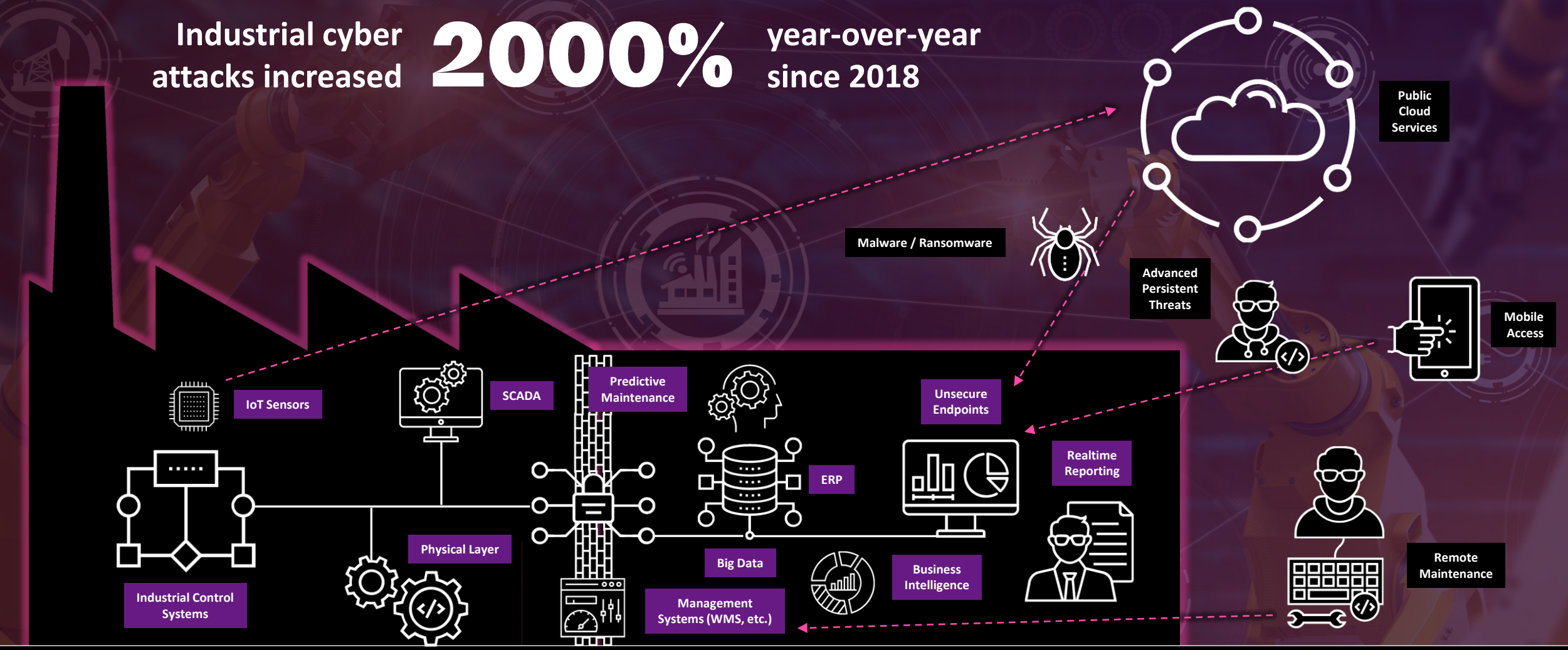
BearingPoint®

Industrial Cyber Security

The increasing connectivity of industrial control systems (ICS) and the convergence of OT and IT networks expands the attack surface of industrial systems and critical infrastructure facilities

We help you prepare for unwanted guests

Industrial cyber attacks increased **2000%** year-over-year since 2018



Safe for the future 4.0?

Targeted attacks are threatening your OT environment every day

Armed for next level challenges

The best way to secure your system is to control it

Innovate

Use latest IT and cloud technologies to boost your productivity to the next level

We help you to connect your production and assets to new technologies through the usage of latest security solutions.

Protect

Improve your security and protect your assets from next generation threats

We solve specific risks for quick improvements of your security level and help to optimize your security architecture in a holistic way.

Fulfill

Fulfill all regulatory requirements and reduce legal risks

We help you efficiently match regulatory specifications and legal standards, through the use of best practice approaches.

See

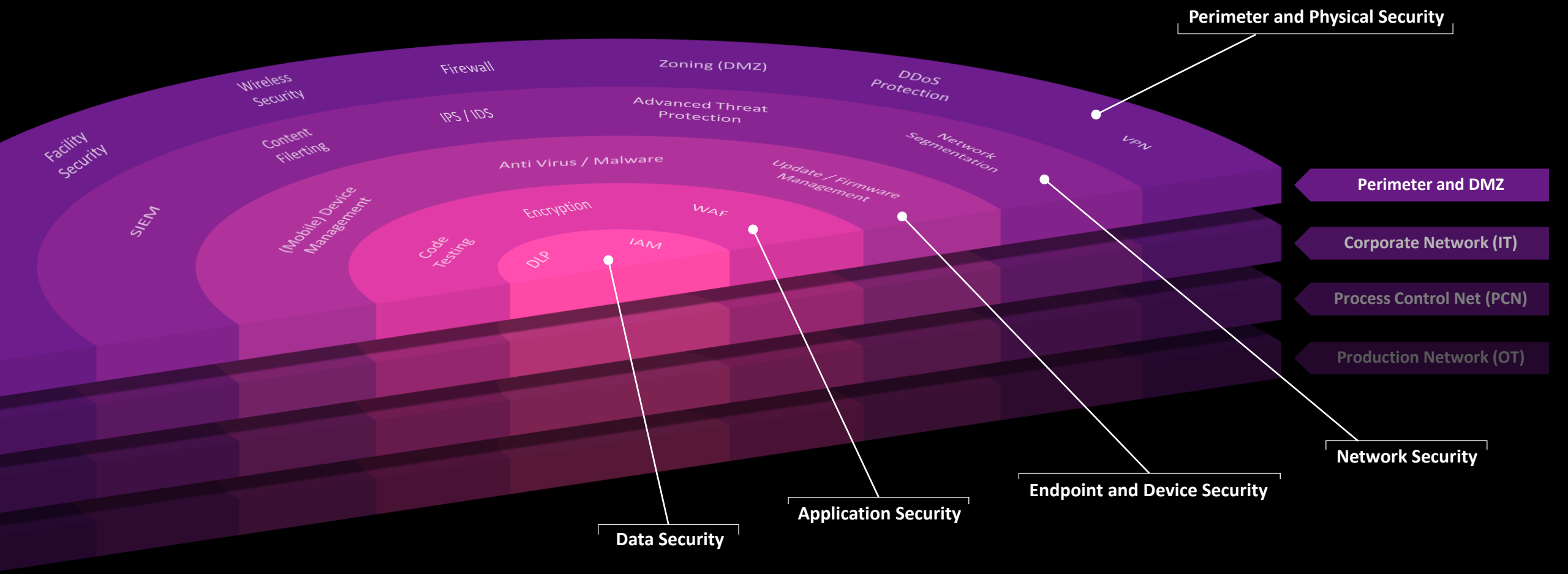
Get real-time visibility of your assets and streams

We help you gain complete insight on all your IT and OT assets, their vulnerabilties, activities and potential attacks for full control.

Defense-in-Depth

The concept of „Security-in-Depth“ is a proven best-practice approach. It describes a design principle where different types of protection mechanisms are deployed in different locations, often based on several technologies, to create a multi-layered protection stack. This shall prevent an attack from being successful after overcoming a single barrier.

We apply this concept horizontally as well as vertically, for maximum security and resilience.



5-step protection approach

Increase the security level of your OT protection step by step, without risks.

Protect OT networks from IT threats

1

OT Isolation

Protect your industrial and production network from external threats or security issues of your IT network.

Protect against standard attacks

2

Transition Hardening

Eliminate potential back doors and vulnerabilities and control access on the transition points between IT and OT.

Protect against untargeted automated attacks

3

OT Segmentation

Isolate critical production systems from each other and limit the distribution potential of cyber threats within the OT network.

Protect against Advanced Persistent Threats (APT)

4

Passive Detection

Detect anomalies and deviations of nominal conditions between specific devices and systems of your production process in a listener-only mode and in real-time.

Protect against advanced and targeted DoS attacks

5

Active Prevention

Define and observe the target conditions and allowed behaviour of your production environment and take necessary actions to protect it automatically and in real-time.

CISCO

radware

Check Point SOFTWARE TECHNOLOGIES LTD.

elastic

kafka

CLAROTY Clarity for OT Networks

FORESCOUT

ANSIBLE

Scenarios from the wild

Every client and installation is unique and faces unique challenges. When it comes to ICS security, there is no silver bullet, but specific solutions for individual challenges.

2+3 Transition hardening and OT Segmentation

Steel-based technology manufacturer

Client IT must secure transition access between office and production network, secure the supplier maintenance access, as well as the different OT domains from each other.

Challenge

- Centrally manage data streams into/between OT networks
- Control maintenance access and authentication by suppliers
- Increase granularity for access control and management
- Protect OT network against zero-day threats

Solution

- Secure transition between IT and OT with NextGen Firewalls
- Secure OT domains from each other with NGFW to prevent spread of untargeted automated attacks
- Control external supplier access to individual components and secure through MFA and sandboxing

2+3 Transition hardening and OT Segmentation

Leading intra-logistics manufacturer

Client is required to secure many generations of its intra-logistics solutions as they become exposed to modern IT threats and have vulnerabilities that cannot be patched.

Challenge

- Design, implement and run universal security solution for all generations of facilities
- Solution must be standalone and non-disruptive
- Secure client maintenance access and handle unsecure protocols

Solution

- Continuously eliminate all vulnerabilities through virtual patching on NGFW
- Access and authentication security introduced and unsecure protocols are handled securly at the frontends
- Maintenance access protected against threats

3+4 OT Segmentation and Passive Detection

High-tech tube manufacturer

Client is not able to implement further security measures within their isolated OT network due to missing segmentation options and has no visibility of OT assets and activities .

Challenge

- OT segmentation without changing existing IP addresses
- Gain full visibility of assets and activities
- Understand vulnerabilities
- Cost-efficient and non-disruptive solution

Solution

- Develop non-disruptive segmentation architecture
- Increase security preventing lateral movement
- Implement asset and anomaly detection for full visibility and control

BearingPoint Business Services

Technology and Services

Platform Services // Cyber Security // Managed Service

Austrians largest management and technology consulting firm

With more than 500 employees in Austria we develop innovative strategies for new and existing business models and design and implement digital solutions and services for leading companies and public institutions.

With our competencies in management consulting, agile transformation, technology-based business services and smart BearingPoint software solutions, we develop innovative business models together with our clients and partners.

Among BearingPoint's clients are Austrias leading companies and organisations. The global BearingPoint network with more than 10.000 employees supports clients in more than 75 countries and actively engages with them for measurable and long-lasting business success.

BearingPoint®