Check Point
SOFTWARE TECHNOLOGIES LTD

CRITICAL INFRASTRUCTURE and INDUSTRIAL AUTOMATION SECURITY

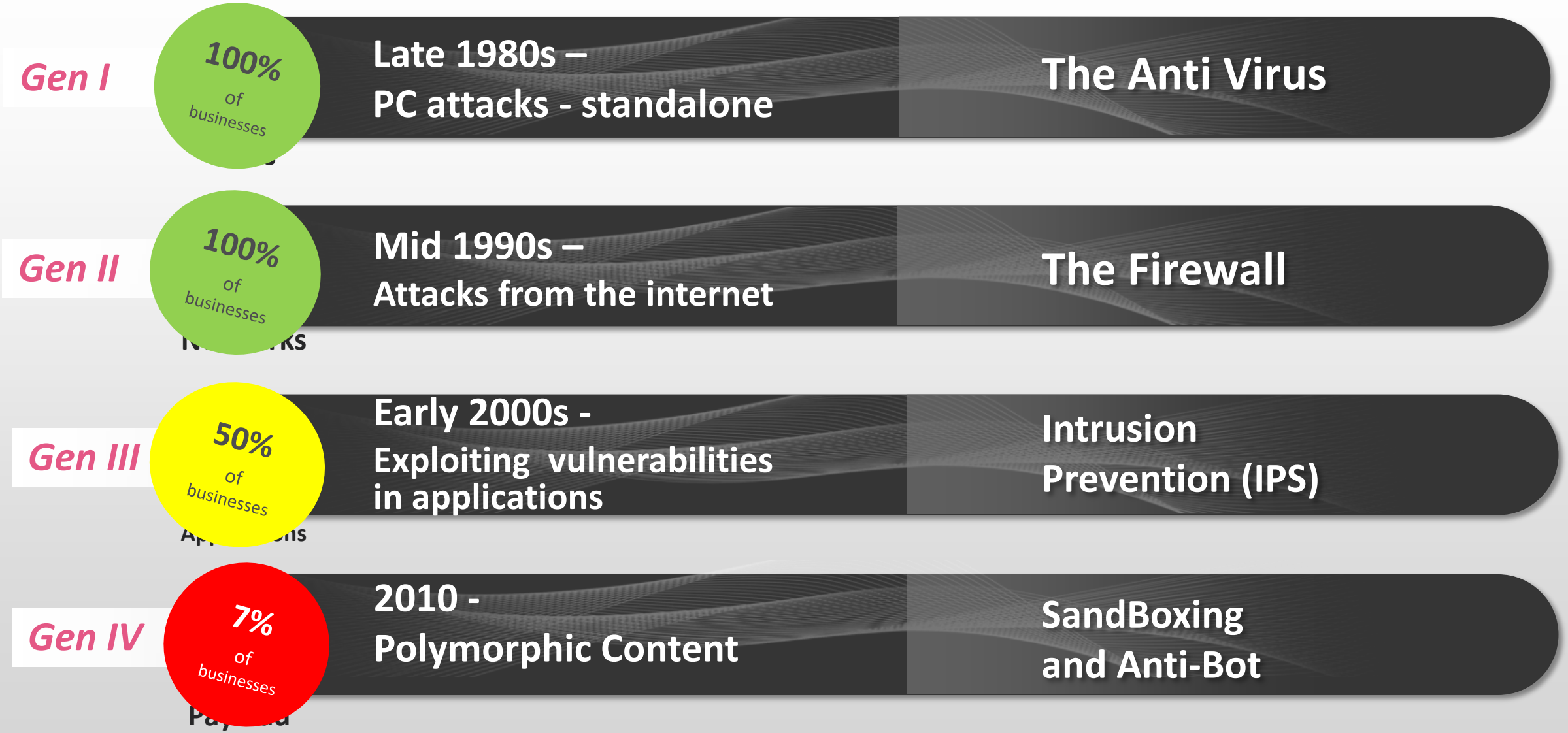
Preventing the Kill Chain in **Industrial Control Systems (ICS) / SCADA**

Mati Epstein
Global sales manager
Critical Infrastructure and ICS

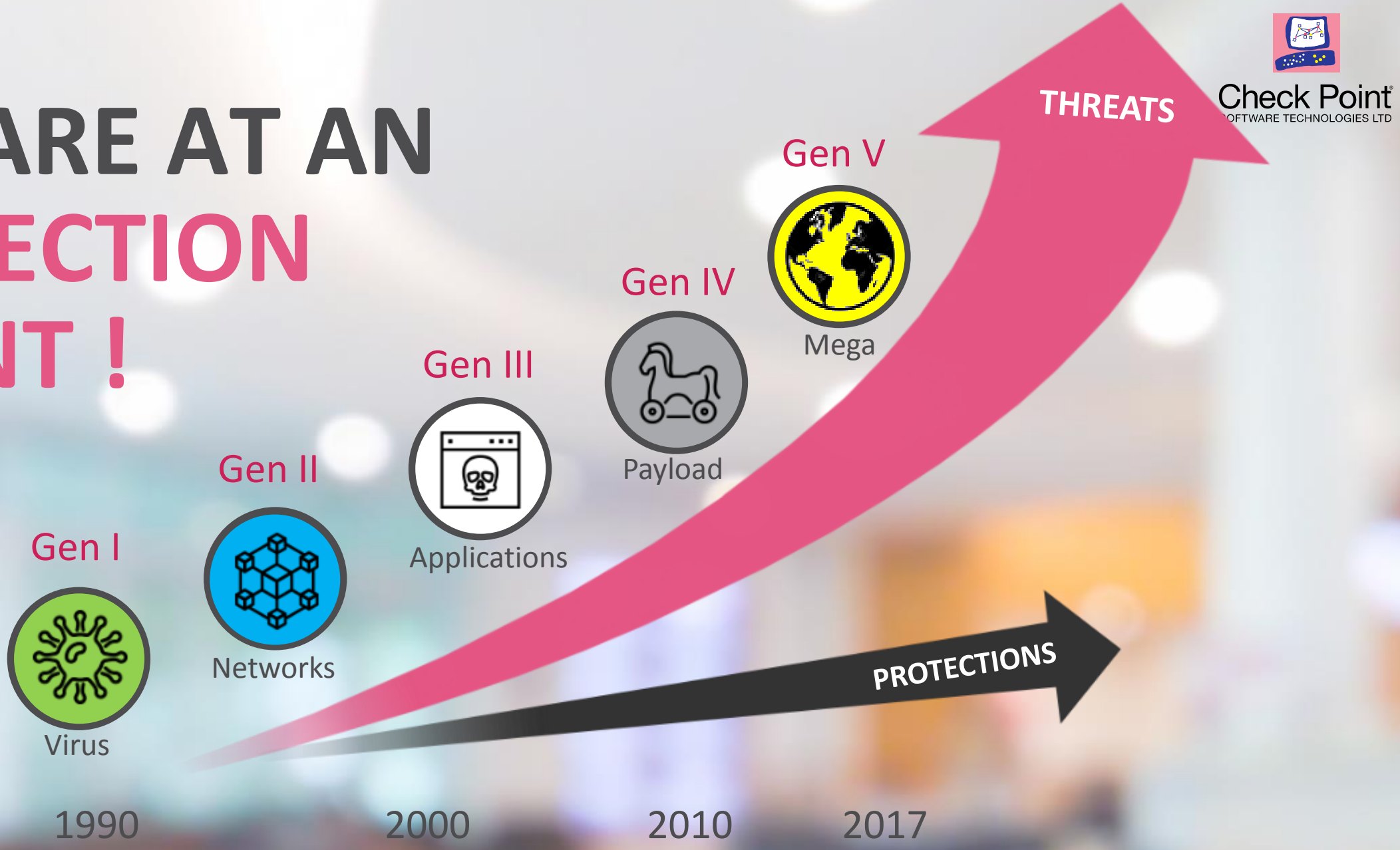
WELCOME TO THE FUTURE OF
CYBER SECURITY
POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION

Generations of Attacks and Protections



WE ARE AT AN INFLECTION POINT !



MAKING GEN V POSSIBLE

Check Point
SOFTWARE TECHNOLOGIES LTD

GEN V

CHECK POINT
INFINITY

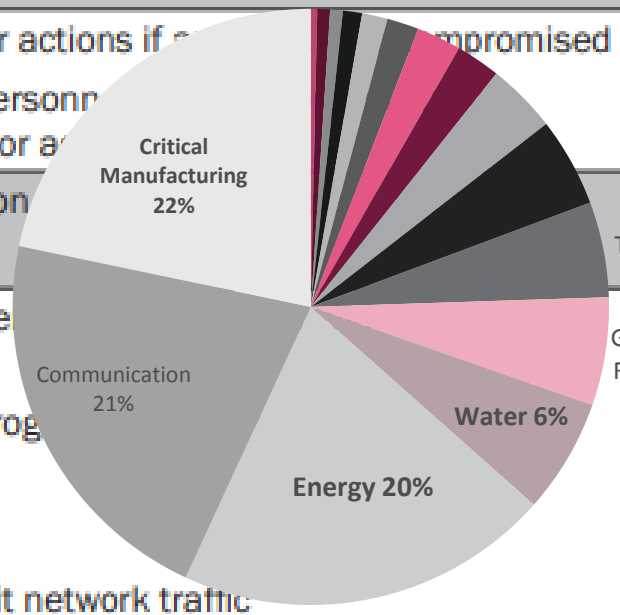
US ICS-CERT report: (Jan-18)

FY 2017 Most Prev… …ses

3rd year in a row

Area of Weakness	Rank	Risk
Boundary Protection	1	• Undetected unauthorized activity in critical systems • Weaker boundaries between ICS and enterprise networks
Identification and Authentication (Organizational Users)	2	• Lack of accountability and traceability for user actions if … …ompromised • Increased difficulty in securing accounts as personn… especially sensitive for users with administrator a…
Allocation of Resources	3	• No backup or alternate personnel to fill position • Loss of critical knowledge of control systems
Physical Access Control	4	• Unauthorized physical access to field equipme… opportunity to: ○ Maliciously modify, delete, or copy device prog… ○ Access the ICS network ○ Steal or vandalize cyber assets ○ Add rogue devices to capture and retransmit network traffic
Account Management	5	• Compromised unsecured password communications • Password compromise could allow trusted unauthorized access to systems
Least Functionality	6	• Increased vectors for malicious party access to critical systems • Rogue internal access established

Most Attacked Sectors 2016



Best Practices for Securing OT

Check Point
SOFTWARE TECHNOLOGIES LTD

Secure **Both** OT and IT Environments

Protect IT with Advanced Threat Prevention Technologies

WELCOME TO THE FUTURE OF CYBER SECURITY

Securing against Attack Vectors

Attack Vector	Check Point solution
Removable Media	Endpoint data protection
Spear Phishing	Sandblast Emulation and Extraction
Ransomware	SandBlast Anti-Ransomware
Remote Technicians	Secured VPN Connectivity and Two Factor Authentication
Software Vulnerabilities	IDS/IPS
Virus's and BOT's	Anti Virus and Anti-Bot
Missing Boundary	Firewall and segmentation

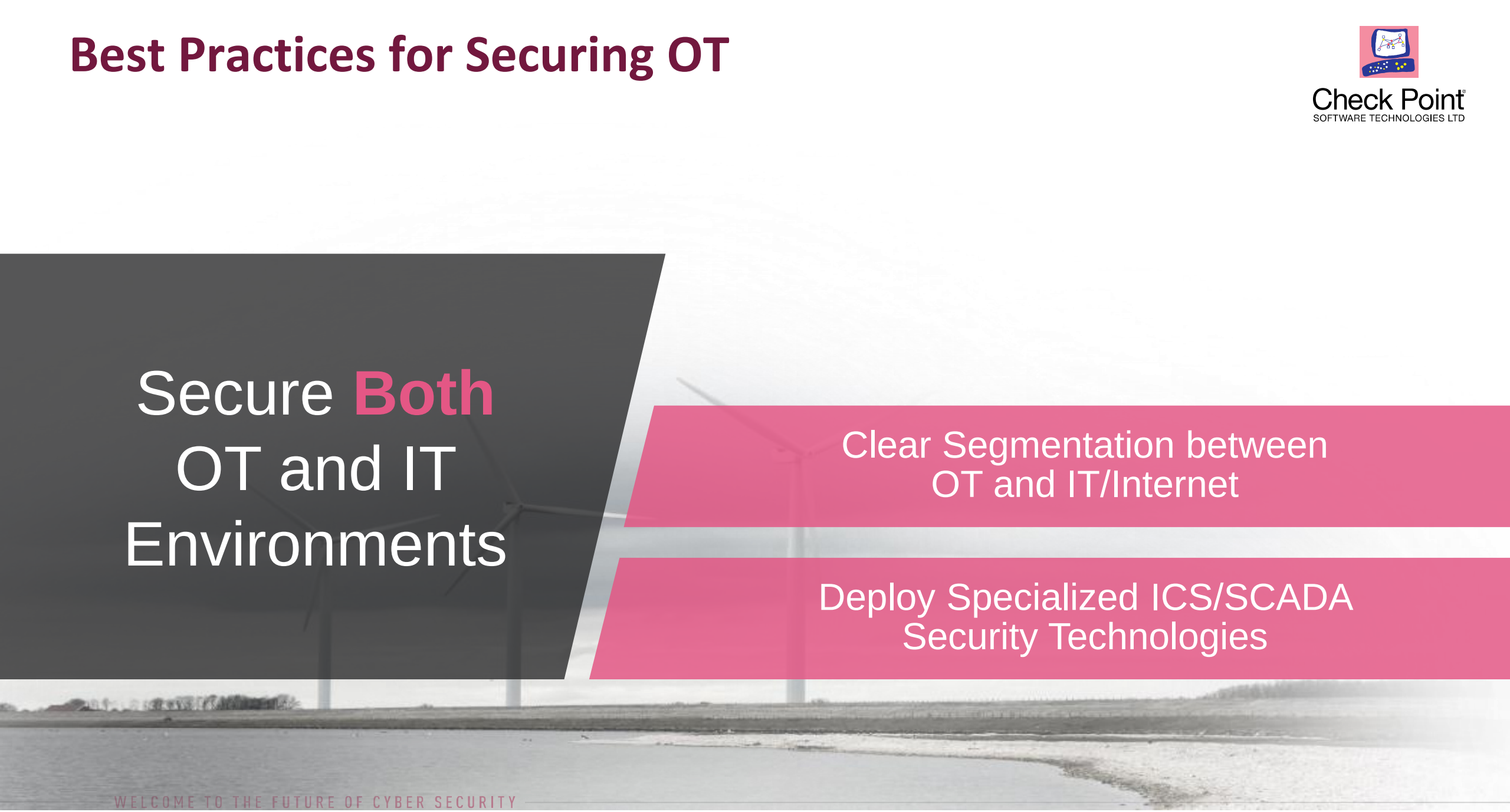
Best Practices for Securing OT

Check Point
SOFTWARE TECHNOLOGIES LTD

Secure **Both** OT and IT Environments

Clear Segmentation between OT and IT/Internet

Deploy Specialized ICS/SCADA Security Technologies



Enhanced OT Visibility

Communication Information

- >50 **Protocols**, >1100 **Commands**
- Asset connections within the ecosystem
- Open/proprietary protocols

Asset Information

- IP and MAC Address
- Equipment vendor
- Equipment type (PLC, HMI, Engineering Workstation, Switch, etc.)
- Asset model name and Serial #
- Firmware version
- Physical data (rack slots)

Network Mapping

- How assets are communicating and who is accessing them?
- Uncover configuration issues and vulnerable assets

Enforcement

Pre-defined Policies

- **Learning phase** - network traffic and logging
- Manual setting of SCADA commands baseline
- Specific Command policies
- Specific Values policies
- Time of Day and traffic patterns policies

Anomaly Detection

- **Learning phase** - Automatically Discover Assets and communication
- Anomaly-Based Behavior Analysis
- Generate High-Fidelity Baseline Model
- Generate security and process threats

Combined Enforcement of
Pre-Defined + Anomaly-Based analysis

Check Point
SOFTWARE TECHNOLOGIES LTD

THANK YOU

WELCOME TO THE FUTURE OF
CYBER SECURITY

POWERED BY CHECK POINT INFINITY

CLOUD • MOBILE • THREAT PREVENTION