



# Next-Gen Vulnerability Management

Be one step ahead of cybercriminals

## AGENDA

- Presentation of participants
- Holm Security
- Our platform & uniqueness
- Demonstration
- Next steps



# Next-Gen Vulnerability Management



**700+ customers**

90% recommend  
**Gartner®**



# STRONG PERFORMER



## Holm Security VMP Reviews

by Holm Security in Vulnerability Assessment  
4.4 ★★★★★ 42 Ratings

5.0 ★★★★★ Aug 4, 2021

### Easy to use, capable, and constantly improved Vulnerability Management platform

Reviewer Function: IT Security and Risk Management    Company Size: 50M - 250M USD    Industry: Manufacturing Industry

The Holm Security platform is a great fit for our organisation and has helped us to better control vulnerabilities and phishing awareness. Premium support is a valuable addition for us, because it enabled us to reduce some of the work required to set up and improve the platform.

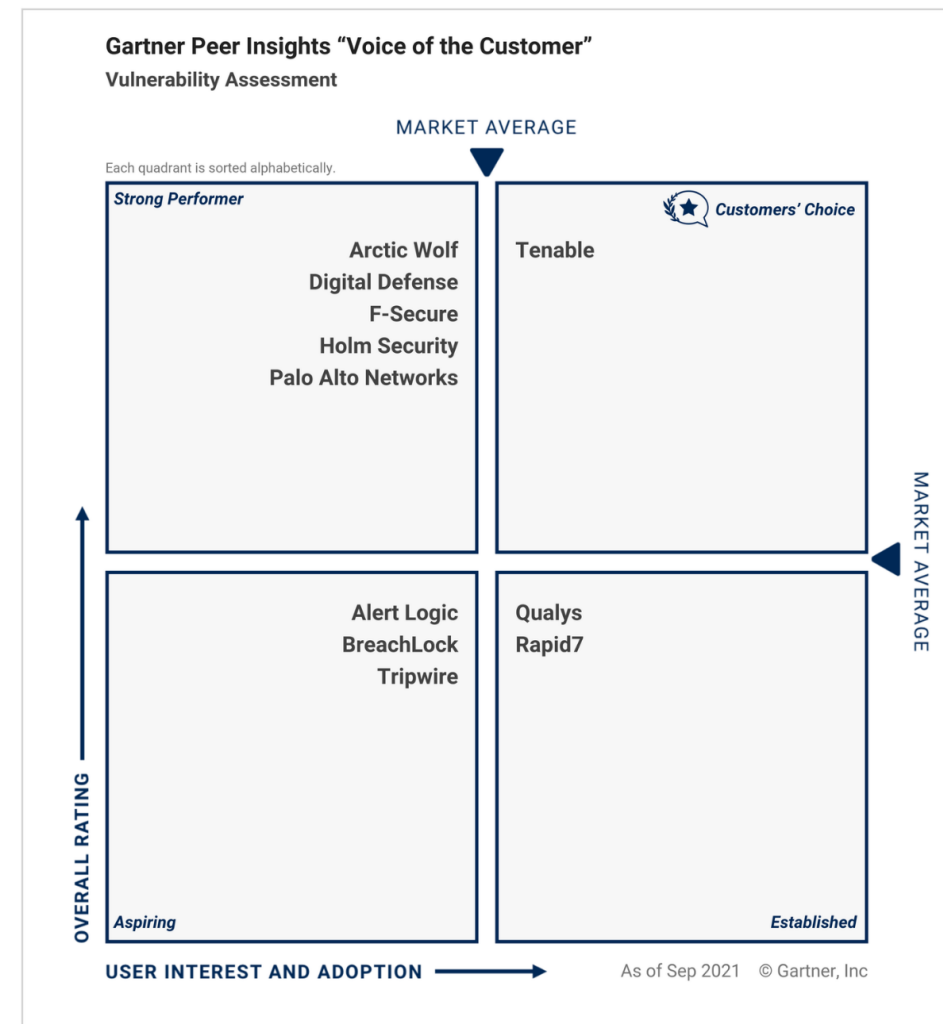
5.0 ★★★★★ Jun 7, 2022

### Helps to learn about potential threats .

Reviewer Role: Analyst    Company Size: 30B + USD    Industry: Finance Industry

Holm security offers security with genuine information into dangers then they react quickly and resist their growth. It also equips staff with the knowledge to spot and respond to assaults when they occur. The whole platform is self contained by saving time.

# Gartner®



[Click here to read more reviews at the Gartner Peer Insight website](#)

Gartner

## CUSTOMER EXAMPLES

**700+  
customers**

**AutoBinck**  
Group



  
**WALLENSTAM**

**stadium**<sup>®</sup>

**VIKING LINE**

  
Strål  
säkerhets  
myndigheten

  
REGION  
SÖRMLAND

  
**ALKION**  
TERMINALS

 **Perstorp**

**bāma**

**Wasa Kredit** 

**ONEMED**

**Intergamma**

*Max Matthiessen*  
Willis Towers Watson

  
**OKQ8**

## THE WORLD OF OUR CUSTOMERS



**Lack of resources**



**Lack of insight & control**



**Reactive cyber security**



**New & existing  
regulatory demands**



**Challenges to  
measure & report**



**Phishing**



**Ransomware**



**Software vulnerabilities**



**Supply chain attacks**



**Cloud misconfigurations**



# Next-Gen Vulnerability Management



## Unparalleled Attack vector Coverage

Cover every corner of your IT infrastructure.



## Attack Surface Management

Stay up to date with your attack surface to make sure it's fully covered.



## Smart Threat Intelligence

Modern telemetry and AI enriching vulnerability data.



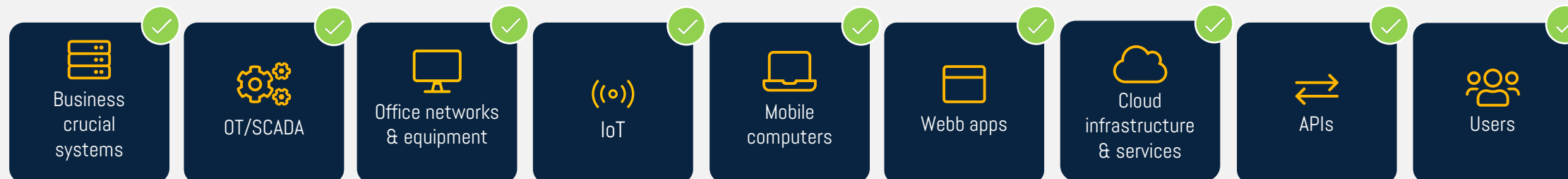
## True Unification

A single pane for all risks for efficient prioritization and remediation.

# ATTACK VECTOR COVERAGE

## Attack surface

### Attack vectors



### Products



Next-Gen Vulnerability Management Platform



# TRUE UNIFICATION

5  
products

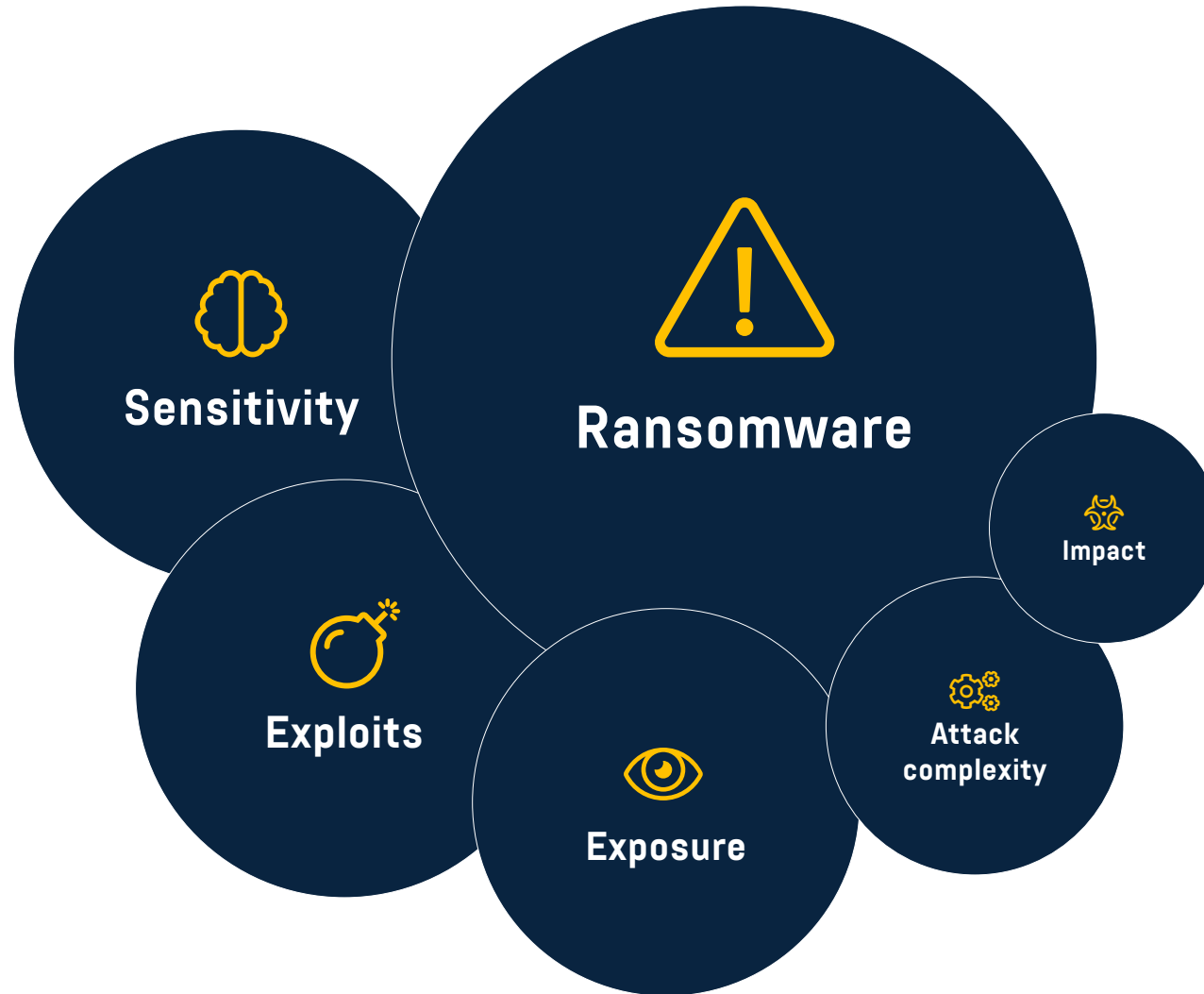


1 platform  
Workflow  
risk model



Time efficient  
Cost efficient





# Best Choice for Data Privacy

Local data storage in your region and  
neutral company control.

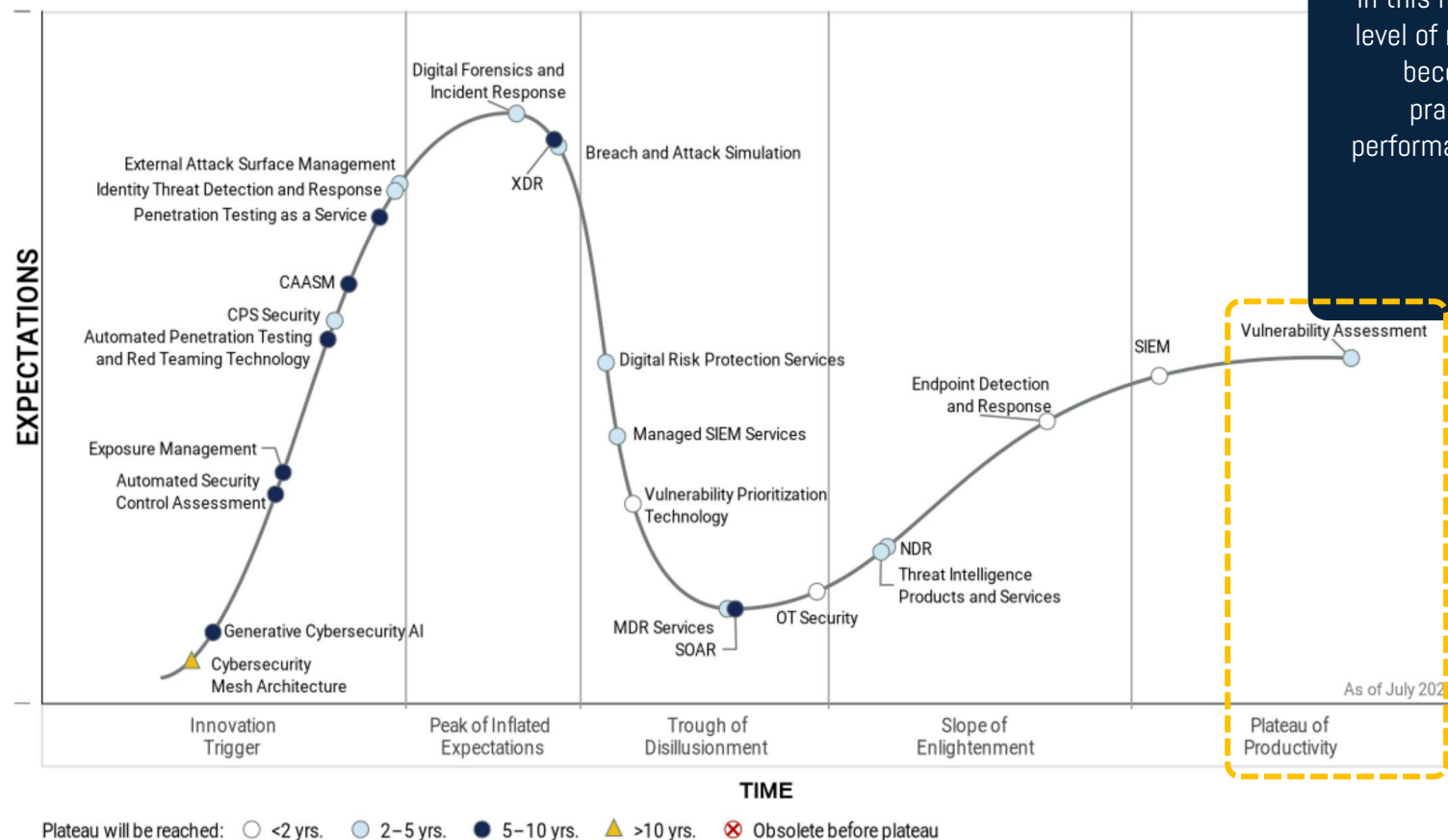


# Meet Compliance

Support meeting compliance like  
NIS/NIS2, DORA, PCI DSS, ISO27001, NIST,  
and local regulations.



## Hype Cycle for Security Operations, 2023

**A proven technology that brings value**

In this final phase, the technology reaches a level of maturity and widespread adoption. It becomes an integral part of industry practices and demonstrates stable performance, delivering measurable business value.

*Gartner*

# PRODUCTS & SERVICES RELATION

Area:	Description:	Competing:	Type:	
			Proactive	Reactive:
Holm Security VMP	Next-Gen Vulnerability Management.	-	✓	
Penetration testing	Cybersecurity assessment and testing technique conducted to evaluate the security of an organization's IT infrastructure, applications, and systems.	Complements	✓	
SIEM	Information & Event Management (SIEM) provides organizations with the ability to collect, analyze, and correlate security event data from various sources across their IT environment.	Complements, integrates	✓	✓
SOC	A Security Operations Center (SOC) is a centralized unit within an organization or outsourced to an IT partner that is responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents and threats.	Complements, integrates	✓	✓
XDR/EDR	Extended Detection & Response (XDR) is a cybersecurity technology and approach that enhances traditional Endpoint Detection & Response (EDR) capabilities by integrating and correlating data from multiple security products across the entire IT environment.	No		✓
Anti-virus	A computer anti-virus is a software program designed to detect, prevent, and remove malicious software, commonly referred to as malware, from a computer or digital device.	No		✓





**Have our experts help  
you achieve your  
goals.**



Training Center



Success Programs



# System & Network Scanning

Finds over 100,000 vulnerabilities across all  
your technical assets.





### Outdated software

Find vulnerabilities in outdated systems and software.



### Misconfigurations

Find misconfigurations in systems, cloud, software, and networks, including policies such as CIS Benchmarks.



### Weak security

Identify weak passwords and encryption in your systems.



### Asset inventory

Gain insight and control over your devices and systems.



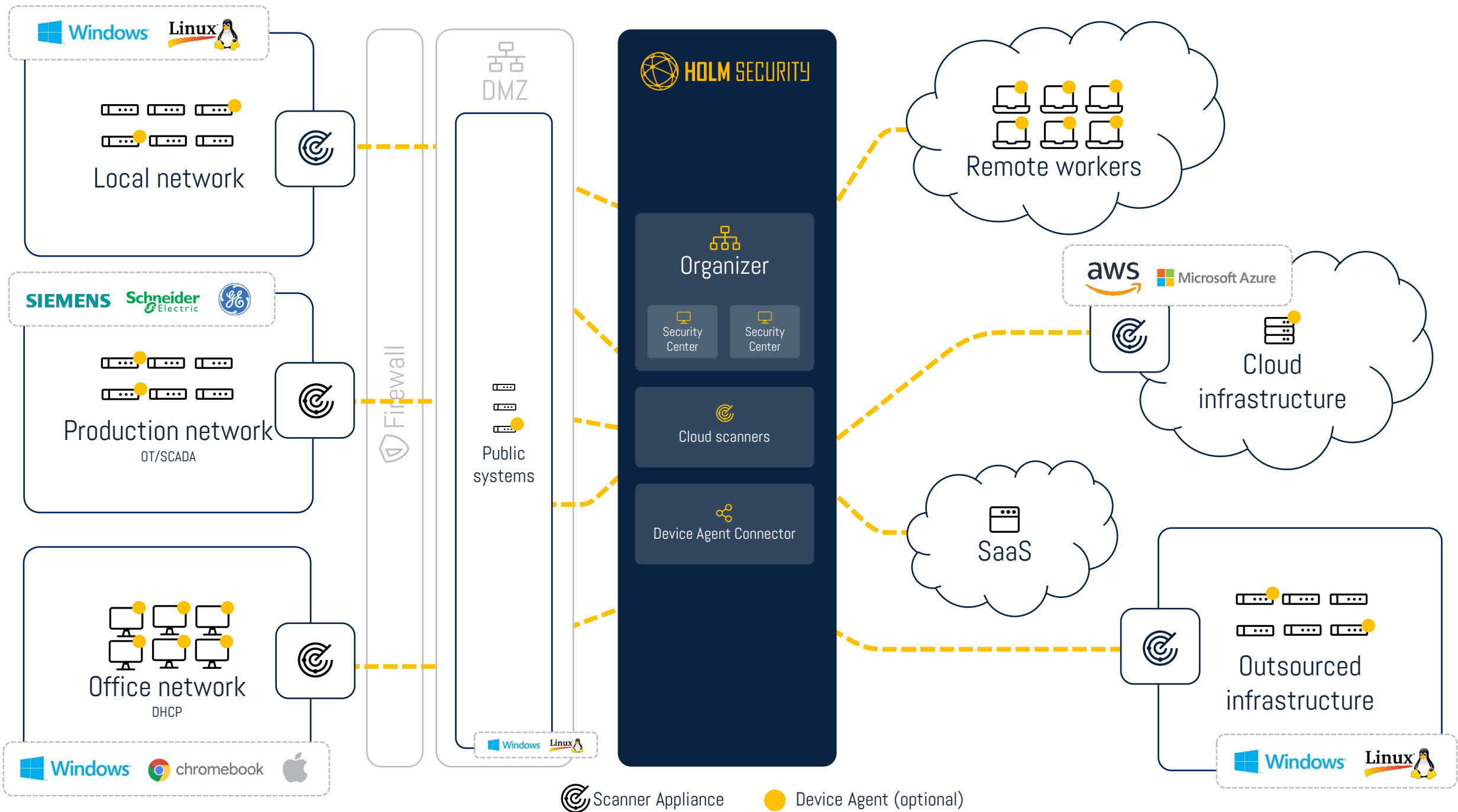
### Exposed data

Find exposed sensitive data like data directories and source code.



### Blank spots

Detect unknown systems before they pose a security threat.



# CAPABILITIES

Area:	Description:	Available in:	
		SaaS / Cloud:	On-premise:
Discovery scanning	Identify active assets running within a network.	✓	✓
Unauthenticated scan	System and network scanning from the outside, without access to the system.	✓	✓
Authenticated scan	Authenticates against scanned targets and performs deeper analysis of vulnerabilities from installed applications and packages.	✓	✓
CIS Benchmarks (Policy Scanning)	CIS Benchmarks best practices for the secure configuration of a target system. Holm Security is certified by CIS (Center for Internet Security).	✓	✓
Endpoint agent scanning	Light-weight endpoint extracting all software installed in a computer to find vulnerabilities. Track Windows devices in dynamic networks and computers that are not within your reach.	✓	×
Enterprise software & OT/SCADA	Coverage for mission-critical infrastructure and industrial systems.	✓	✓
PCI DSS ASV	Certified for compliance scans according to the Payment Card Industry Data Security Standard (PCI DSS) as a ASV (Approved Scanning Vendor).	✓	✓



# Cloud Scanning

Identify vulnerabilities across your cloud infrastructure with Cloud Security Posture Management (CSPM).





### **Cloud Misconfigurations**

Gain complete visibility and actionable context related to misconfigurations in your cloud-native applications.



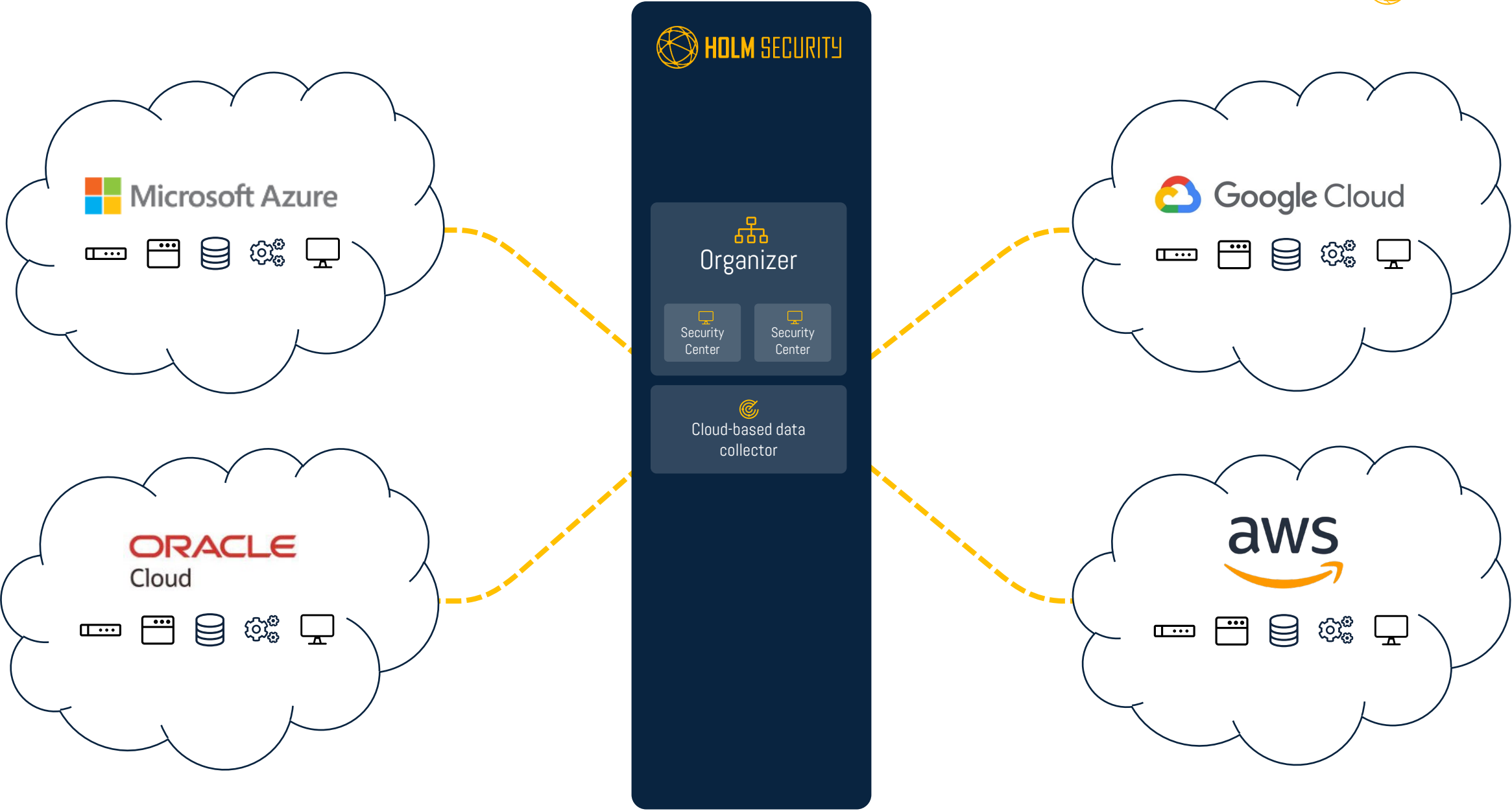
### **Multi-Cloud Support**

Manage your full asset inventory across platforms, regions, accounts, and divisions.



### **Agent- less**

No need for software or hardware – get started within hours using the API provided by the cloud vendor.







# Web Application Scanning

Find vulnerabilities, such as OWASP Top 10, in  
your websites and web apps.



### OWASP Top 10

Find the most common web application vulnerabilities, such as injection, broken authentication, sensitive data exposure, and XML external entities (XXE).



### Misconfigurations

Find vulnerabilities like directory listing.



### Weak passwords

Detect logins that use weak usernames and passwords.



### Exposed data

Find exposed personal information like personal IDs, and credit card details.



### Insecure certificates

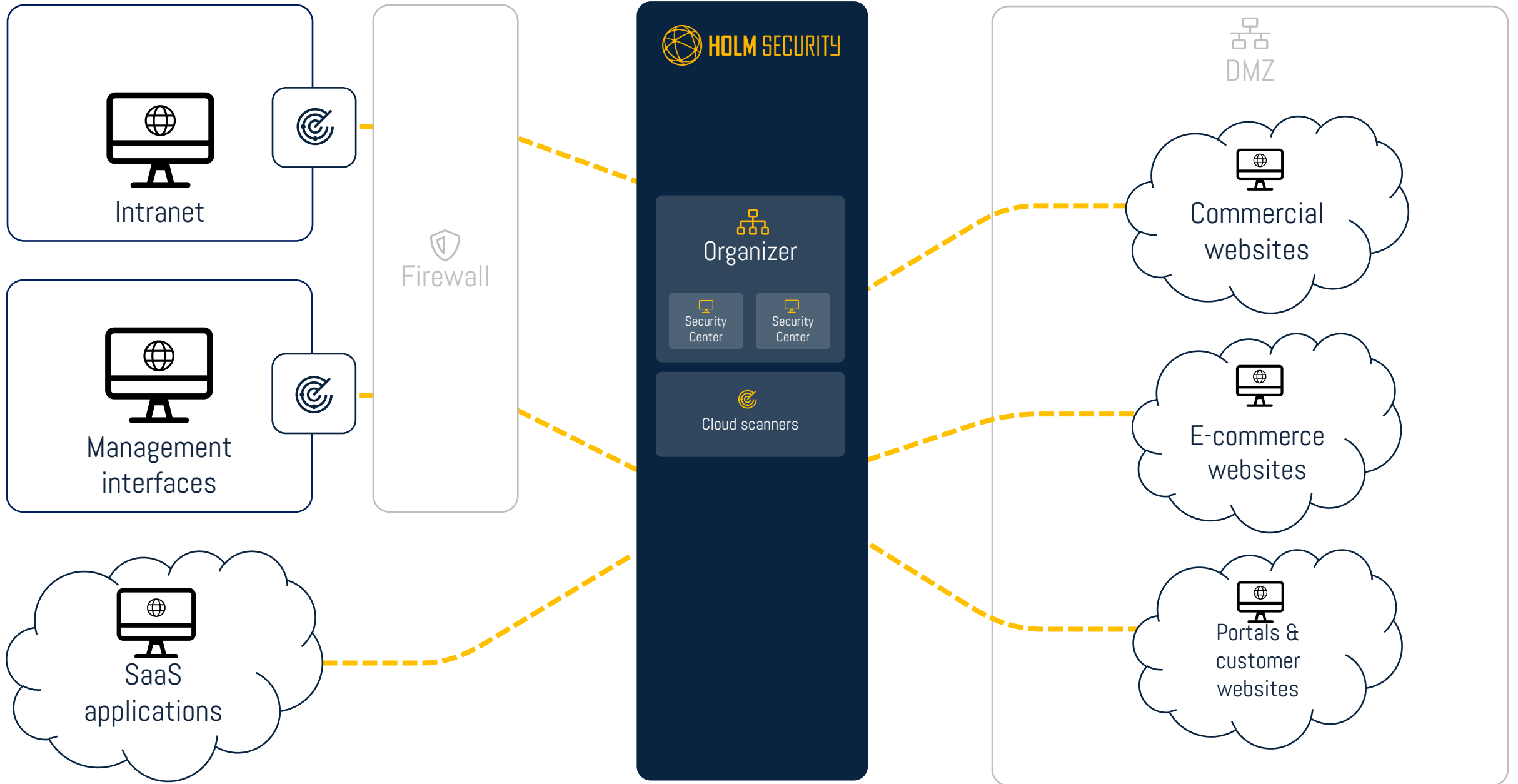
Detects SSL certificates that are about to expire, have expired, or are vulnerable.



### Modern apps

Detect risks in modern JavaScript empowered web applications.







# API Scanning

Find vulnerabilities, such as OWASP Top 10, in  
your APIs.



<https://www.holmsecurity.com>



### OWASP API Top 10

Coverage for OWASP API Security Top 10 and additional security vulnerabilities.



### User & Object Authentication

Finds broken or incorrectly configured authentication methods and function level authorization.



### Data exposure

Identify excessive exposed data and object properties that imposes a risk.



### Injectons

Finds injection flaws for common attacks such as SQL, NoSQL and command injections.



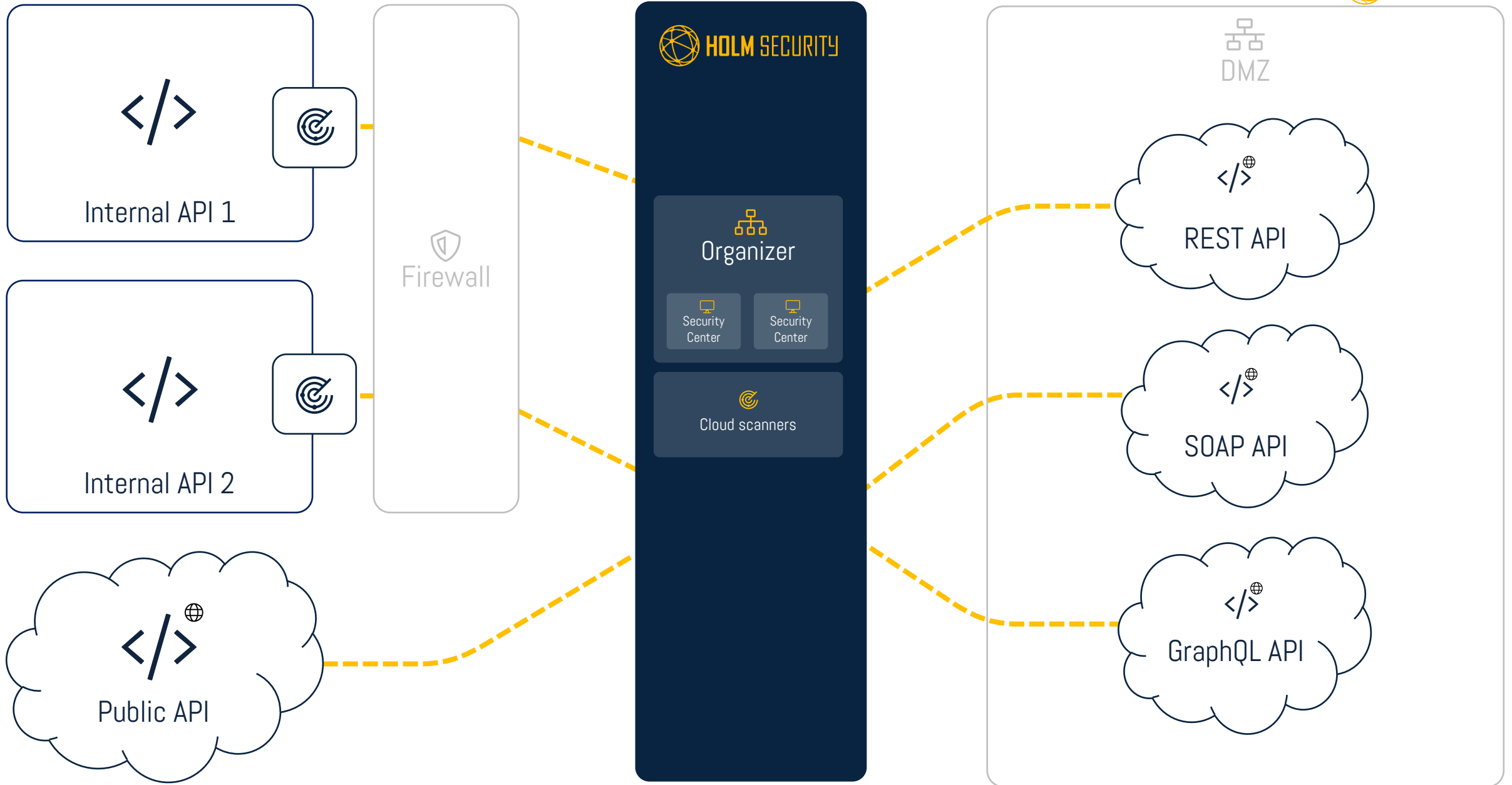
### Insecure certificates

Detects SSL certificates that are about to expire, have expired, or are vulnerable.



### Misconfigurations

Finds misconfiguration for the hosted API and the server hosting it.





# Phishing & Awareness Training

Build your own human firewall by identifying users with risky behavior and training them to become more resilient against phishing and ransomware attacks. Build your own human firewall.



### Phishing simulation

Realistic out-of-the-box phishing scenarios and customizable templates.



### Awareness training

Automated and tailored nano-learning based on the individual user's behavior in phishing simulations.



### Automated sequences

Sequences of simulations, awareness training and follow up quizzes.



### Videos

Built-in awareness videos and support to embed your own visual material.



### Quiz

Ready-made interactive questionnaires to measure users' knowledge.

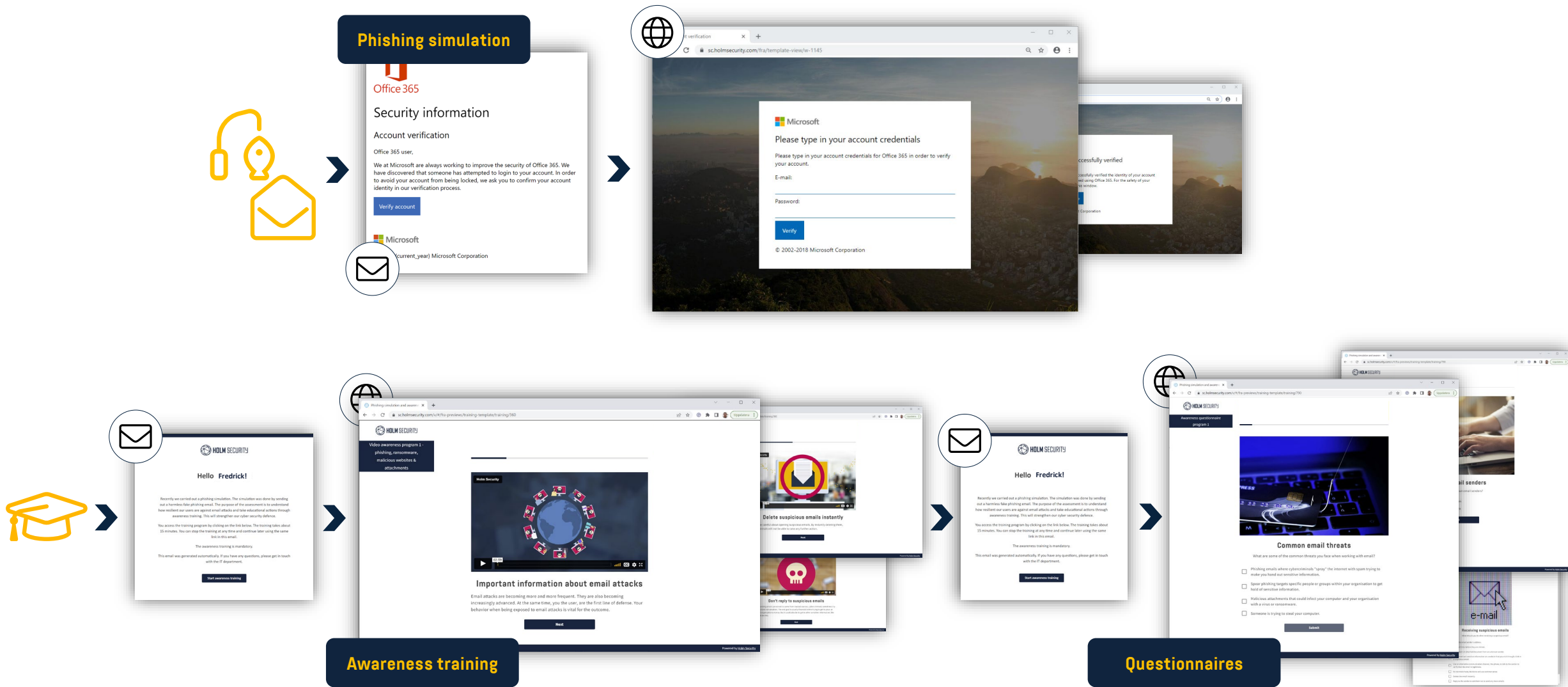


### Out-of-the-box

Ready-made and customizable templates for simulations, awareness training, and questionnaires.

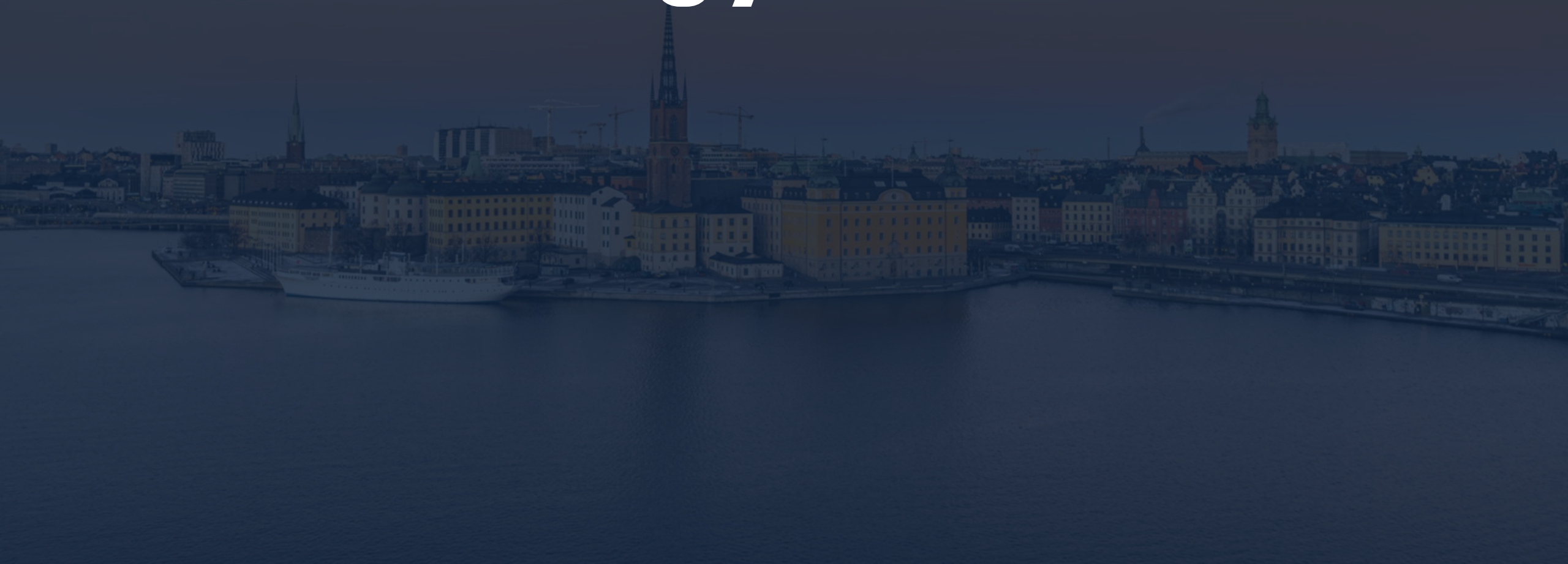


# A complete flow



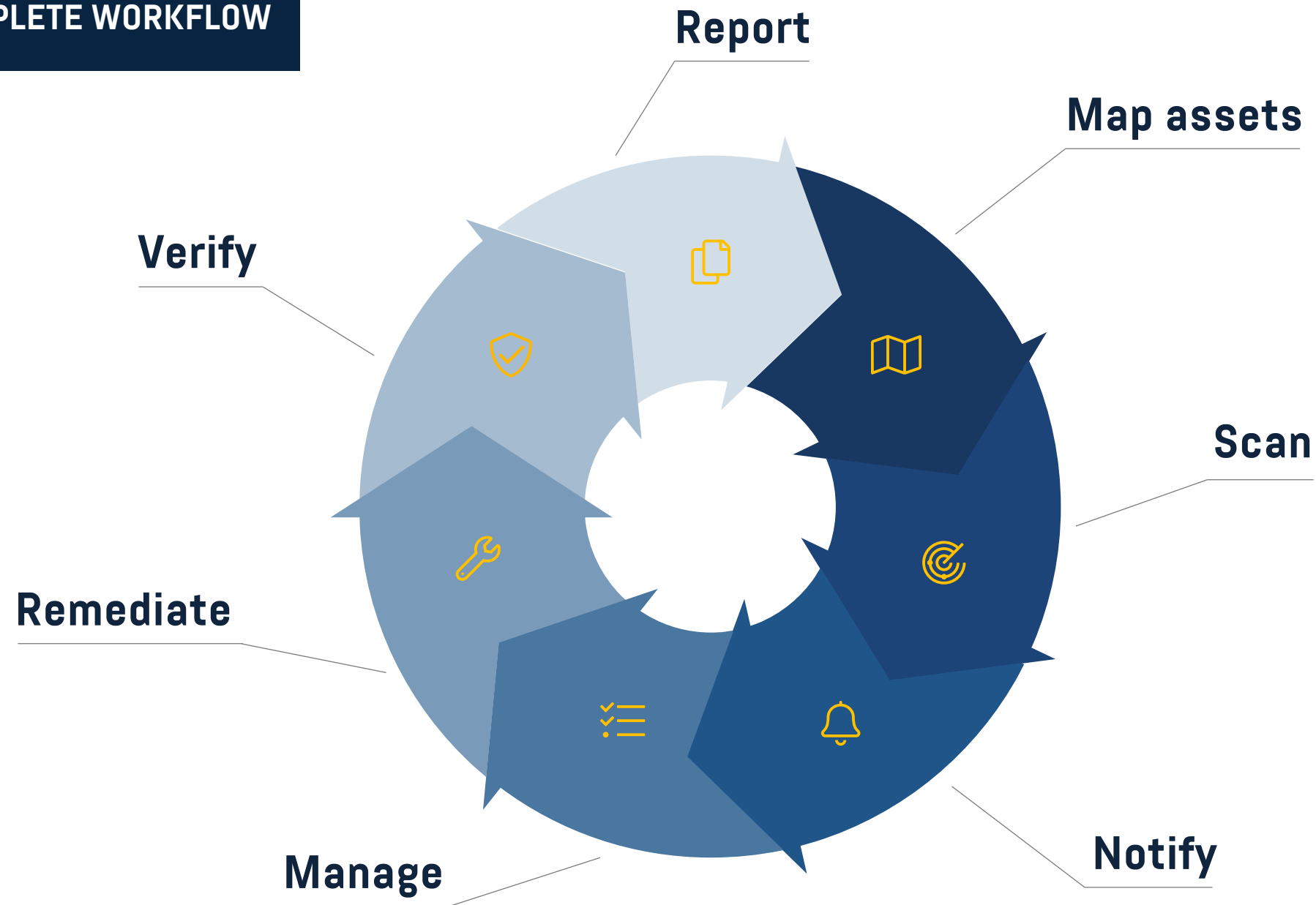
PLATFORM

# Technology

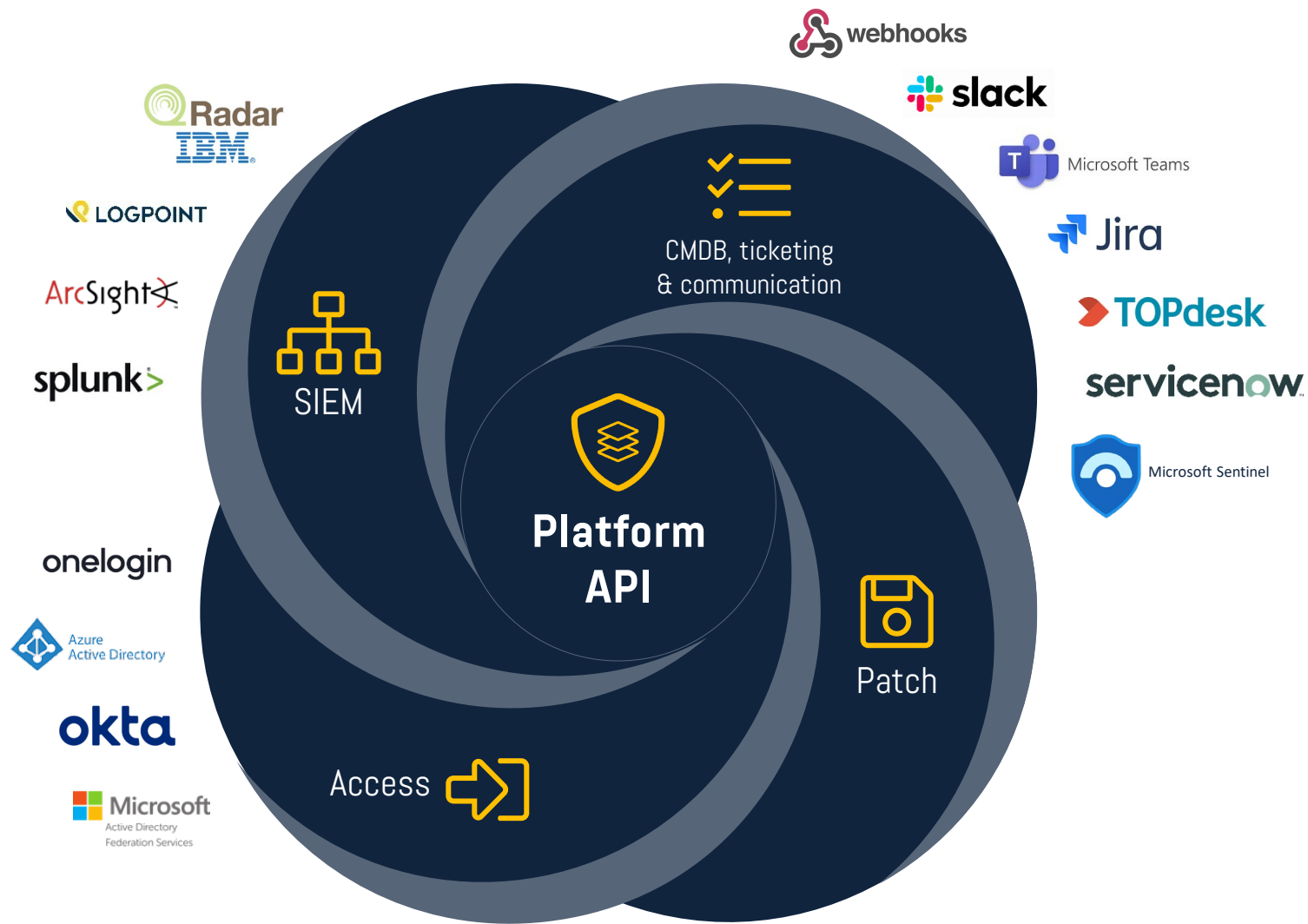




## A COMPLETE WORKFLOW



READY-MADE INTEGRATIONS



# ORCHESTRATION

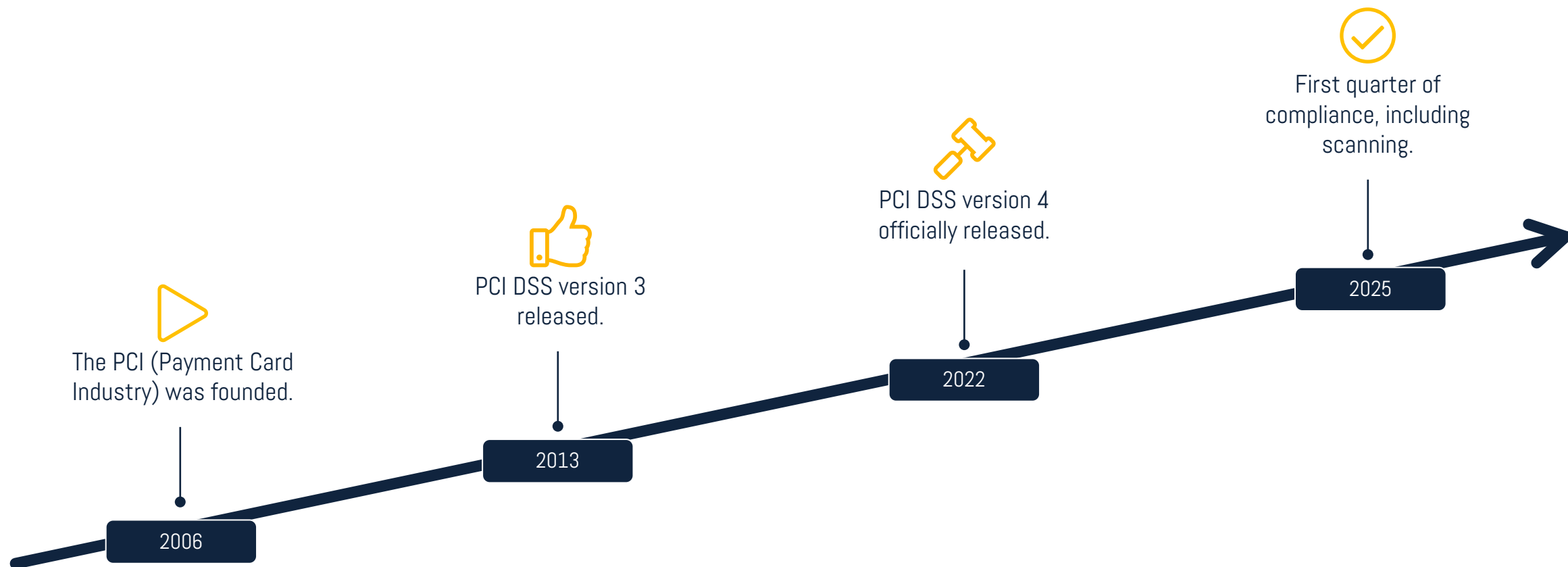


COMPLIANCE

# PCI DSS



# PCI DSS V4 TIMELINE



# Requirement:



## Enhanced Security Measures

The new version was expected to introduce more rigorous security requirements to address modern cyber threats and vulnerabilities.



## Emphasis on Risk Management

Version 4.0 emphasizes a risk-based approach to security, encouraging organizations to assess their unique risks and implement appropriate controls.



## Secure Software Development

With the growing importance of software security, version 4.0 includes updated guidelines for secure software development practices.



## Third-Party Risk Management

The new version will address the challenges of managing security risks associated with third-party service providers.



## Remote Work Considerations

The COVID-19 pandemic highlighted the need for secure remote work practices, and version 4.0 will offer guidance in this area.



# Our solution:

Protect the modern attack surface covering modern attack vectors such as cloud platforms.

Our platform provides all the tools need for a risk-based approach by understanding risks throughout your entire infrastructure.

Secure applications by scanning systems, web applications and API – before they go out in production.

Support the process of evaluating risks in third-party solutions.

Proactively strengthen your work force against phishing and related threats such as ransomware.



# Holm Security VMP is an ASV scanner

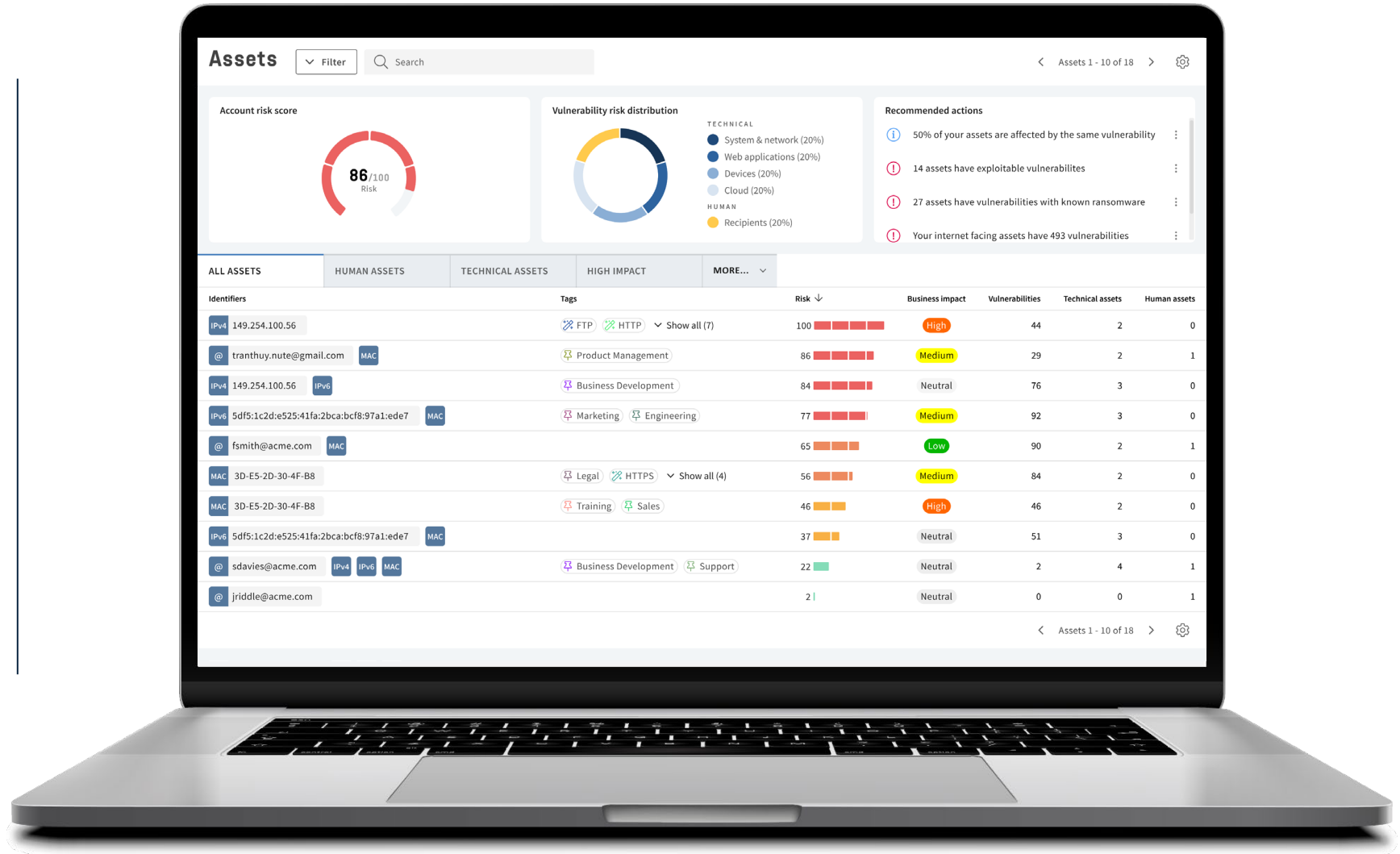
We support the process of scanning requirements with a certified product (Approved Scanning Vendor).





# Fully automated scans

Scans are running in the  
background without impact  
on the system.

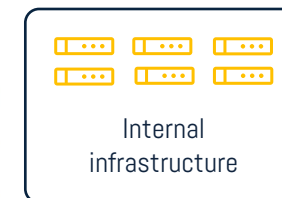
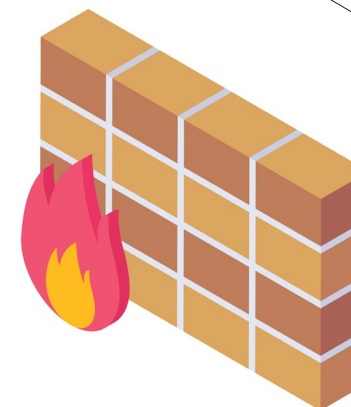
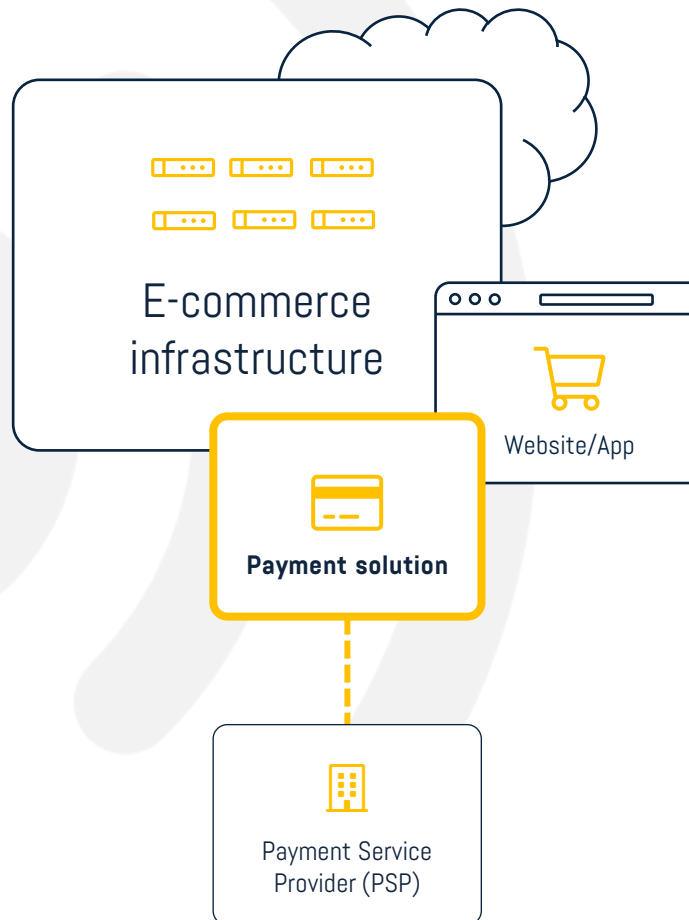
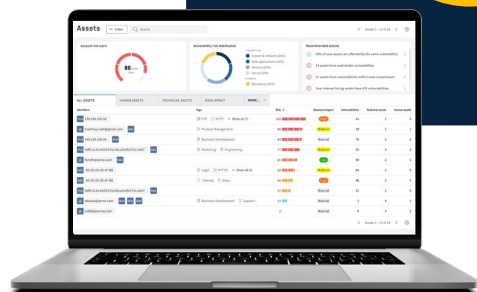




# ASV SCANNING

Unauthenticated scans from our cloud scanners.

Authenticated scanning using our Scanner Appliance. Set up together with our experts.





**Organizations must have both technical mechanisms and perform training to prevent phishing attacks.**

**Key functions: Phishing & Awareness Training**

- Phishing simulation and awareness training.
- Automated sequences (simulation, awareness training, questionnaires).
- Out-of-the-box templates and awareness material, including videos.
- Tailored awareness training.
- Fully integrated with unified risk score for more efficient prioritization.

# PCI DSS IMPLEMENTATION PROCESS

**1**

**Information about  
version PCI DSS 4**

**2**

**Evaluation of  
requirements**

**3**

**Presentation of  
proposed solution**

**4**

**Implementation of  
scanning and routines**



**Continuous  
compliance**

COMPLIANCE

# ISO 27001



# Requirements:



## **Risk assessment (§6.1.2)**

ISO 27001 requires organizations to perform a risk assessment to identify and assess information security risks.



## **Risk treatment (§6.1.2)**

Once risks are identified, ISO 27001 mandates that organizations develop a risk treatment plan. Part of this plan may involve vulnerability management.



## **Control selection (§6.1.3)**

ISO 27001 provides a list of control objectives and controls in Annex A of the standard. Some of these controls are directly related to vulnerability assessment and management, such as:

- A.12.6.1 - Management of technical vulnerabilities
- A.14.2.7 - System vulnerability assessments
- A.14.2.8 - Remediation of technical vulnerabilities



## **Continuous Improvement (§10.1)**

ISO 27001 promotes a cycle of continuous improvement. Organizations are required to regularly review and update their risk assessment, risk treatment plan, and information security controls.



# Our solution:

Automated and continuous risk assessments (vulnerability management) to identify risks.

We support our customers in implementing a long-term risk treatment plan.

We support finding technical vulnerabilities, as well as performing vulnerability management and supporting the process of remediating vulnerabilities.

Vulnerability management play a crucial role in this ongoing process by helping organizations stay informed about emerging vulnerabilities and adapting their security measures accordingly.



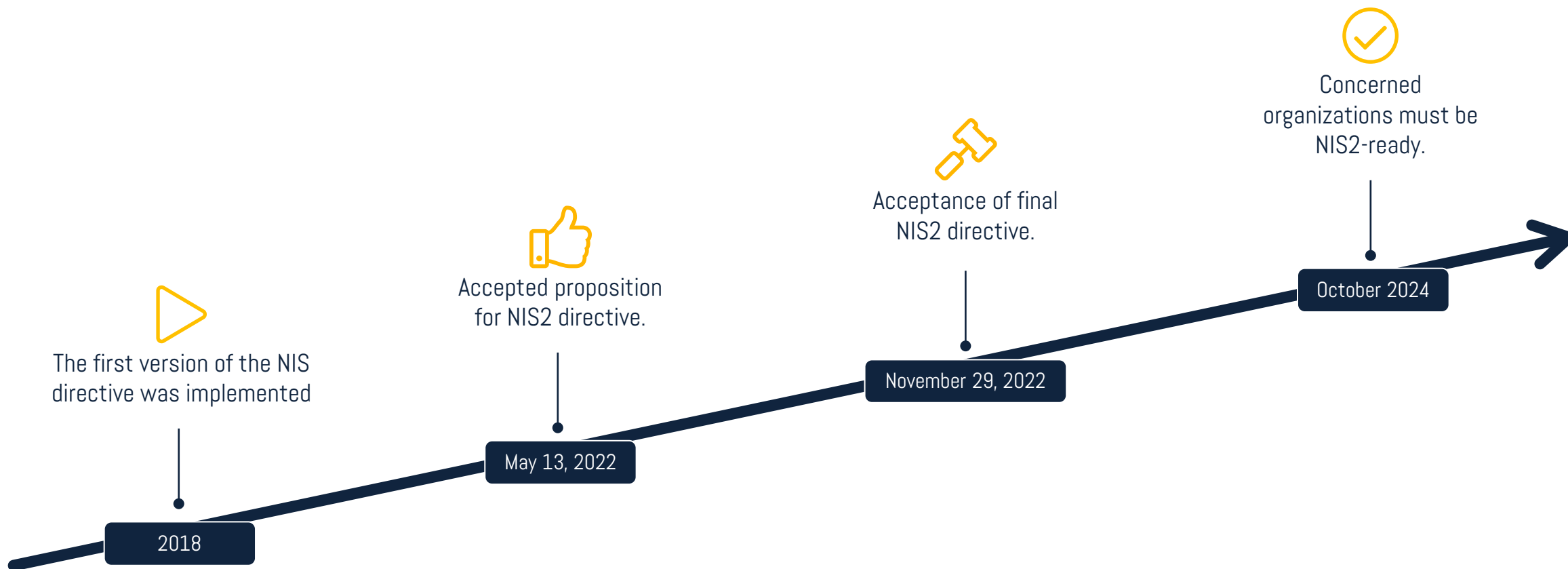
COMPLIANCE

# NIS & NIS2





# NIS2 TIMELINE



## Essential Entities



## Important Entities



## Demands/impact:



A systematic, analytical, risk-based work within information security and perform risk assessments.



Report Incident reporting – also for exposure without an incident.



Be able to demonstrate compliance today and historically.



Administrative sanctions; lost permits, certifications and similar.



Personal responsibility for top management.



## Our solution:

Automated and continuous risk assessments.

Discover vulnerabilities and generate reports.

Reports that shows compliance today and historically.

Proactively strengthen your cyber defense to avoid incidents.

Proactively strengthen your cyber defense to avoid incidents.



# NIS2 applies direct or indirect

Essential entities and  
Important entities  
must secure the  
entire supply  
chain.

**USE CASES**

# **OT/SCADA**

**Supervisory Control & Data Acquisition  
Operational Technology**





# The Stuxnet worm sabotage

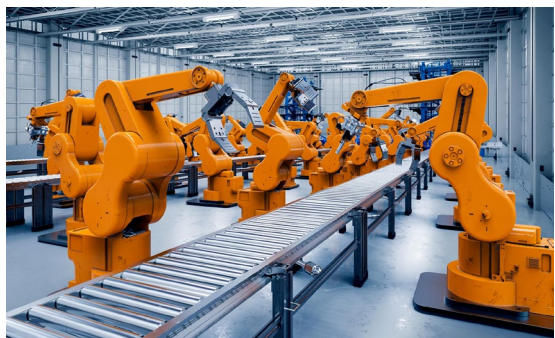
- The malicious computer worm, was first officially uncovered in 2010.
- Used to attack a uranium enrichment facility at Iran's nuclear site.
- Destroyed almost one-fifth of Iran's nuclear centrifuges.
- The worm infected over 200,000 computers and caused 1,000 machines to physically degrade.





## Ukrainian power grid hack

- In 2015 and 2016, cyber-attacks on the power grid cut electricity to nearly a quarter-million Ukrainians.
- Shut off power at 30 substations, leaving around 230,000 people without electricity for up to six hours.
- SCADA equipment wasn't working, and power restoration had to be done manually.



**We provide a  
market leading  
coverage for the  
supervisory layer.**

# CAPABILITIES

## Supervisory layer

Computers (software), network data communications and HMI (Human-Machine Interface).



Full coverage for the supervisory layer and all layers above.

## Control layer

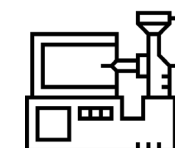
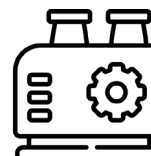
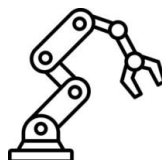
PLCs/RTUs, PIDs and DCS.



Partial coverage for the control layer.

## Field layer

Sensors, pumps, actuators, valves, engines, and other peripheral devices.



## COVERAGE

Schneider  
Electric

ABB

SIEMENS

Honeywell

General  
Electric

westermo

MITSUBISHI  
ELECTRIC

Circuit

Rockwell  
Automation

YOKOGAWA



# 50+ vendors covered

Major coverage of vendors within  
OT/SCADA.



# 1600+ vulnerabilities covered

Market leading vulnerability test  
coverage within OT/SCADA