NEXT-GEN SECURITY AWARENESS SERVICE

STRENGTHEN YOUR HUMAN FIREWALL

HORNETSECURITY

Agenda

- Why is security awareness so important?
- Product overview - This is new!
  - Patented Spear-Phishing
  - ESI® - Employee Security Index: makes security behavior measurable
  - Demand-driven e-training
  - Control Panel - Awareness Dashboard & Security Hub
- Live Demo
- Security Awareness Suite – Key Features at a glance

HORNETSECURITY

YOUR PRESENTER TODAY

Andy Syrewicze has been in the IT Industry for more than 20 years, is a Microsoft MVP, VMware vExpert and currently a Technical Evangelist for Hornetsecurity.

Andy Syrewicze
Technical Evangelist
Microsoft MVP and VMware vExpert
Mastadon - @andysandwich@infosec.exchange

YOUR PRESENTER TODAY

Bernardo Reyes has been in the IT Industry for more than 15 years helping partners grow their MMR revenue via cloud and security products.

Bernardo Reyes
Partner Account Manager
reyes@hornetsecurity.com

HORNETSECURITY – LEADING CLOUD EMAIL SECURITY, COMPLIANCE, AND BACKUP PROVIDER

- Our portfolio
  - 365 Total Protection - Covers all aspects of security for Microsoft 365: from spam, malware, and threat protection, compliance and email management, to backup and recovery
  - 5,000+ partners & 50,000+ customers worldwide

- About Hornetsecurity
  - In-house development: From the initial idea to the final product, our services are planned, conceived, and developed in house
  - In-house support in our offices in German, English, Spanish, and French
  - Security Lab: 24/7 monitoring of email traffic; continuous evaluation, analysis, and reporting of email threats

HORNETSECURITY WORLDWIDE

HOW IT ALL STARTED – OUR STORY

HORNETSECURITY

2007 — Ready for **Take Off**

2008 — Beginning of **internationa-lization**

2010 — Presence in more than **10 countries** with over **200 sales partners**

2013 — Over **25,000 companies** as customers

2014 — **Market leader in Germany;** Awarded with Deloitte Technology **Fast 50 Award**

2015 — antispameurope becomes **Hornetsecurity**

2016 — **Over 550 resellers worldwide**

2017 — 10 years of Hornetsecurity; **Foundation of US subsidiary**

2018 — Acquisition of AVIRA Spamfilter division; **Market leader in German-speaking region**

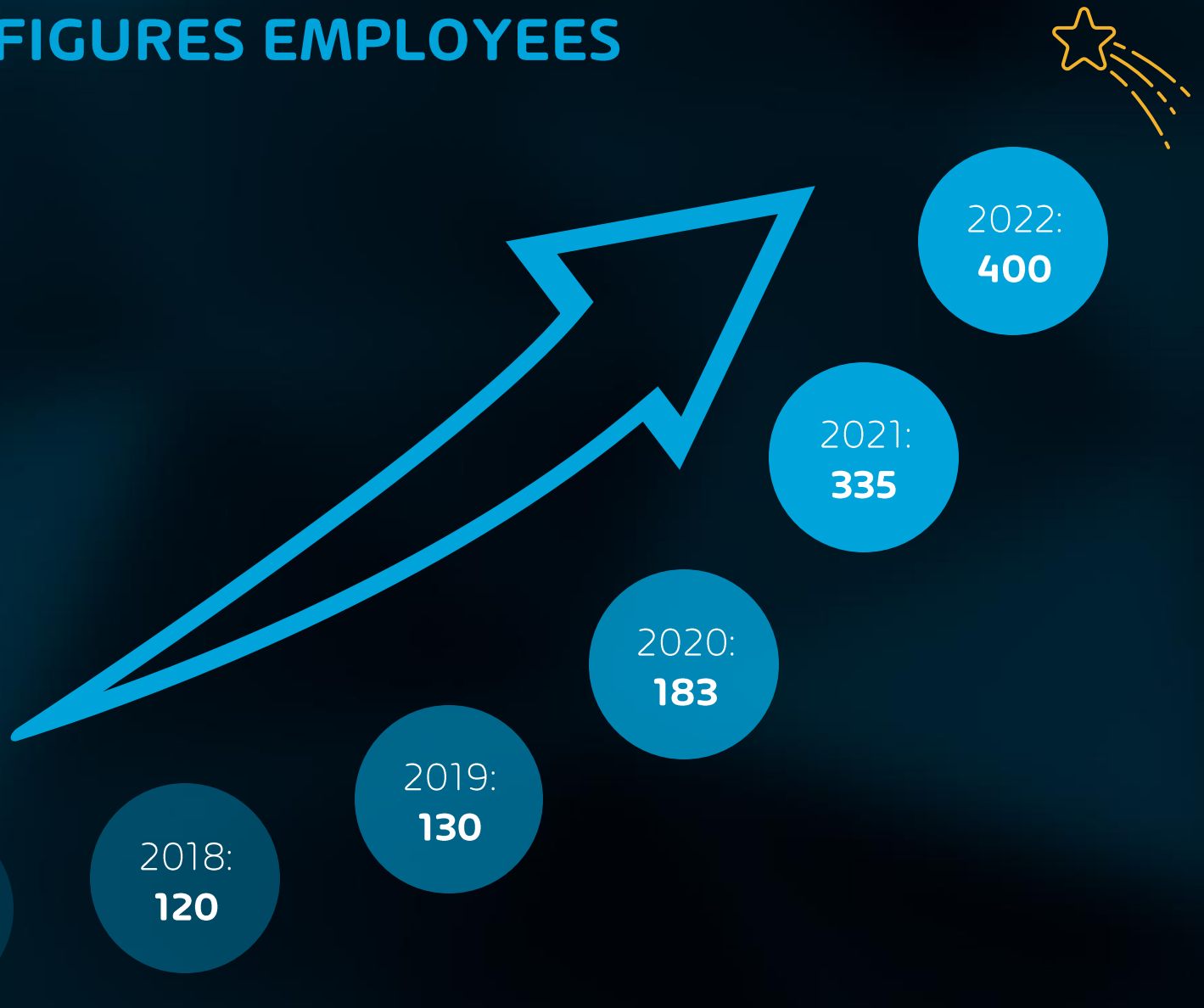
2019 — Partnership with Swisscom; **Acquisition of Spamina**

2020 — **Acquisition of EveryCloud**

2021 — Acquisition of **ALTARO;** Acquisition of **ZEROSPAM**

2022 — **Acquisition of IT-Seal**

GROWTH FIGURES EMPLOYEES



HORNETSECURITY

NEXT-GEN
SECURITY AWARENESS SERVICE

STRENGTHEN YOUR HUMAN FIREWALL.
FOR A SUSTAINABLE SECURITY CULTURE.

HORNETSECURITY

THE LACK OF A SECURITY CULTURE LEADS TO IMMENSE DAMAGE

"I'm not going to be attacked anyway."
Maria (28) — HR Manager

"Our IT is already taking care of that."
Roland (41) — Controller

"I have more important things to do than worry about IT security."
Gabi (54) — Head of Sales

\+ Working from home will continue to become more prevalent

95% of all cyber security incidents are caused by human error.

Source: World Economic Forum - The Global Risks Report 2022

IT security: Humans are risk factor No. 1

HORNETSECURITY

WHY IS SECURITY AWARENESS SO IMPORTANT?

THAT IS WHY PURELY TECHNICAL MEASURES ALONE ARE NOT ENOUGH. Some examples:

- Employees access business applications via their own inadequately secured devices and premises, e.g. in the home office
- They use business devices to surf the web or check e-mail privately

- They receive phishing calls and are contacted on social networks by fake profiles
- They overestimate their own capabilities to protect themselves from cyber attacks

- They don't know what to do when they observe a security incident

HORNETSECURITY

PSYCHOLOGICAL BACKGROUND: SECURITY AWARENESS

Kahneman: Subdivision of human thinking into

- System 1 ("fast thinking"): experience-based, automated information processing, intuitive, and automated actions
- System 2 ("slow thinking"): deliberative, rational, analytical behavior for evaluating major decisions

REQUIREMENTS FOR A SUSTAINABLE SECURITY CULTURE

HORNETSECURITY

MINDSET

Motivation and open communication

- Understanding of threat situation
- Emphasize personal responsibility

Communication aids for all stakeholders

SKILLSET

Acquire skills and knowledge

- Phishing-Simulation
- E-Learning
- Short Videos

Awareness Materials

TOOLSET

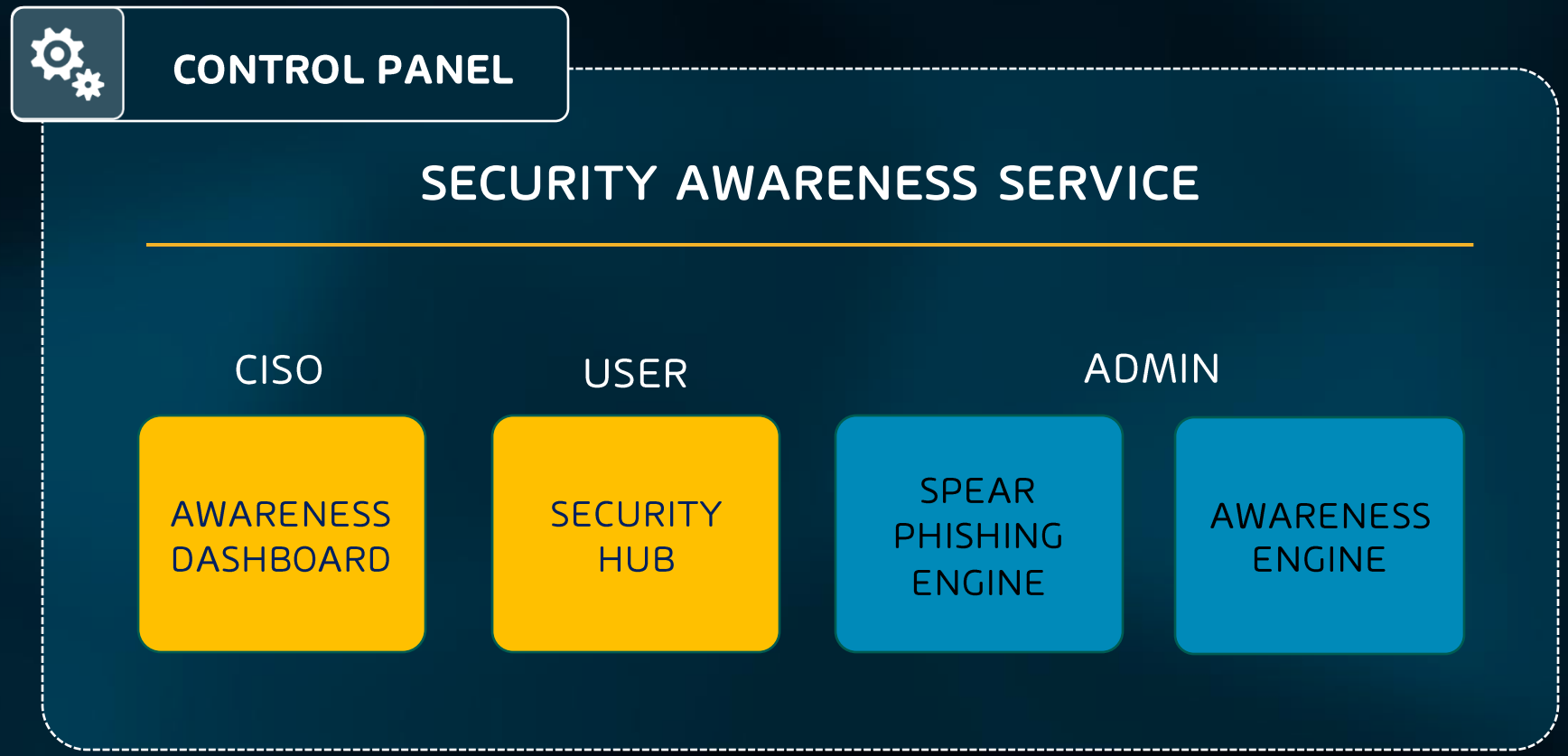
Actively get involved in taking action

- Live-Dashboard
- Incident reporting chains

Reporter-Button
Outlook Add-In

PRODUCT OVERVIEW

HORNETSECURITY



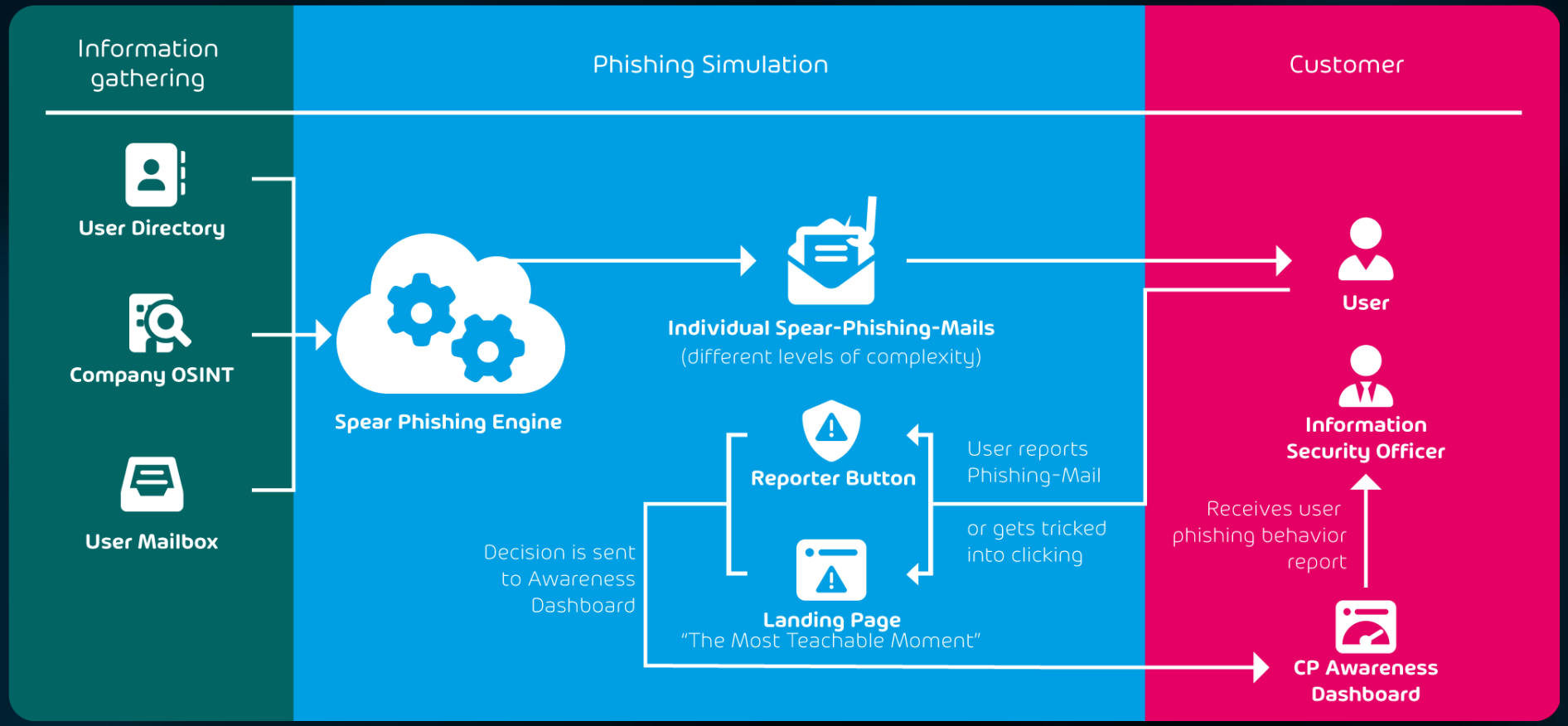
PATENTED SPEAR-PHISHING ENGINE

Level	Prep Time	Example
1	ca. 15 minutes	Typical mass phishing e-mail such as the order confirmation of a well-known shopping portal
2	ca. 1 hour	Alleged email from the CxO (CEO Fraud)
3	ca. 2 hours	Spear phishing e-mail including public information about the company, e.g. from job rating portals
4	ca. 4 hours	Spear phishing email with reference to the recipient's department and job position, email from direct colleagues or managers
5	ca. 6 hours	Spoofed email from a business partner who has not enabled email spoofing protection or has had an account hacked
6	ca. 12 hours	A business partner or colleague has been hacked: email of a personal contact responding to a previous email conversation
7	More than 20 hours	Spear phishing email related to topics the recipient is working on, such as a status update on an ongoing project the recipient is involved in

HORNETSECURITY

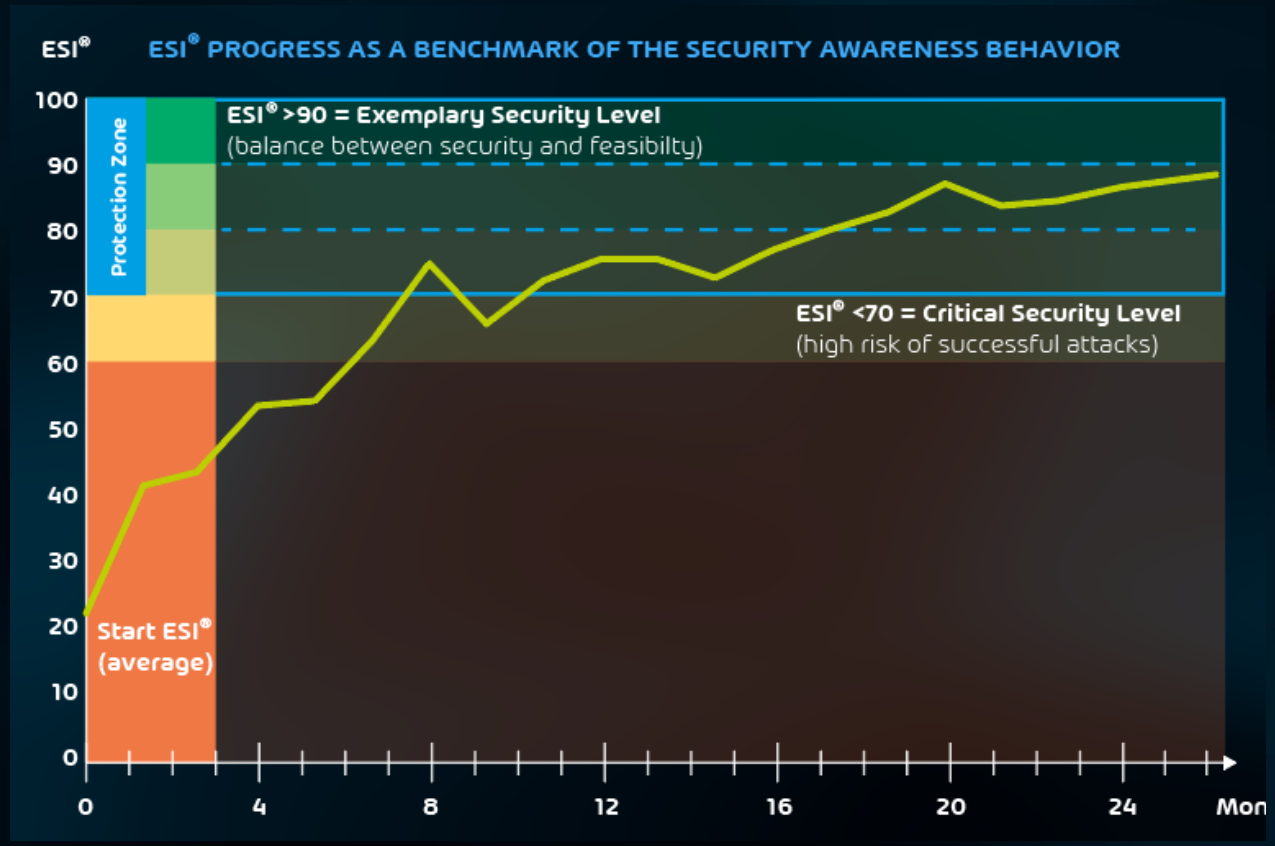
PATENTED SPEAR-PHISHING ENGINE

SPEAR PHISHING SIMULATION FLOW



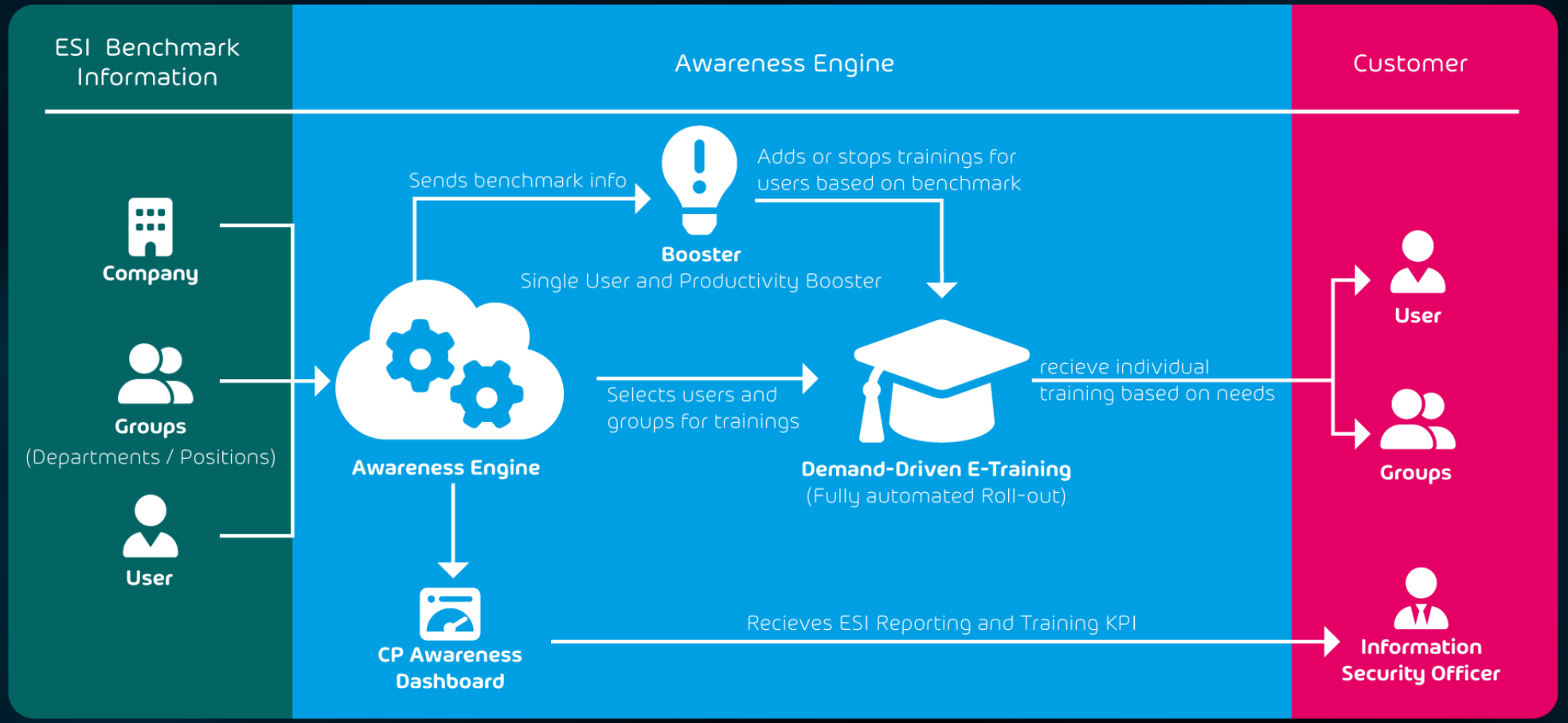
ESI® - EMPLOYEE SECURITY INDEX

- ESI® - A scientifically based and patented method to make employee security behavior measurable.
- The ESI® Awareness Benchmark enables standardized, transparent measurement and management of security behavior at the enterprise, group, and user levels.



AWARENESS ENGINE

AS MUCH TRAINING AS NECESSARY, BUT AS LITTLE AS POSSIBLE



HORNETSECURITY

LIVE DEMO

- Start with Phishing E-Mail
- Most Teachable Moment
- Security Hub
- Awareness Dashboard

SECURITY AWARENESS SERVICE
KEY FEATURES AT A GLANCE

HORNETSECURITY

Awareness Engine – Key Features

- Auto Training Mode: Learning content is automatically rolled out to users and groups on demand.
- Single User & Productivity Booster: Users with additional learning needs are trained more intensively; users at a very good security level, on the other hand, are trained less.
- Automatic onboarding of new users (requires LDAP/AD Sync.)
- Manual Training Mode: There is an option to manually roll out training modules to the groups and users.

SECURITY AWARENESS SERVICE
KEY FEATURES AT A GLANCE

HORNETSECURITY

Spear Phishing Engine – Key Features

Automatically generated, individually tailored spear phishing attacks with different difficulty levels. Incl. fake login pages and file attachments with macros.

Level 7 – Incl. Hidden Reading of Mailbox	✓
Level 6 – Incl. E-mail Response History	✓
Level 5 – Incl. Spoofing Domains	✓
Level 4 – Incl. Job-Position + Department	✓
Level 3 - Company-OSINT	✓
Level 2 - Spear-Phishing from C-Level	✓
Level 1 - Mass-Phishing	✓

✓ Level 6 & 7 Phishing scenarios planned for later expansion.
Prerequisite: Spam and Malware Protection or 365 Total Protection required.

WE PROTECT YOU

HORNETSECURITY

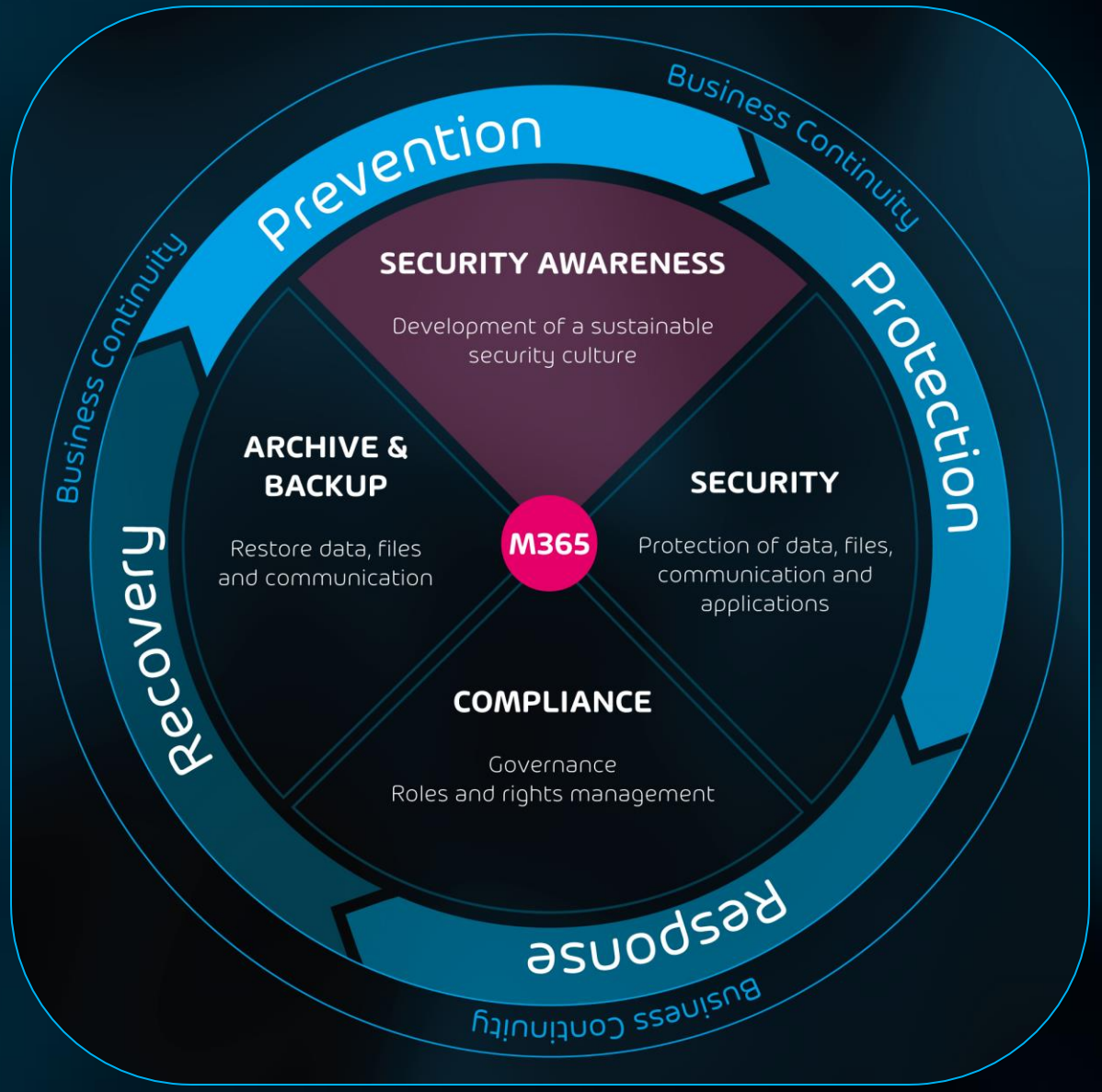
DOCUMENTS & MATERIALS AVAILABLE IN THE PARTNER PORTAL

- ✓ Marketing Materials
- ✓ Service Description
- ✓ Offer generator
- ✓ Offer Template
- ✓ Whitepaper
- ✓ Pricelist

Partner Portal Registration

HORNETSECURITY

ENRICHING THE MICROSOFT 365 SOLUTION WITH HORNETSECURITY'S PRODUCT PORTFOLIO



HORNETSECURITY

HORNETSECURITY

How Would You Like Us to Follow Up?

1

Sign me up for your newsletters!

2

I'd Like a Free Trial of 365 Total Protection!

3

Schedule an individual appointment with one of our experts

4

Sign Me Up for More Content!

*Type your selection in the Q & A Box!

ASK A QUESTION!

Do you have questions or input of your own?

HORNETSECURITY