AXS | GUARD

CYBERSECURITY WITHOUT WORRIES
ALWAYS & EVERYWHERE

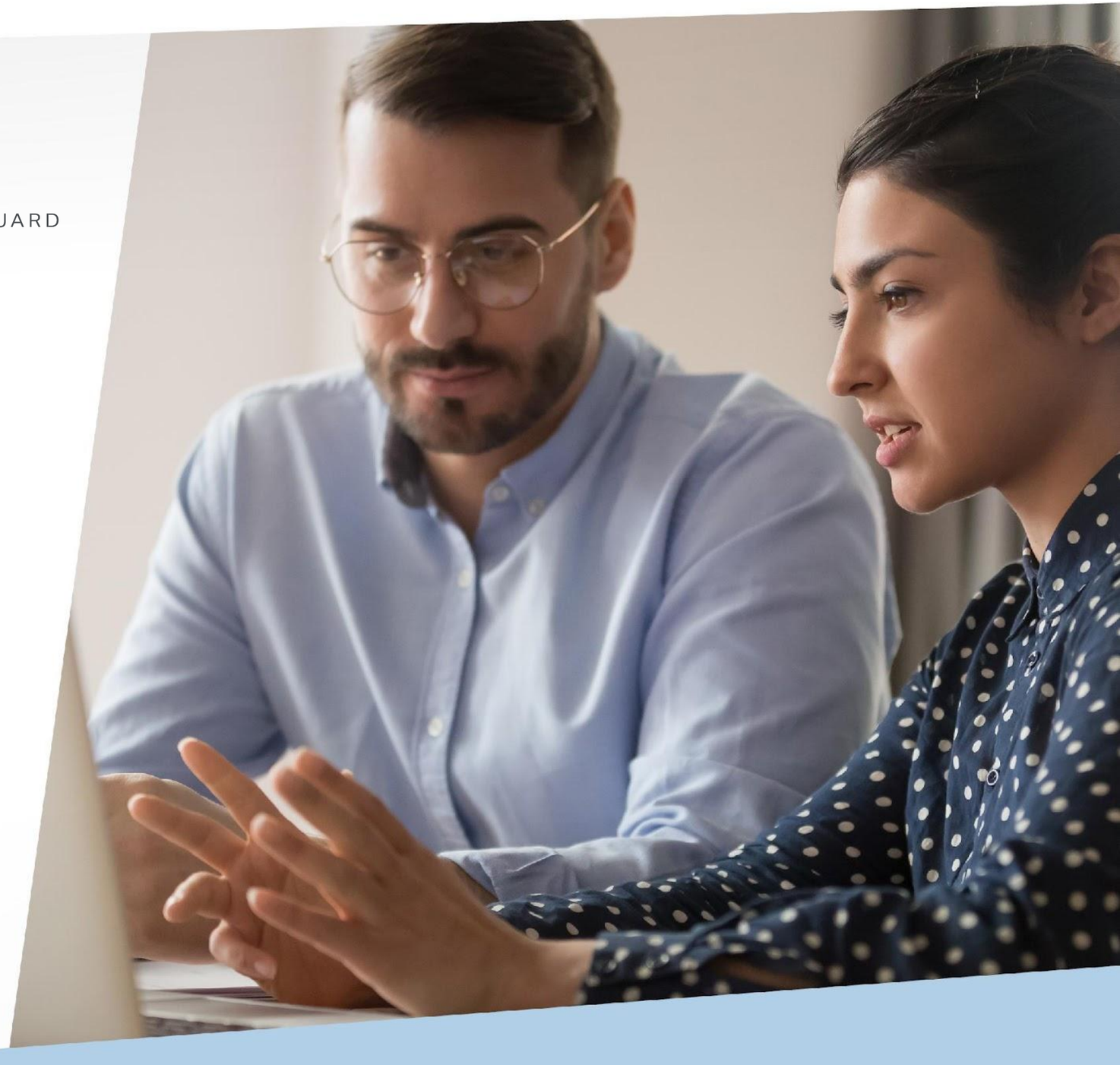
# AI use cases in network security

Alex Ongena
CEO AXS Guard

## WHO

# Over 25 years of expertise and local leadership in cybersecurity.

- Founded by Alex Ongena in 1996.
- Ahead of our time from the start with avant-garde security solutions.
- Continuous innovation in an ever-evolving cybersecurity landscape.
- Acquired twice over the years, proudly independent again since 2017.
- Protecting +1500 customers.
- Developed in Belgium



## WHAT

# AXS Guard's worry-free platform is a managed Cybersecurity platform that secures employees, sites and IT infrastructure.

We offer a 'zero trust' approach: restricting access controls to anyone we do not know, without sacrificing performance and user experience. Never trust, always verify.

The AXS Guard platform covers the full spectrum of cybersecurity, including:

- **Connectivity - VPN**
- **Application Security**
- **Network Security**
- **Access Protection - 2FA**
- **Content Protection**
- **Device Protection**

# AXS Guard protects your company on these fields

CONNECTIVITY

ACCESS PROTECTION

NETWORK PROTECTION

APPLICATION PROTECTION

CONTENT PROTECTION

DEVICE PROTECTION

# AXS Guard connects you!

CONNECTIVITY »

- Connecting your company sites with each other and/or the cloud, remote access through VPN or secure homeworking

- Multiple internet connections
- Load Balancing
- Internet Failover
- Dedicated Routing (VOIP)
- Bandwith management

# AXS Guard knows who you are

ACCES PROTECTION »

- With AXS Guard, you always **know who does what and when** on your network and you are in full control of who has access to which application and when.

  This can be usefull when you want different policies at the office and via remote access through VPN.

- RADIUS server
- Strong and 2FA authentication: OATH & digipass
- Integration with Directory services (LDAP)
- Brute Force Attack Protection

# Security is only as strong as its weakest link!

NETWORK SECURITY »

The Next Gen Firewall that secures incoming and outgoing internet traffic.

The intrusion prevention system (IPS & IDS) closely monitors all network traffic to quickly detect and block suspicious network activity.

- Next-Gen Firewall
- Automatic blacklist updates
- Intrusion Prevention System
- Network Threat Prevention System

# An extra security layer between your users and your applications.

APPLICATION SECURITY »

- Shield your HR-applications, customer portals and webshops in the most secure way.

- Application Firewall
- Reverse Proxy Server
- Strong and 2FA authentication: OATH & digipass
- SSL offloading

# AXS Guard keeps your incoming and outgoing data secure

CONTENT SECURITY »

Control and monitor all mail and web traffic. Decide who, when and which applications are aloud.

- Web content scanning
- Anti-spam
- Anti-malware
- URL scanning
- Malware pattern updates

# WE ARE AVAILABLE ON THESE PLATFORMS

HARDWARE »

VIRTUAL »

CLOUD (AZURE) »

# AXS Guard Appliances

HARDWARE >>



Cybersecurity

# What does it mean?

- Protect assets & users against
  - information theft
  - identity theft
  - extortion & hostage
  - computer damage & down time
  - reputational damage
  - ...

## Applicability & feasibility

# Domains where AI might help

- Network traffic
- Email traffic
- Web access
- Endpoint Protection

Applicability & feasibility

# Stages of the project

- Use case discovery
- High Level analysis => go / no go
- Data collection & human analysis
- Feature extraction & POC implementation
- Model training & optimization
- Result Analysis

Applicability

# Network traffic

- Goal: filter “benign” from “malicious” traffic
- Problem: labeling of data
  - No practical way to label large amount of packets
  - Unsupervised training?
    - too complex to start as a first project….

Applicability

# Email traffic

- Goal: block malicious content
- Succes!
  - labeling of data by existing scanners
  - 30+ features available
  - large datasets for training & validation
  - by using the “ensemble” ML model
- Performance 1000 samples, ML decision < 50 ms.

Applicability

# Webaccess

- Goal: block malicious downloads
- No luck so far:
  - Very few features available
  - Limited datasets with malicious samples
  - Large impact on user experience

Applicability

# Endpoint Security

- Goal: detect & stop malicious behavior
- Succes!
  - Many features available
  - Large datasets of malicious samples

Applicability & feasibility

# Future research

- Authentication auto-lock / unlock
- Dynamic Authentication Policies
  - 2FA only when in doubt to raise User Experience
  - ...
- ...

Conclusion

# AI to the rescue in [network] CyberSecurity?

Yes…

- Domain expertise is key
- Applicable to real-time webaccess alike traffic uncertain
- Excellent when large **labelled** datasets are available
  - Email
  - Endpoint Security

# THANK YOU
# &
# Questions?

**Alex Ongena**
**alex.ongena@axsguard.com**

AXS | GUARD