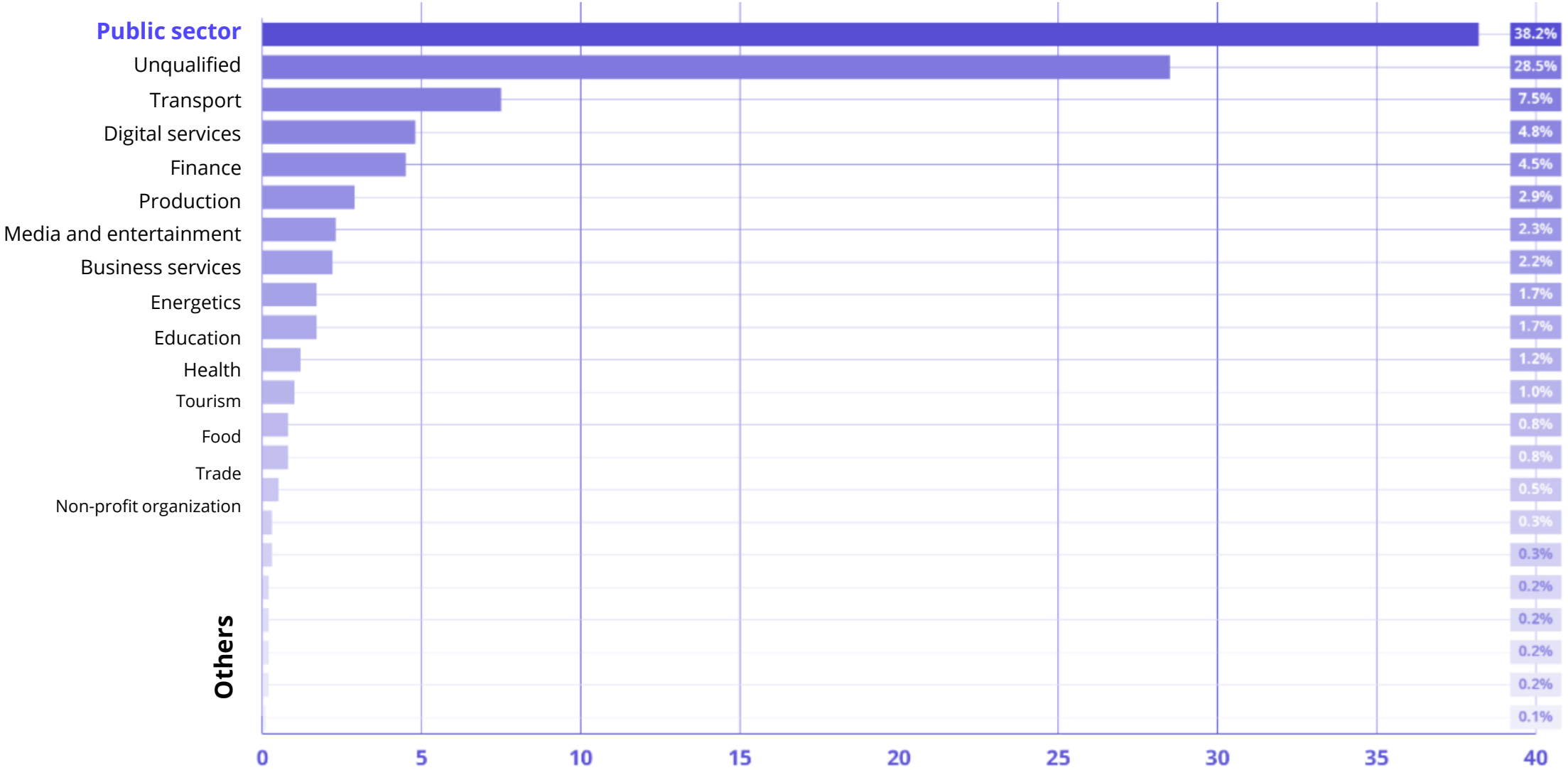
Lack of user knowledge

60,8%



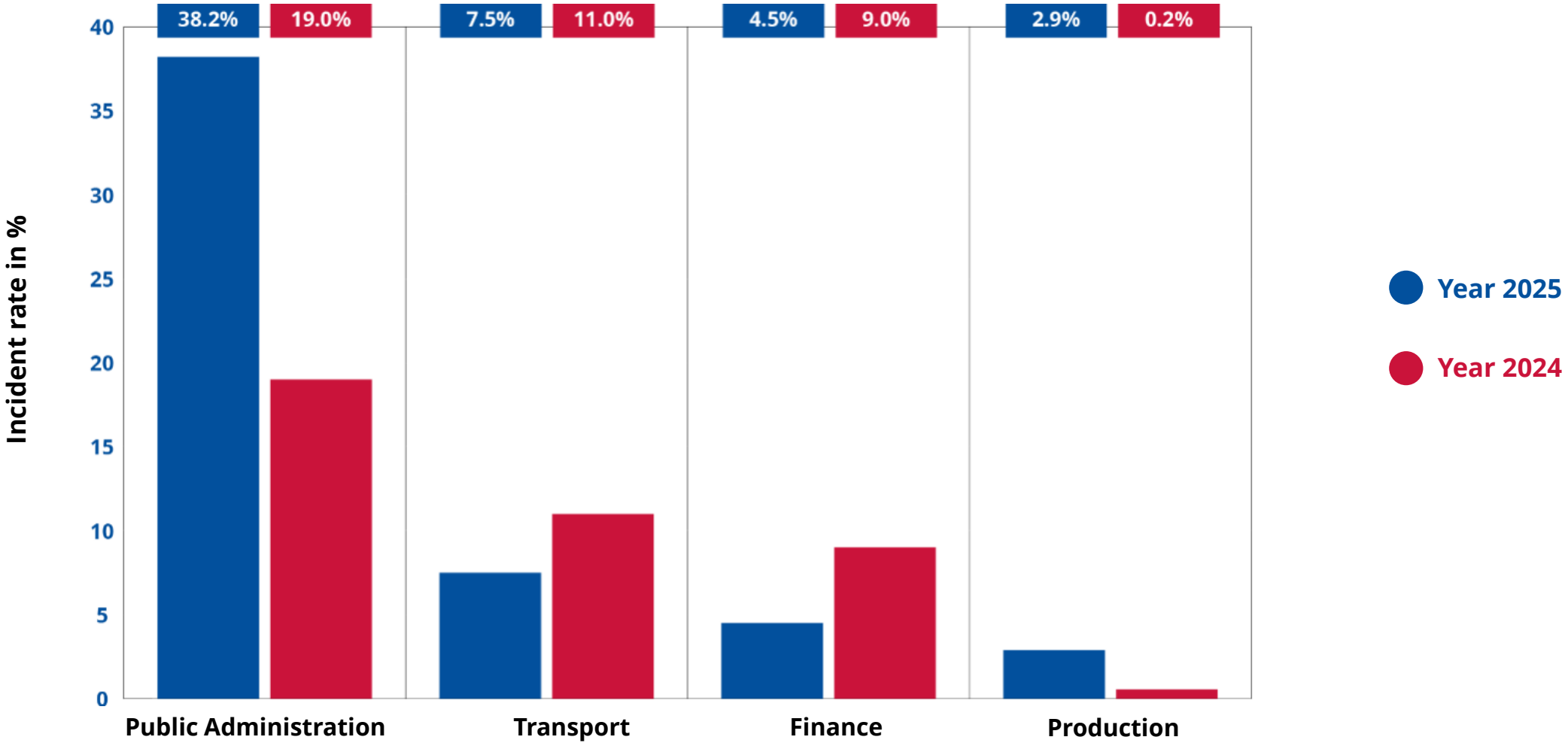
Source: Lords of the net Report 2025

Modern attack vectors by sector



Source: ENISA THREAT LANDSCAPE 2025

Increase in attacks in major sectors



Źródło: ENISA THREAT LANDSCAPE 2025

Entity qualification

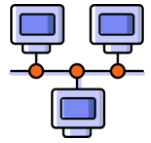
- What is the qualification of important and essential entities?
- How to identify sectors?
- How do I submit an application for entry?

Essential Sectors in NIS2

Power engineering

Public administration

Health care



Digital infrastructure

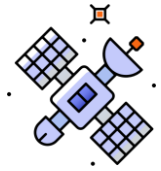
Drinking water supply and distribution

Transport

Banking and financial market infrastructure

ICT service management

Sewage



Outer space

Important Sectors in NIS2

Postal services

Digital service providers

Production and
Distribution of Chemicals

Waste management

Scientific research

Production
(medical devices, computers, electronics, machines, devices, cars, transport equipment)

Food Production and
Distribution

The important entity and its service

In the context of NIS2, a “service” is an activity provided by an entity that is of significant importance to the functioning of the economy or society, but is not classified as the most critical (these belong to key sectors).

- The service in the important sector is:
  - important for society or the economy
  - provided by a medium or large enterprise
  - dependent on IT systems
  - potentially exposed to cybersecurity incidents

Threats in the era of the NIS2 directive

Threats from employees

- Accidental infections by malware, ransomware, viruses, botnet,
- Leaks of personal data on USB drives
- Installing risky applications on workstations
- Unauthorized system access, dangerous employees

Threats from infrastructure

- Outdated software,
- No supervision of network events, no event logging
- Unmonitored critical systems
- Backup system vulnerabilities

Implementation Timeline

01 COMPLETE

Effective Date

19 Jun 2025

ZInfV-1 enters into force, transposing NIS 2 into Slovenian law.

02 COMPLETE

Registration

19 Dec 2025

In-scope entities self-register with URSIV within 6 months.

03 UPCOMING

Tech. Compliance

19 December 2026

Full technical security measures implemented per Article 21.

System construction and security implementation

- How to build an ISMS?
- How to identify risk?
- What safeguards are adequate?
- What safeguards are provided by the regulations?

New responsibilities at NIS2

General rules

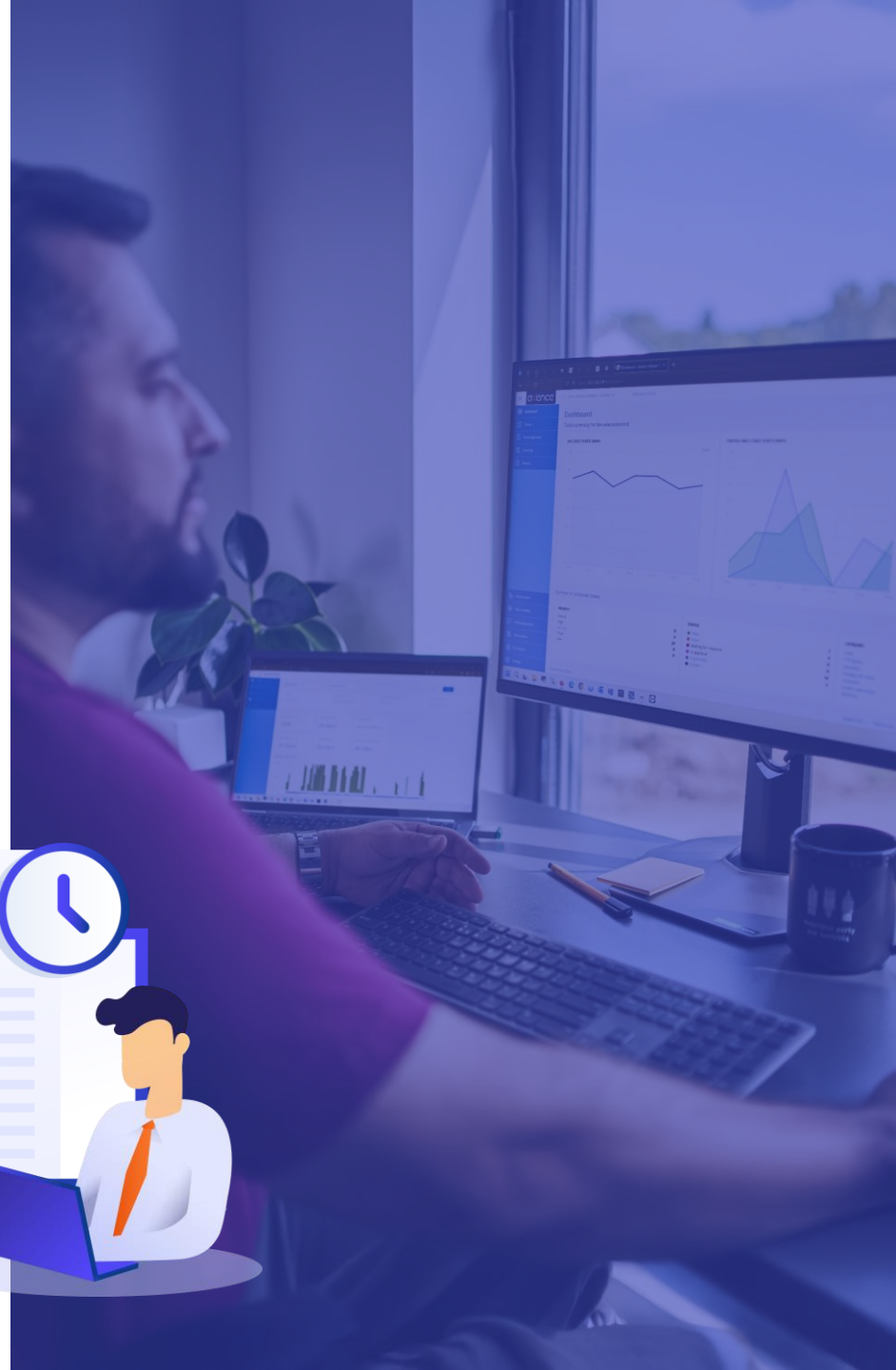
Required Resources

- Risk analysis and risk management
- Incident reporting to CSIRT
- Implementation of system security policy
- Securing the supply chain
- Development and implementation of a Business Continuity Plan
- Regular staff training in cybersecurity
- Systems architecture
- Audit
- The role of Management

24h/72h Rule

NIS2 Incident Reporting Mechanism

- **Initial notification**
  – withing 24 hour of incident detection
- **Interim report**
  – within 72 hour of incident detection
- **Final report**
  – within 1 month from incident report



Format and content of reports

Quality and completeness of the information provided

- Date and time of the event and detection
- Type of incident
- Scope and scale
- Impact and consequences
- Root cause
- Actions taken and planned next steps

The process of notifying cyber incidents in the organization

Preparation and implementation

- Defined roles and responsibilities
- Integration of NIS2 requirements into IR procedures
- Automated detection and alerting
- Maintaining readiness for communication with CSIRT
- Staff training and exercises
- Cooperation with external entities

Surveillance measures in NIS2

Surveillance tools

- On-site inspection and remote monitoring
- Independent and targeted security audits
- Requesting information, access to data and documents
- Issuing warnings regarding violations
- Issuing binding orders and commands

Penalties in NIS2

Possible consequences and penalties

- Temporary suspension of certification or authorization
- Temporary ban on holding management positions
- Penalties in the following amounts will/could be imposed on a key or important entity for failure to fulfil its obligations under the Act:
  - In the case of a **essential entity**, up to 10M EUR or up to **2%** of global annual turnover
  - In the case of an **important** entity, up to 7M EUR or up to **1.4%** of global annual turnover
- **Periodic penalty for each day of delay** – if the authority issued a warning or decision and the entity does not comply with it
- Management has obligations

The most important benefits of having Axence nVision®

You will meet legal requirements

- Mechanisms supporting the application of the GDPR
- ISO 27001 certified supplier, not on the DWR list
- Solutions supporting the NIS2 directive

You will reduce costs

- Information about network failures and problems before they occur
- Full knowledge of unused software

You will minimize the risk of penalties

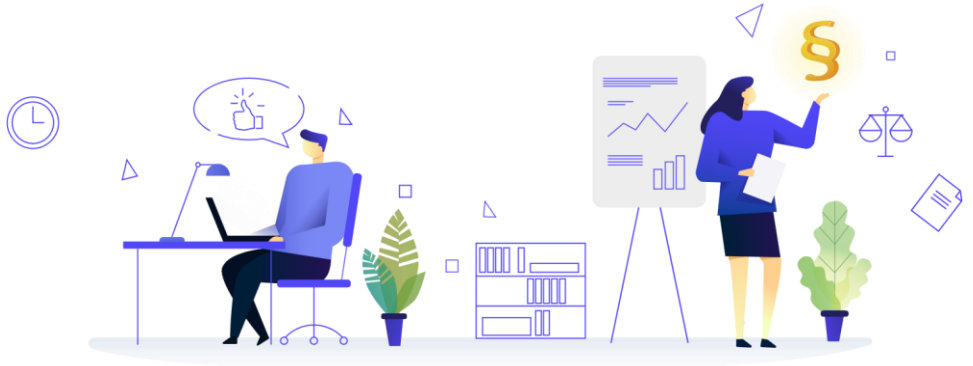
- For acting in accordance with directives and laws
- For data leaks

You will ensure the security of your company

- Blocking dangerous websites and applications
- Solutions supporting the ISO 27001 standard
- Control over access to resources

You will organize remote work

- Secure, encrypted access to your company computer
- Remote technical support system for employees
- Monitoring work efficiency



nVision

axence®

$5,600

Network downtime / per minute

$1,2 m

Overspend & Shadow IT

$4,45 m

Per data breach

*IBM – Cost of data breach report
*Flexera – State of IT Asset Management Report

Your IT.
Your Modules.
Your Rules.

One product | Six modules

Single database

Network

ITSM | ITAM | CMDB | Endpoint management & Cybersecurity

78%

admins rated real-time monitoring as most useful function

Agentless devices discovery	Treshold alerts via Teams / Slack / SMS	Live auto-generated topology maps	Critical service auto-restart

Pain Point

Solved

✕ Unauthorized device joined network	→	Auto-discovery fires alert immediately ✓
✕ Network failure location unknown	→	Topology highlights the failed node ✓
✕ Critical service crashed at 3am	→	Auto-restarts without human intervention ✓
✕ Fixing before users notice problems	→	Proactive threshold alerts & automation ✓
✕ No historical network event record	→	Full searchable timestamped event log ✓

Inventory

ITAM | SAM | CMDB | Endpoint management & Cybersecurity

88%
of public organizations run unlicensed software

Full HW, SW & OS Audit per endpoint	Owned & Installed licenses count	MSI remote software deploy and removal	Automatic asset registry

Pain Point

Solved

✕ No visibility of installed software estate	→	Full audit runs automatically per endpoint ✓
✕ License compliance unknown before audit	→	SAM shows over-deployment in real time ✓
✕ Software rollout to 200 machines takes days	→	Push MSI from console in minutes ✓
✕ Auditor requests asset register, nothing exists	→	Inventory built it automatically already, export ✓
✕ EOL software running somewhere undetected	→	Flagged continuously, not just at audit ✓

Helpdesk

ITSM | ITAM | Knowledge | Support

#1

rated module of nVision

Ticketing with SLA tracking	Buil-in remote desktop	Application Kiosk	Konwledge base | Whistleblower channel

Pain Point

Solved

Security incident needs all-staff notification	→	Desktop Alert hits every screen instantly
Remote endpoint needs support, no tools	→	Built-in remote desktop, zero extra cost
Ticket queue unfairly distributed	→	Auto-routing rules balance it automatically
Users bypassing IT to install software	→	Kiosk creates a controlled approval channel
No asset context when ticket opens	→	Inventory asset linked directly to ticket

Users

CMDB | SAM | UAM | Endpoint management & Security

90%

cyberattacks begins with only phishing

Websites and Apps blocking by policy	Bandwidth monitoring and control	After-hours activity alerts	Full GDPR-Compliant per-user activity log

Pain Point

Solved

- Malicious sites reached on managed devices → Category-based blocking enforced at endpoint
- Data exfiltration suspected, nothing to prove it → User activity log is the forensic record
- Unauthorized applications running on endpoints → Process blocking enforced silently, centrally
- HR investigation needs user activity evidence → Per-user log exports on demand, GDPR-clean
- Bandwidth consumption source unidentified → Per-user tracking shows it live and historically

DataGuard

CMDB | ITAM | Endpoint management & Security

Not content DLP - device control
+ files & paths audit

USB and removable media device policy	File operations - who, what, when, where	Defender / Firewall compliance	BitLocker enforcement across endpoints

Pain Point → Solved

Pain Point	Solved
Unknown devices connecting to endpoints	Only approved devices allowed, enforced centrally
File copied or deleted, no record who did it	Every file operation logged with full attribution
Endpoint encryption status unknown	BitLocker status visible and enforceable remotely
Defender turned off on some machines	Non-compliant endpoints surfaced automatically
NIS2 requires endpoint protection evidence	BitLocker and Defender logs ready for auditor

SmartTime

Work time & Productivity

Objective data for IT & HR - not surveillance, no guesswork

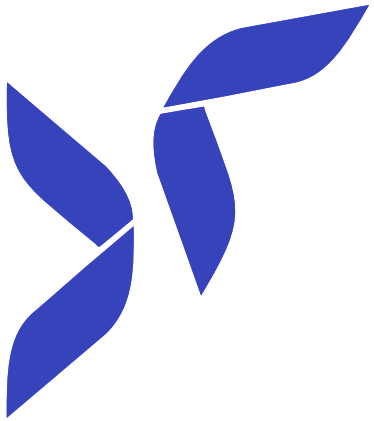
System-level active vs idle time tracking	Productive, unproductive app classification	Private time – disable possible

Pain Point

- Remote worker productivity unverifiable
- Overtime dispute, no neutral data source
- Monthly attendance reports take hours

Solved

- Active time recorded at system level
- SmartTime log is the neutral reference
- Visible for manager in seconds



Bonus

Admin Center

Web dashboard | Reports

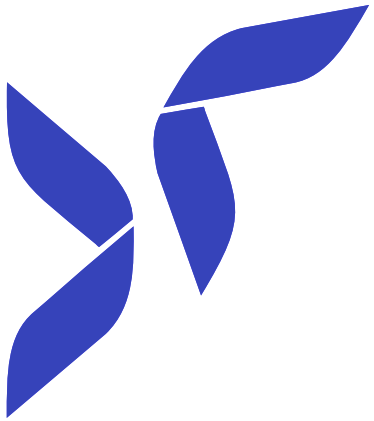
Browser based – any device, no VPN	Shareable read-only dashboard links	Live + Historical data	All modules aggregated in selective views

Pain Point

- Scattered data across tools
- Critical incidents unnoticed
- Risky stakeholder data exposure

Solved

- Unified web browser dashboard
- Automatic real-time or historical data
- Read-only secure sharing



Bonus II

NIS2 Compliance map

Obligation → Module

	INVENTORY	NETWORK	HELPDESK	DATAGUARD	USERS
Risk Analysis & Asset Identification	✓				
Incident Management & Detection		✓	✓		
Cybersecurity Training & Hygiene			✓		
Business Continuity & Crisis Management		✓	✓		✓
Supply Chain Security	✓				
Vulnerability Management	✓				
Cryptography & Encryption Policies				✓	
Access Control & Personal Security	✓			✓	✓
Incident Reporting Deadlines			✓		

What it is.

What it’s not.

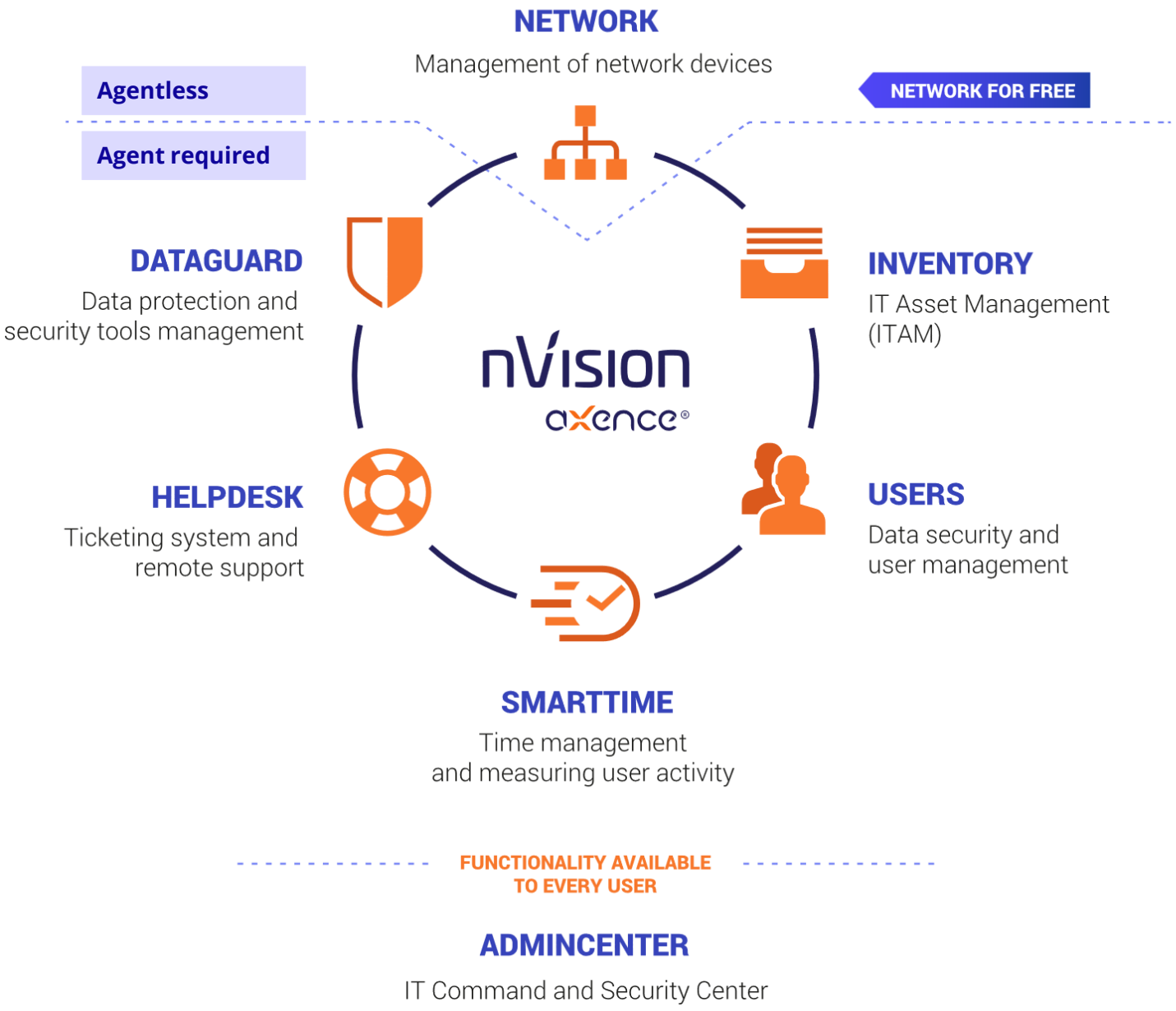
Where it fits?

Windows-based environment	→	20-5000 endpoints
Operating infrastructure	→	On-premise
NIS2 / cybersecurity audit	→	Needed / In progress
Multi-location	→	Centralized remote support
No SaaS subscription	→	Perpetual license

Where to be upfront?

✕ No patch management (yet)	→	Inventory shows which OS version is installed on every machine
✕ DataGuard ≠ DLP	→	Device control + file & path audits only
✕ Windows-first today	→	MacOs / Android on the roadmap
✕ Not MSP native	→	1 installation per customer / doable but no data separation in HelpDesk

Don’t be like Josh



Pick & choose

- IT Service Management (ITSM)
  Network, Helpdesk
- IT Asset Management (ITAM)
  Network, Helpdesk, Inventory, Dataguard
- Configuration Management Data Base (CMBD)
  Network, Helpdesk, Inventory, Dataguard, Users
- Software Asset Management (SAM)
  Network, Helpdesk, Inventory, Dataguard, Users
- Service Desk
  Helpdesk
- Endpoint Management & Security
  Network, Inventory, Dataguard, Users

Licensing
Network + Any module

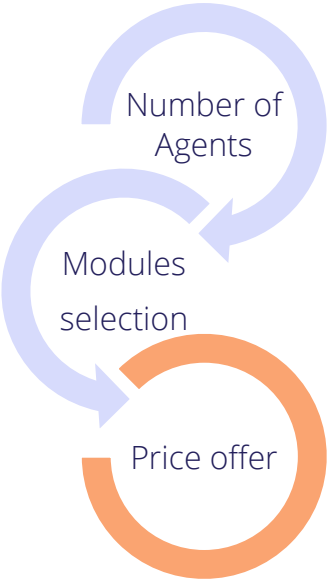
Axence nVision® PRO - licensing

Module	Agents (monitored workstations / users)	
	Min / Max	Increment
Network (Agent less)	--- / ---	---
Inventory	20 / ---	1
Users	20 / ---	1
Data Guard	20 / ---	1
Help Desk	20 / ---	1
Smart Time	20 / ---	1

Flexible module configuration

one Agent = number of workstations or users sesions at a the time

it determines how the number of AnV Agents is calculated for standard workstations and Windows terminal servers



New License (NL)

Service Agreement (SA) continuation of the service contract without interruption, 20% current cost

0 1 2 3 4 5 6 7 8 9 10 11 12 1 2 3 4 5 6 7 8 9 10 11 12 1

[month]

Extensions (EXT) – modules or Agents - possible to buy at any time

Upgrade (UPG) without SA continuation, 60% current cost

Axence nVision® licenses types

License type	Validity	Complimentary bonus	Remarks
PRO	perpetual	• Network module • maintenance support for 12 months • software update for 12 months	After initial 12 months the maintenance support and software update available in annual subscription model.
Test License	1-3 months	• maintenance support	For potential clients / registered projects
Trial License	1 months	• maintenance support	For potential clients who want to test nVision (self registration on Axence website)

- ☑ number of monitored network devices (Network) > **unlimited**
- ☑ number of administrator / operator > **unlimited**
- ☑ remote Axence nVision® administration consoles > **unlimited**

Thanks!

Mariusz Maślanka