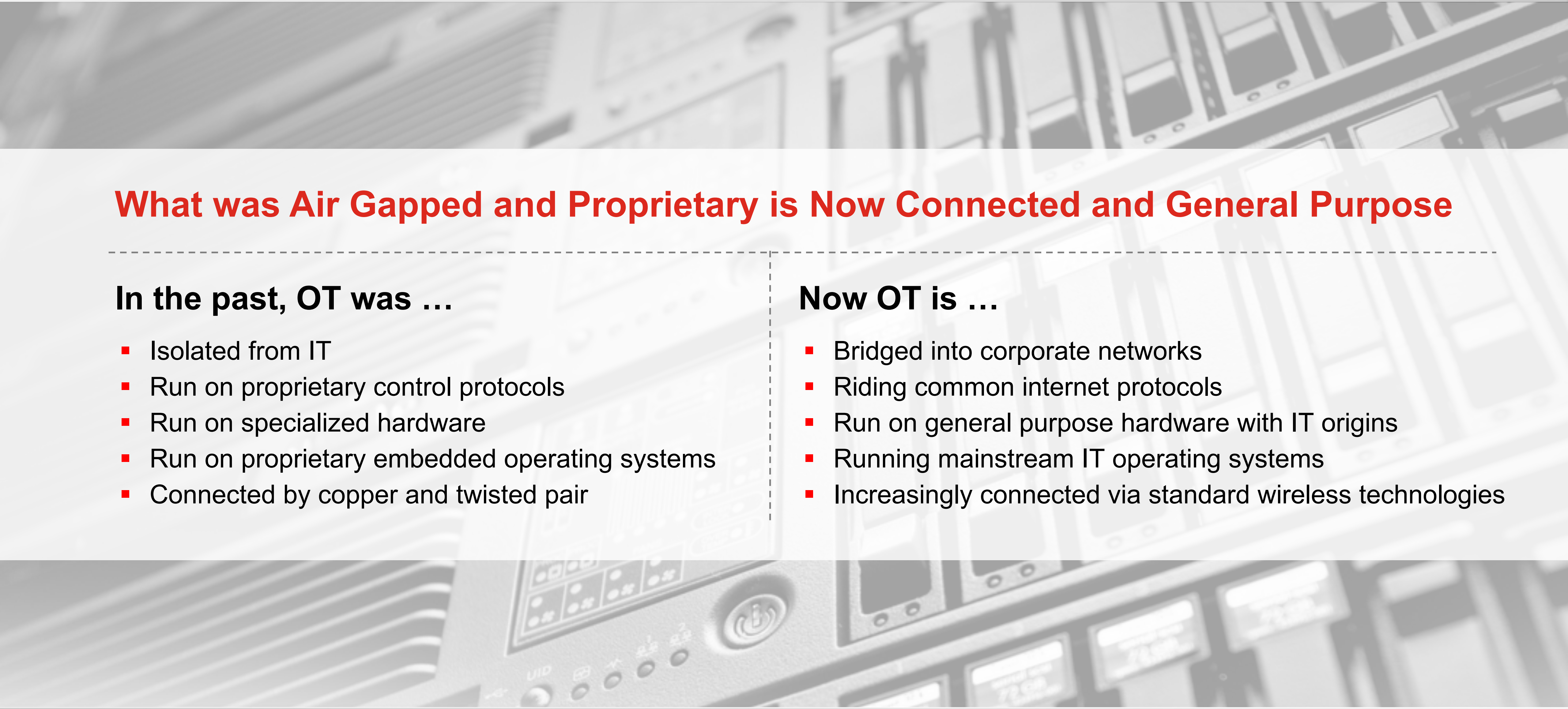
Bezpečnosť kritickej infraštruktúry bez kompromisov!

Ako ochrániť Vašu ICS sieť s Fortinet Security Fabric-om

Peter Kocik, Systems Engineer, CEE

Convergence of Information and Operational Technology



What was Air Gapped and Proprietary is Now Connected and General Purpose

In the past, OT was …

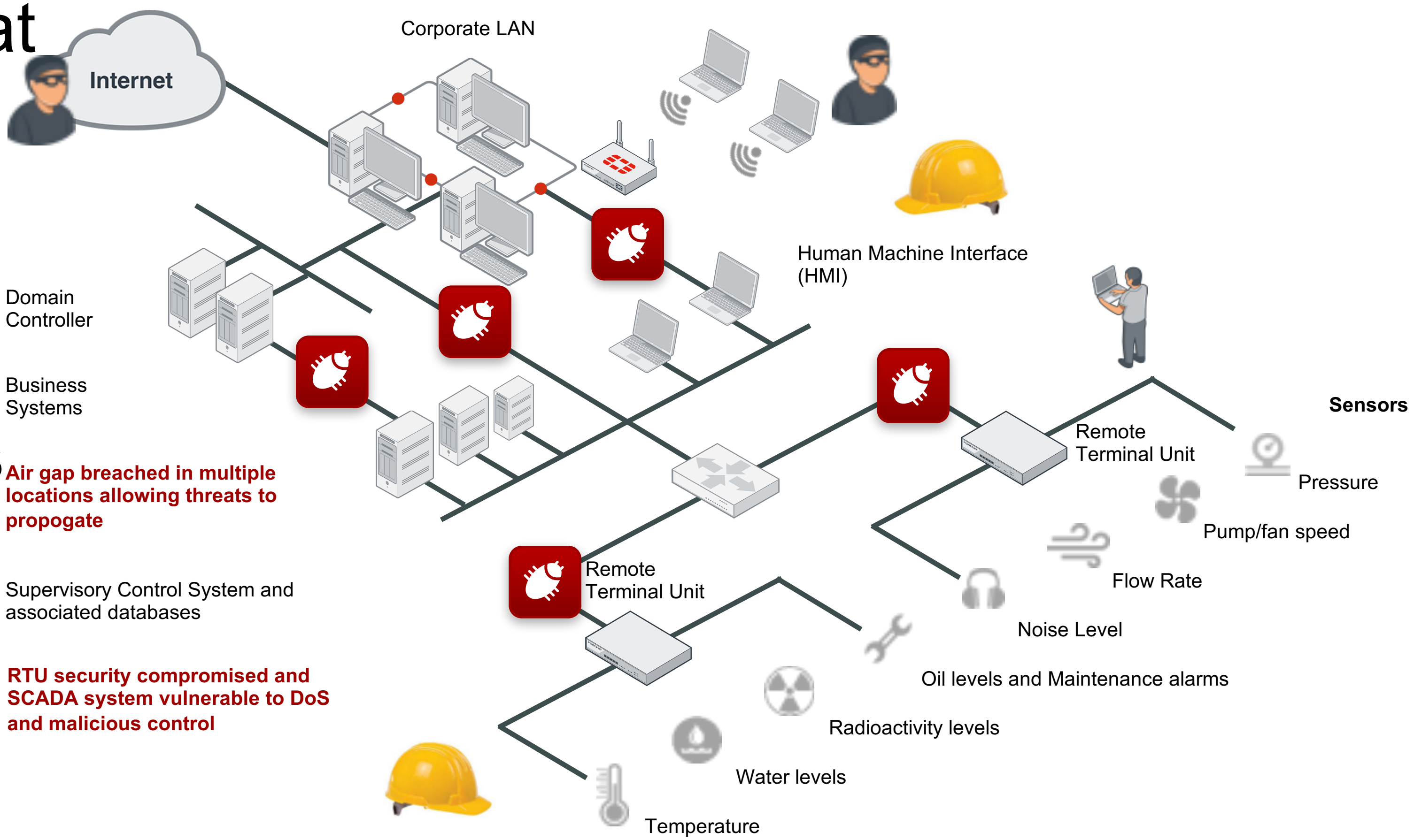
- Isolated from IT
- Run on proprietary control protocols
- Run on specialized hardware
- Run on proprietary embedded operating systems
- Connected by copper and twisted pair

Now OT is …

- Bridged into corporate networks
- Riding common internet protocols
- Run on general purpose hardware with IT origins
- Running mainstream IT operating systems
- Increasingly connected via standard wireless technologies

Breach points everywhere

- Outside threat: Black Hat
- Inside threat: Hard Hat
- Air gap breached
- RTU or HMI exploits
- DOS attack of Protocols
- Droppers USB

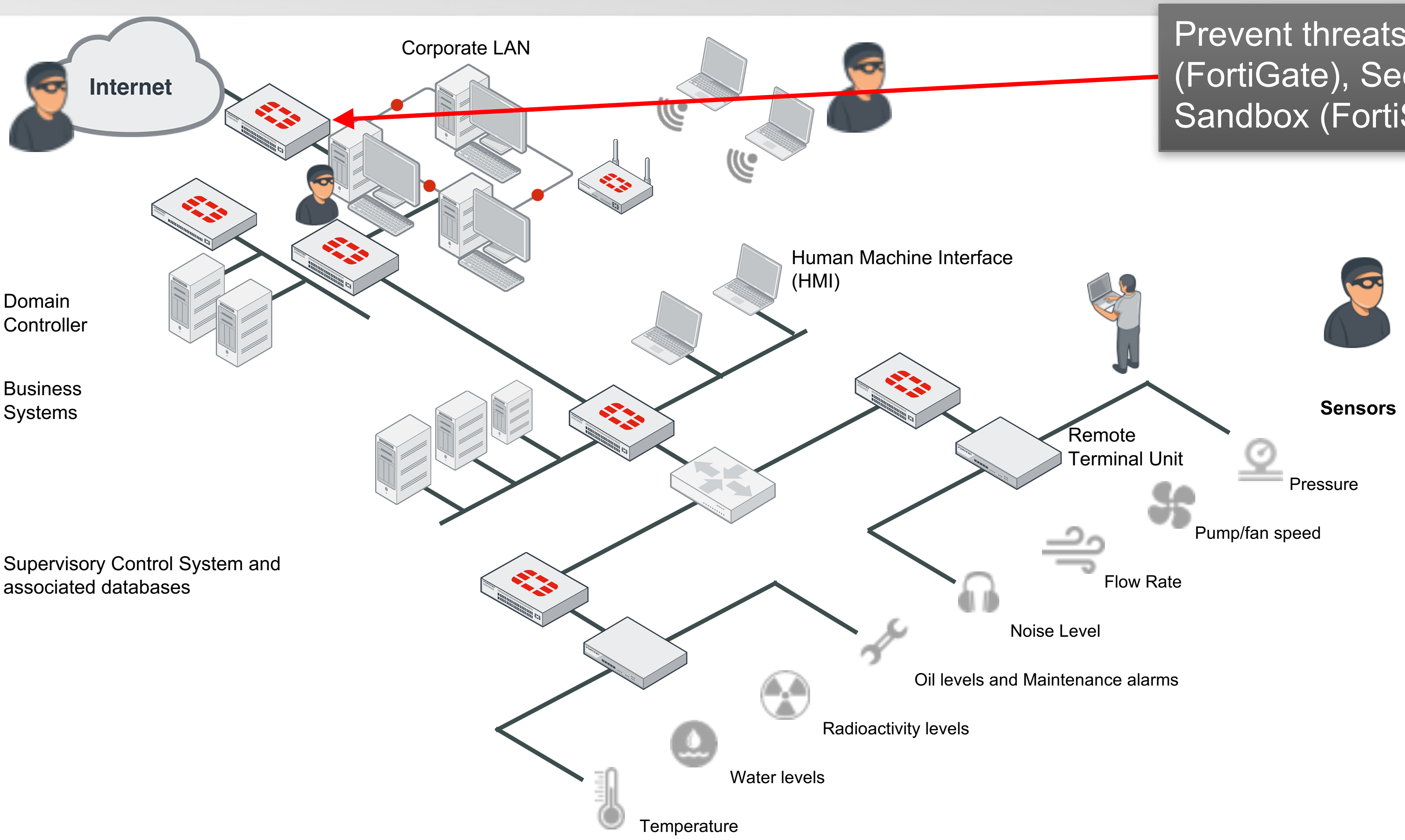


Air gap breached in multiple locations allowing threats to propogate

RTU security compromised and SCADA system vulnerable to DoS and malicious control

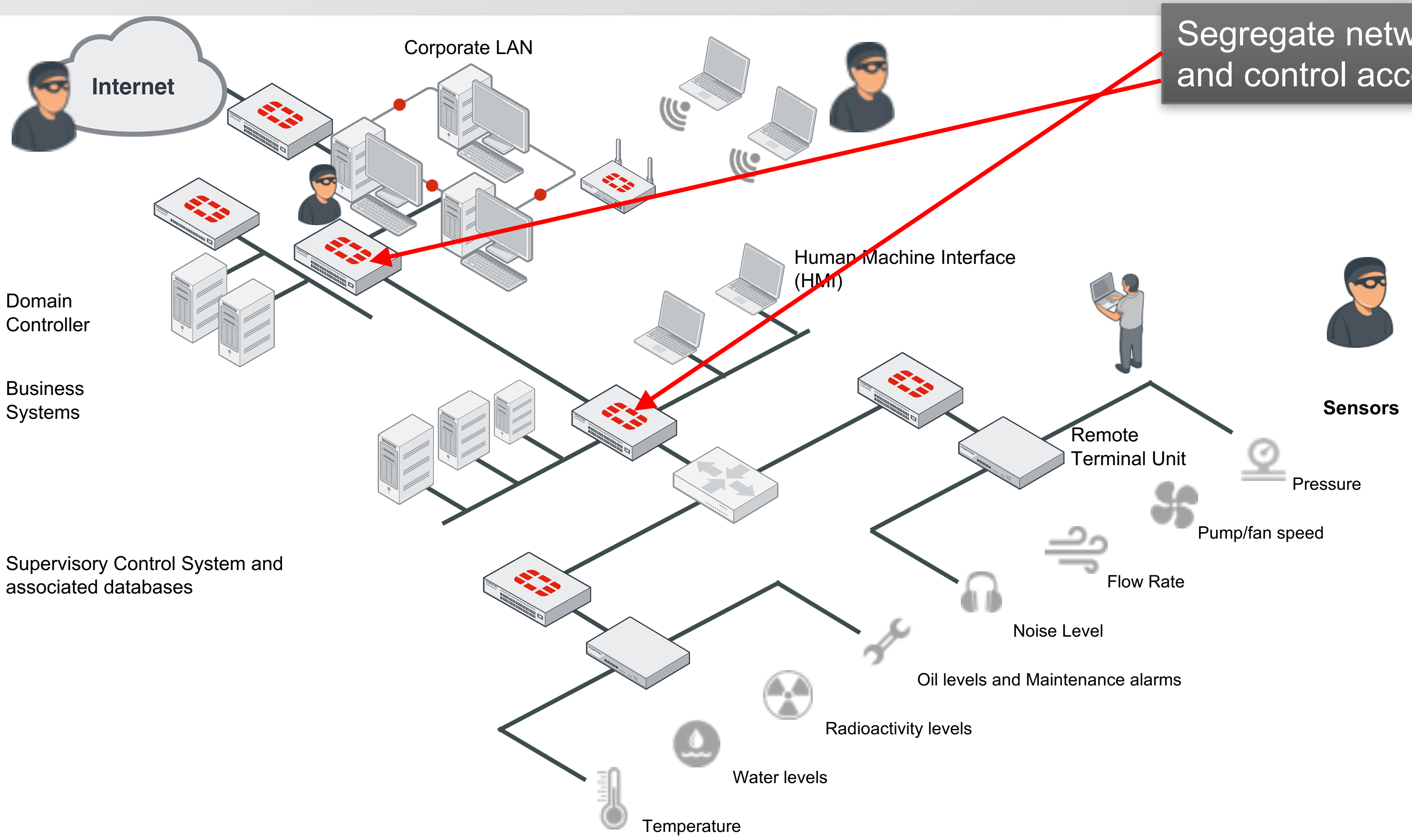
Fortinet Security Fabric for IT/OT Convergence

Prevent threats from entering with NGFW (FortiGate), Secure Email Gateway (FortiMail) and Sandbox (FortiSandbox)



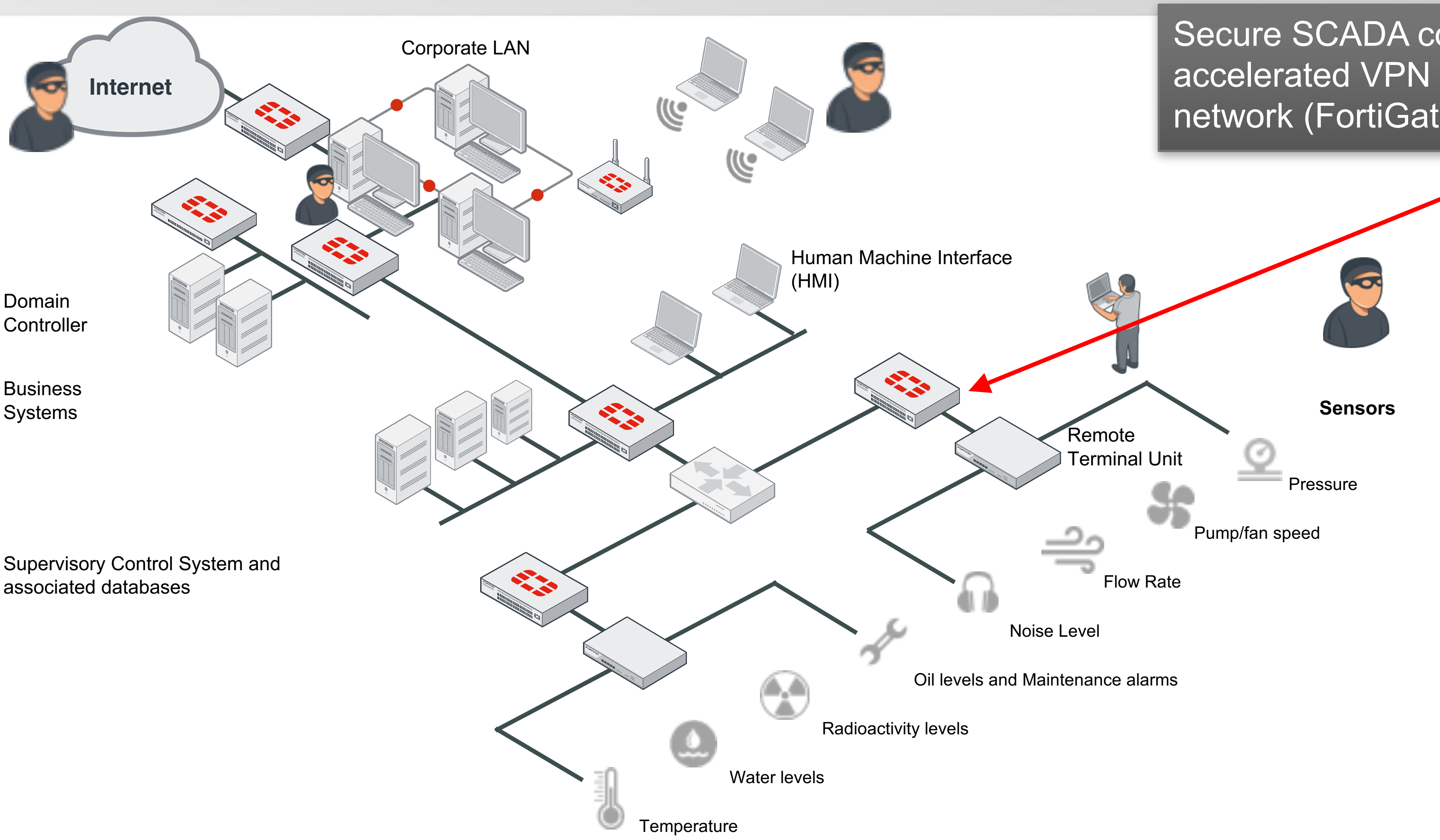
Fortinet Security Fabric for IT/OT Convergence

Segregate networks, prevent malware (FortiGate) and control access (FortiAuthenticator)



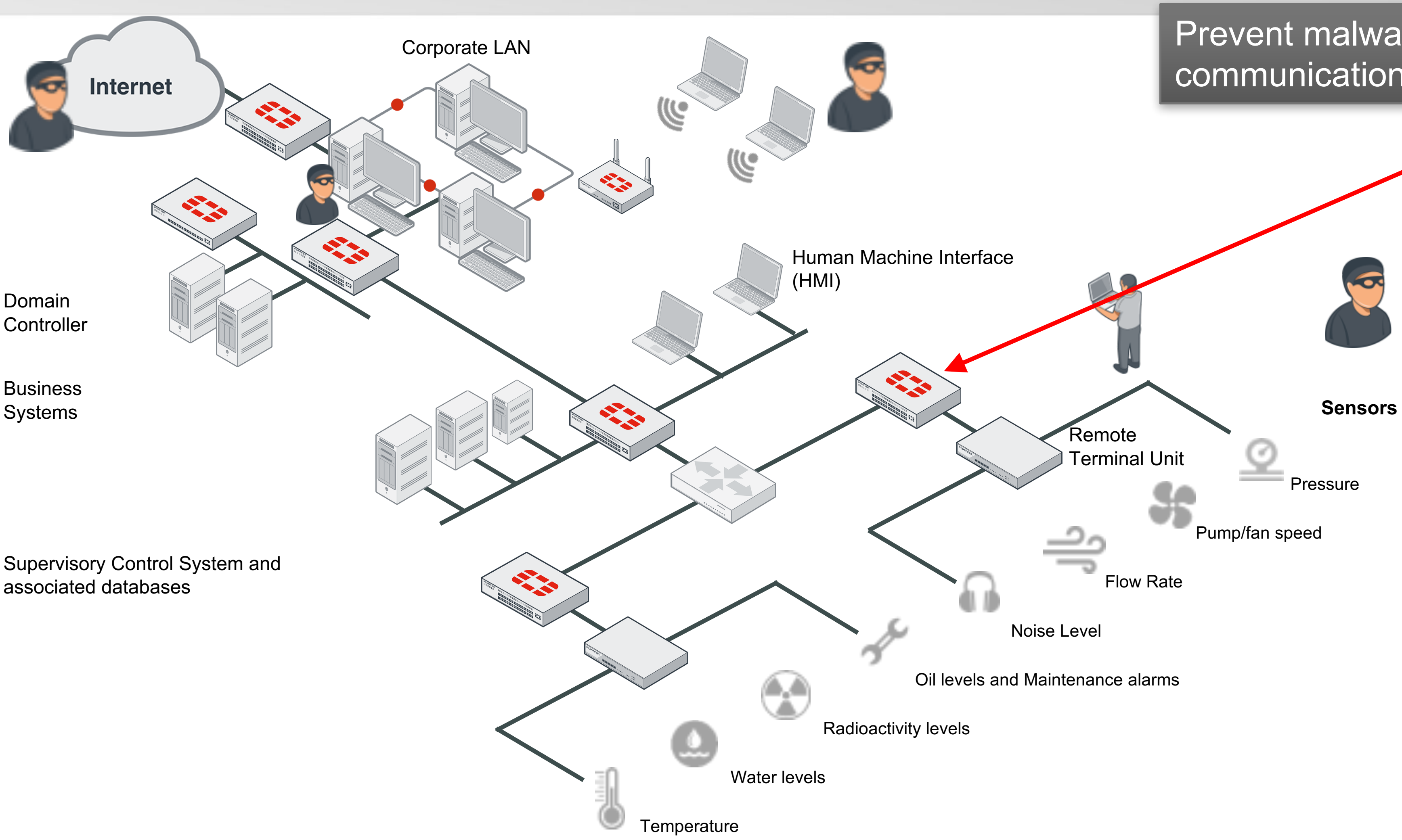
Fortinet Security Fabric for IT/OT Convergence

Secure SCADA communications with hardware accelerated VPN back to the Management HMI network (FortiGate)



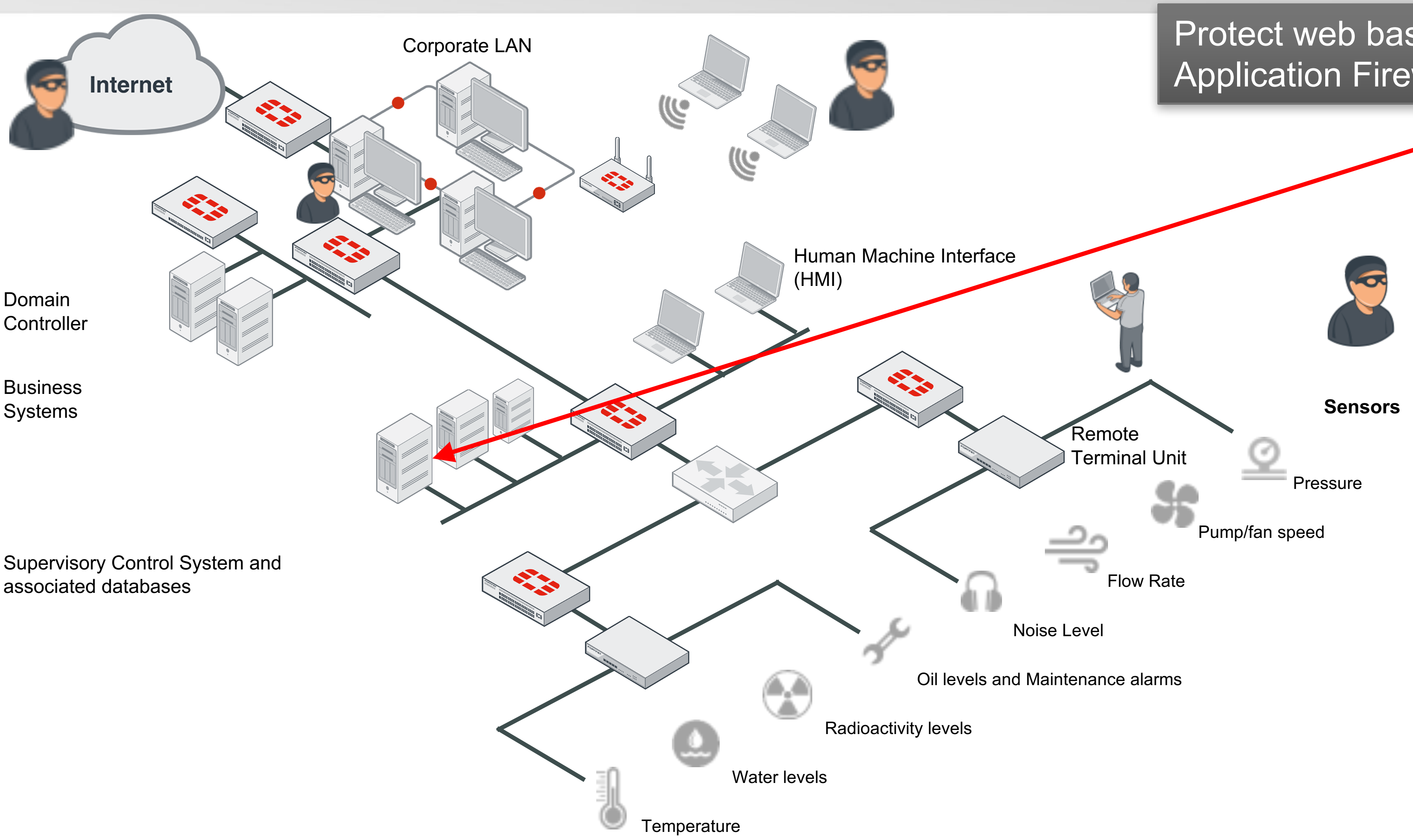
Fortinet Security Fabric for IT/OT Convergence

Prevent malware propagation and non-authorized communication channels (FortiGate)



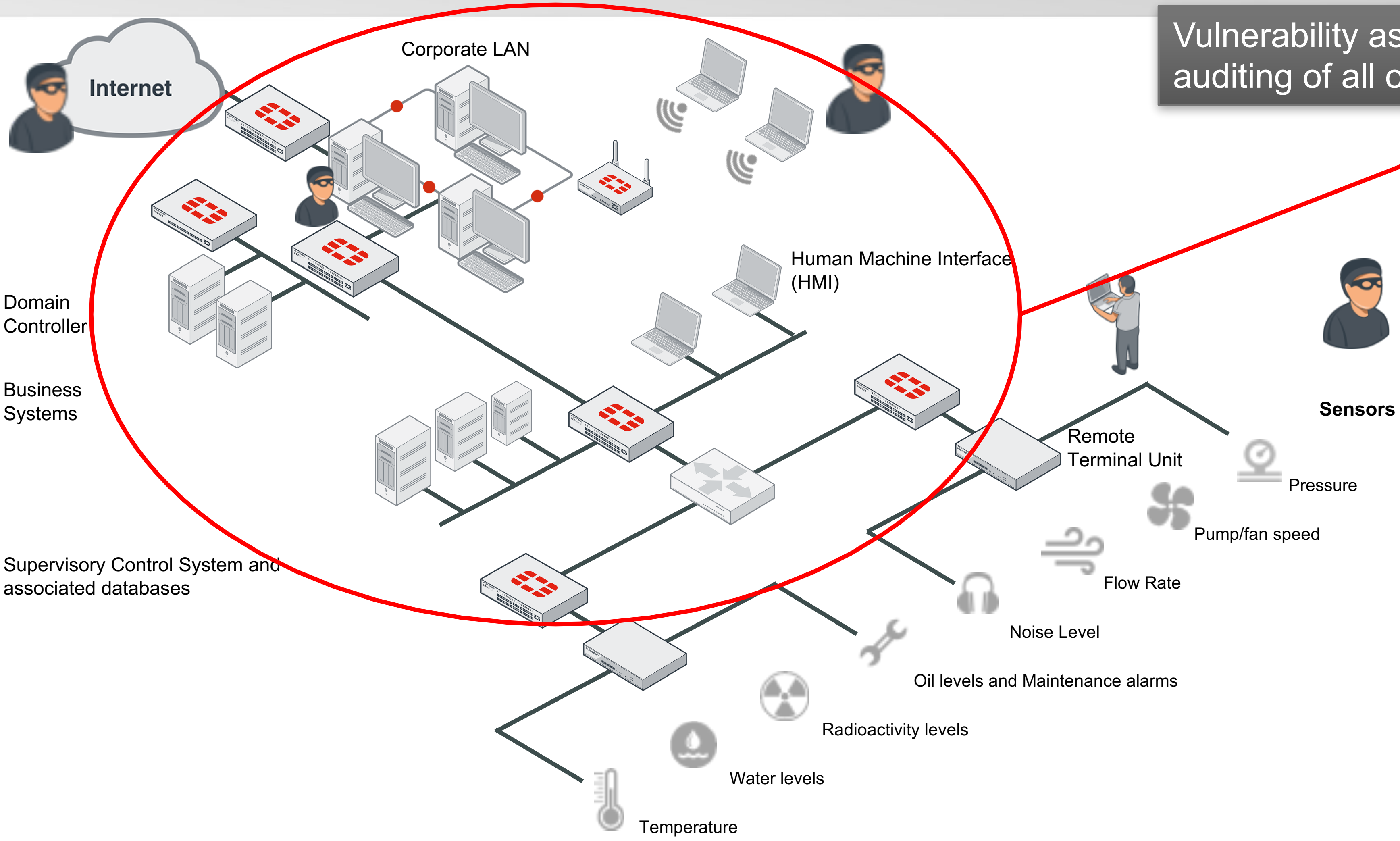
Fortinet Security Fabric Strategy

Protect web based HMI from exploitation with Web Application Firewalling (FortiWeb)



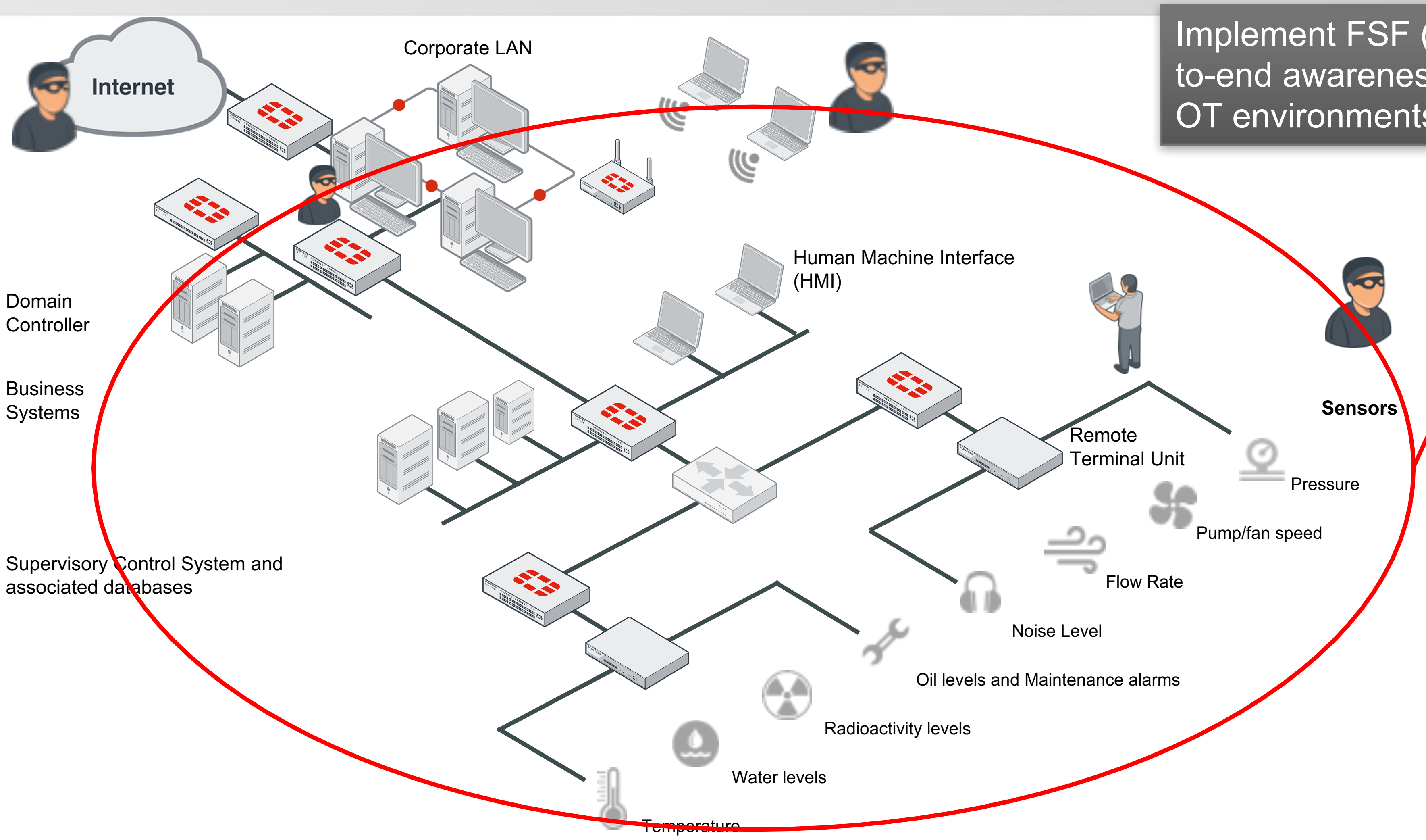
Fortinet Security Fabric for IT/OT Convergence

Vulnerability assessment, patch management and auditing of all organizational assets (FortiClient)



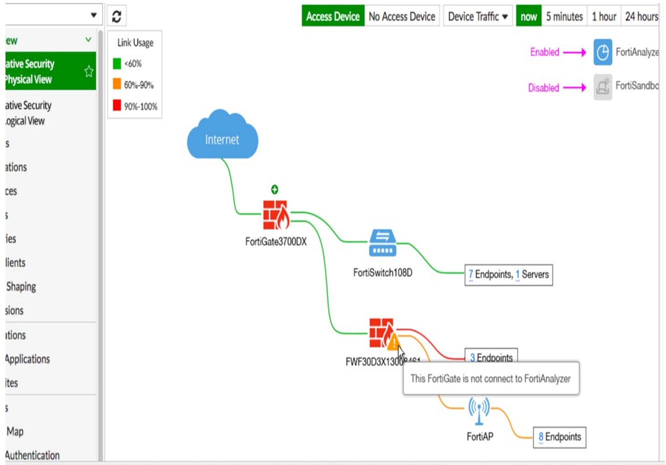
Fortinet Security Fabric for IT/OT Convergence

Implement FSF (Fortinet Security Fabric) for end-to-end awareness and control across both IT and OT environments



OS

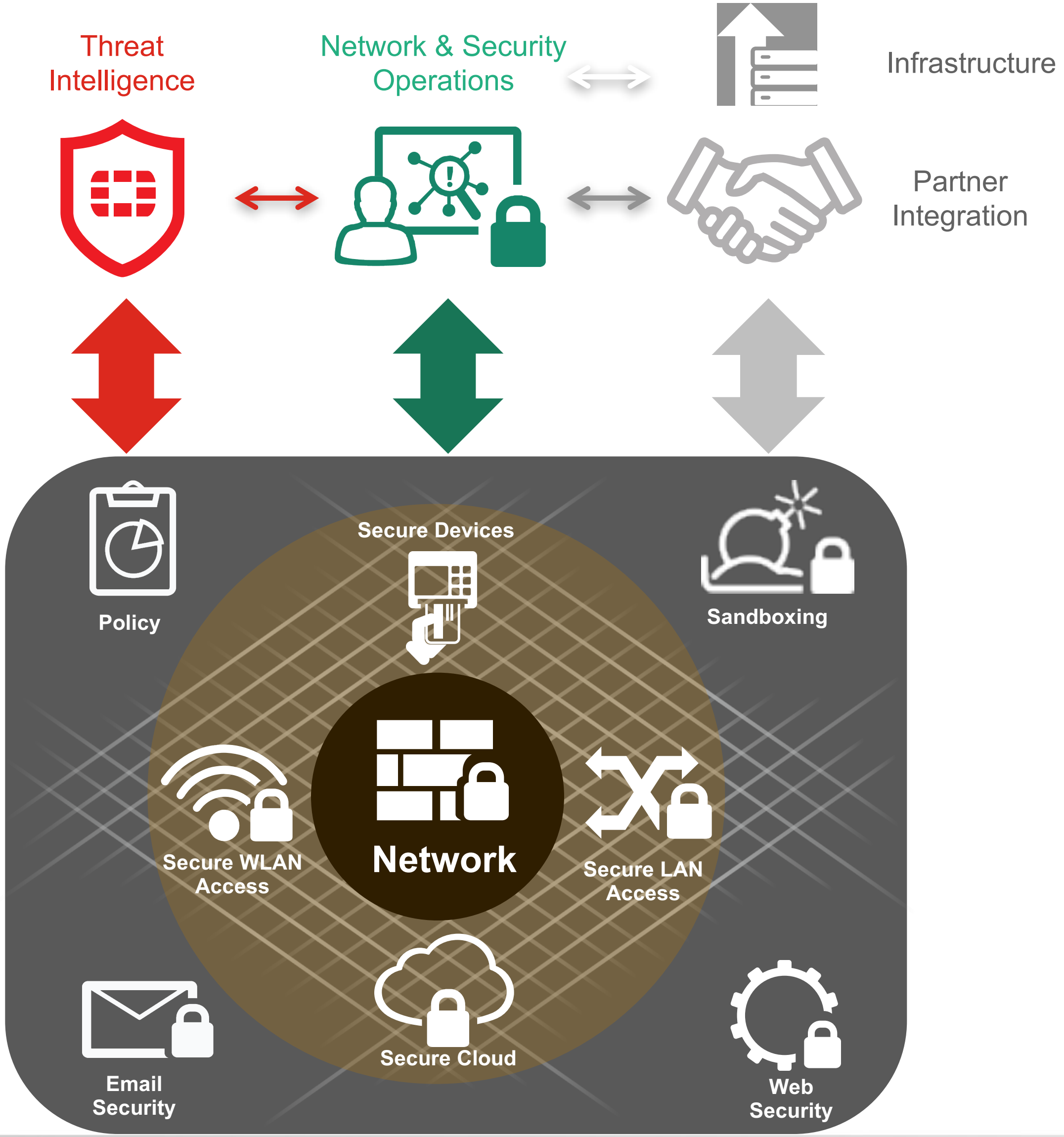
Fortinet Security Fabric



This FortiGate is not connect to FortiAnalyzer

FAST. SECURE. GLOBAL.

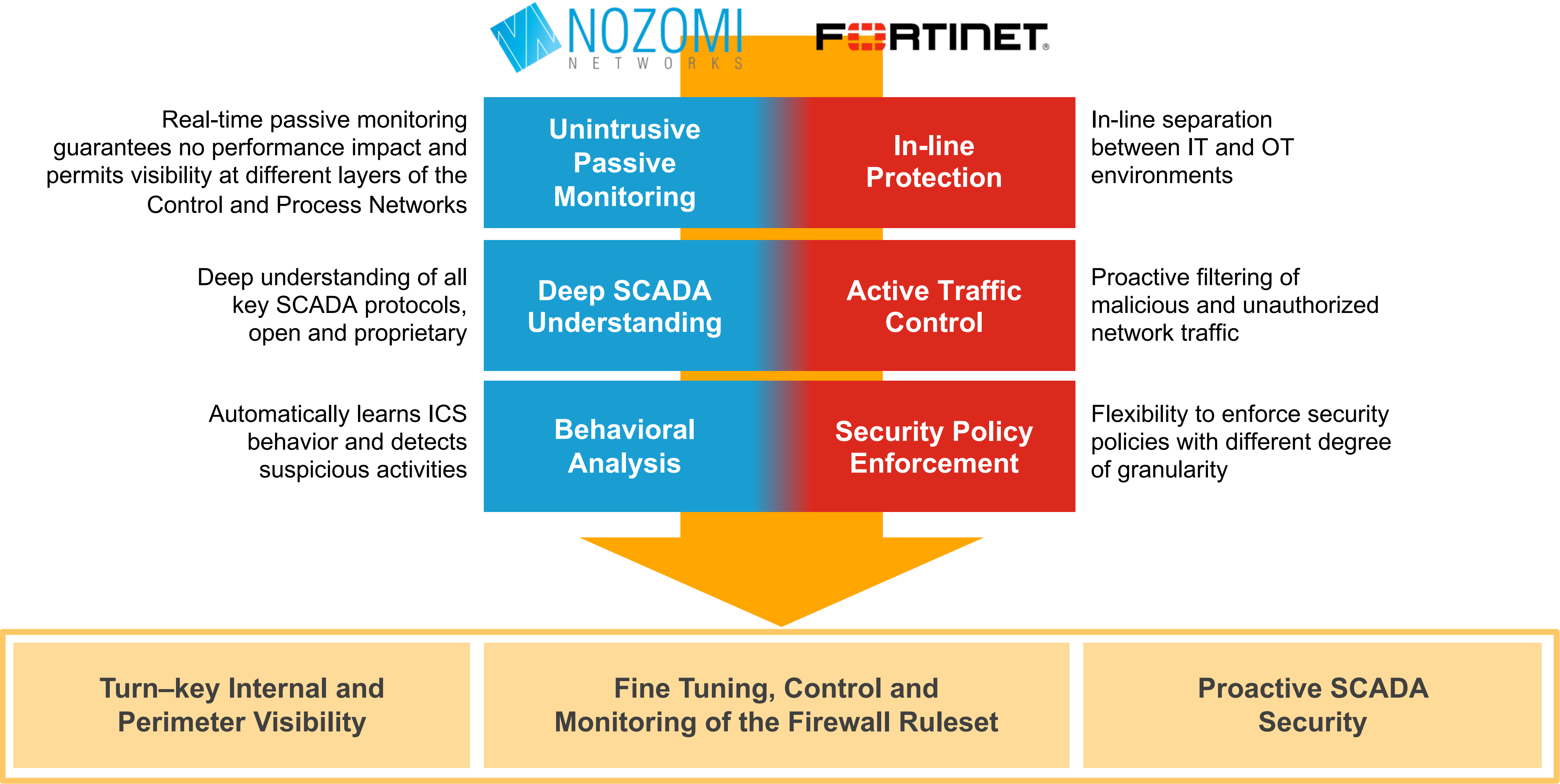
Fortinet Security Fabric from IoT to Cloud



Automated Operations

- Inner Core Network Security
- Outer Core Security
  - Access, Cloud & Endpoints
- Extended Security
  - ATP, Email, Web & Policy
- Threat Intelligence
- Security Operations
- Partner Integration

… our Answer is an Active Integration between SCADAguardian and Fortigate



Real-time passive monitoring guarantees no performance impact and permits visibility at different layers of the Control and Process Networks

Unintrusive Passive Monitoring

In-line Protection

In-line separation between IT and OT environments

Deep understanding of all key SCADA protocols, open and proprietary

Deep SCADA Understanding

Active Traffic Control

Proactive filtering of malicious and unauthorized network traffic

Automatically learns ICS behavior and detects suspicious activities

Behavioral Analysis

Security Policy Enforcement

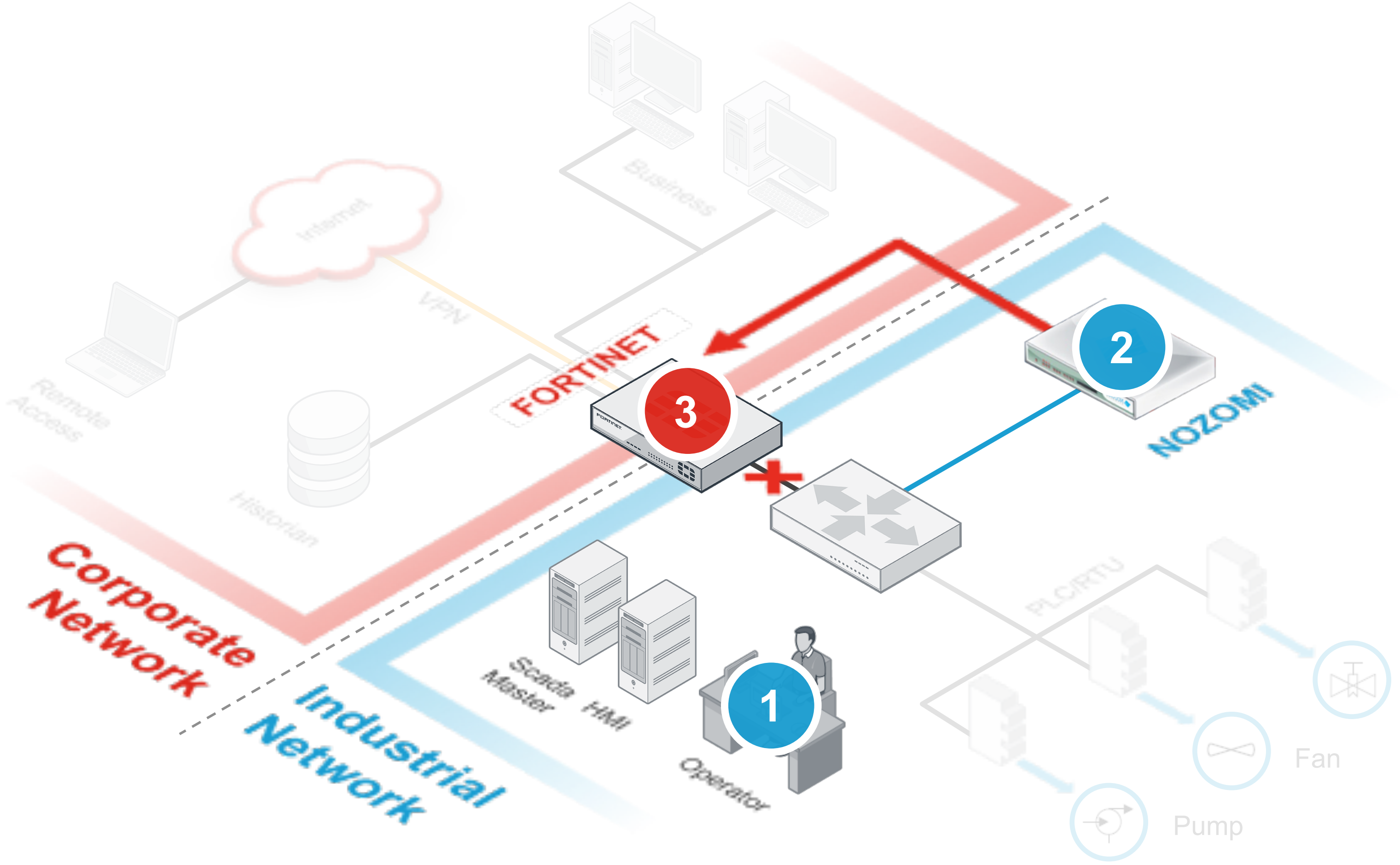
Flexibility to enforce security policies with different degree of granularity

Turn–key Internal and Perimeter Visibility

Fine Tuning, Control and Monitoring of the Firewall Ruleset

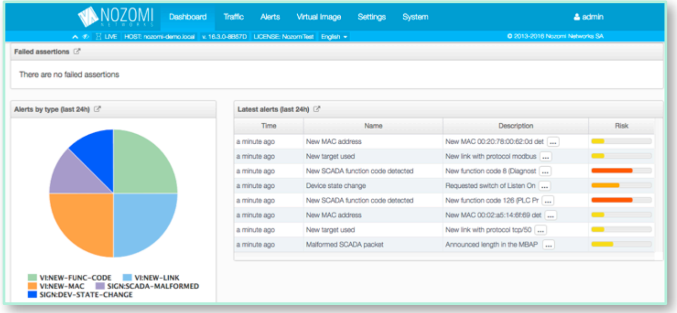
Proactive SCADA Security

Responding to Threats in Real Time



1 Monitor

A threat is detected by SCADAguardian and an alert is generated



Failed assertions

There are no failed assertions

Alerts by type (last 24h)

Latest alerts (last 24h)

Time	Name	Description	Risk
a minute ago	New MAC address	New MAC 00:20:78:00:62:0d det ...	
a minute ago	New target used	New link with protocol modbus ...	
a minute ago	New SCADA function code detected	New function code 8 (Diagnost ...	
a minute ago	Device state change	Requested switch of Listen On ...	
a minute ago	New SCADA function code detected	New function code 126 (PLC Pr ...	
a minute ago	New MAC address	New MAC 00:02:a5:14:6f:69 det ...	
a minute ago	New target used	New link with protocol tcp/50 ...	
a minute ago	Malformed SCADA packet	Announced length in the MBAP ...	

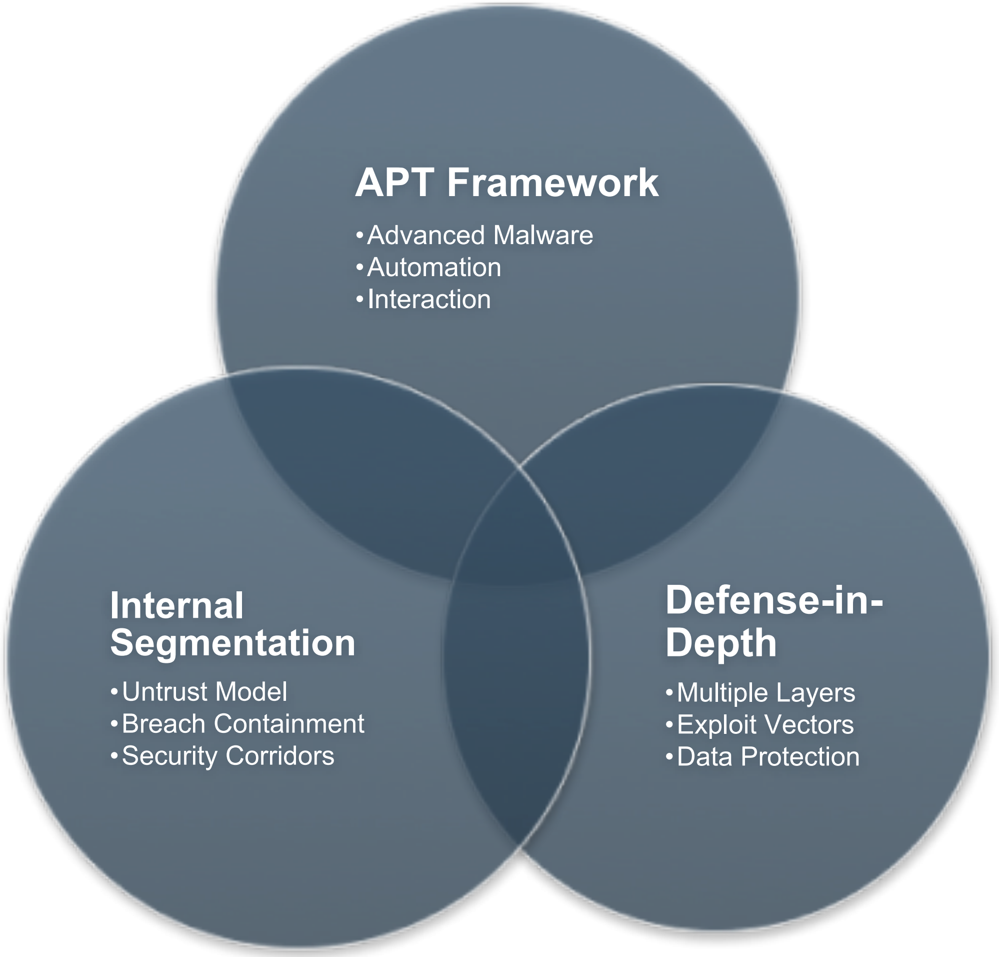
2 Detect

User-defined policies are examined and the appropriate corresponding action is triggered

3 Protect

FortiGate responds according to the user-configured action (Node Blocking, Link Blocking, or Kill Session) in order to mitigate the issue

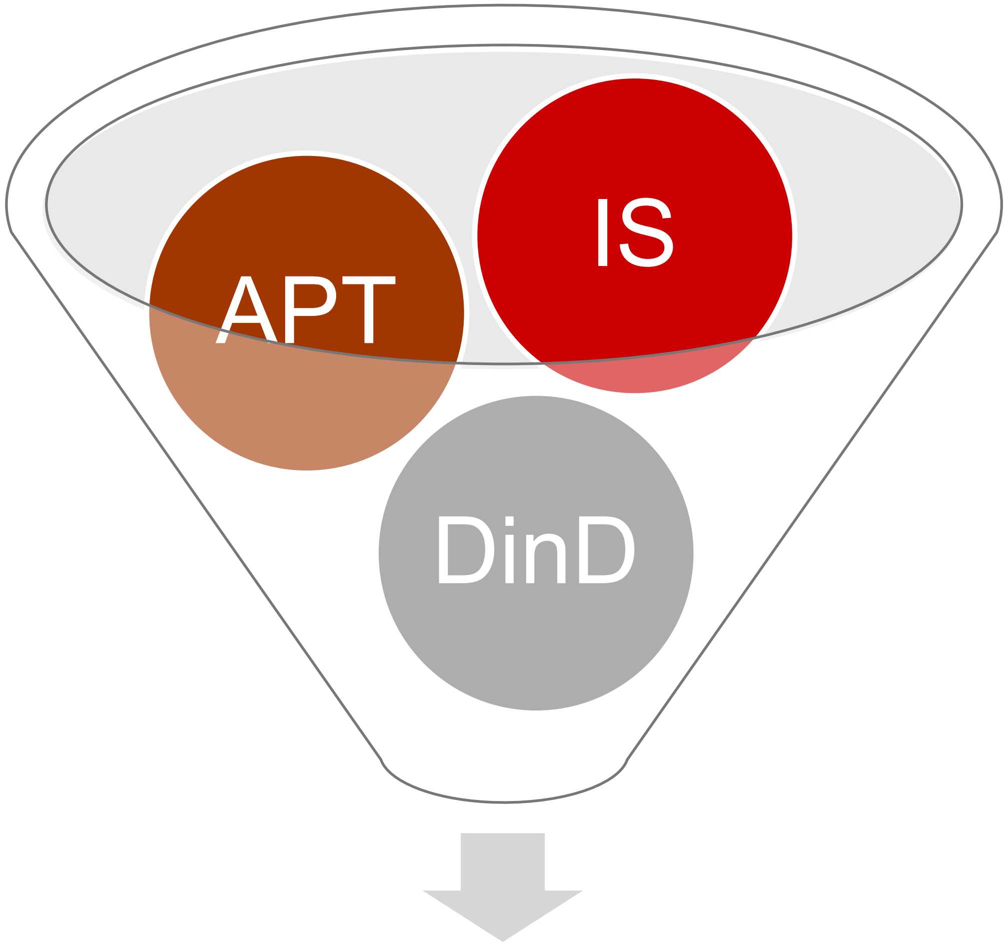
Fortinet's ICS Layered Defense Model



APT Framework
- Advanced Malware
- Automation
- Interaction

Internal Segmentation
- Untrust Model
- Breach Containment
- Security Corridors

Defense-in-Depth
- Multiple Layers
- Exploit Vectors
- Data Protection



Fortinet ICS Layered Defense Model

FORTINET®