APERIO
Critical System Resilience

ARE YOUR SYSTEMS LYING TO YOU?

91%
of public-facing ICS components are remotely exploitable
(**Kaspersky Labs**)

X2 X4
Compromise of operational systems more than **doubled** in 2015; exploits of embedded systems **quadrupled**
(**PWC Global State of InfoSec Survey**)

$1 TRILLION
The estimated cost of a cyber attack on the U.S. power grid
(Lloyd's of London)

A PERSISTENT ATTACKER WILL EVENTUALLY BREACH CRITICAL CONTROL SYSTEMS

Attacker **BREACHES** Operational Network

To Inflict Severe Damage, Attacker **MUST BLIND** Operators And Protection Mechanisms

Attacker Deceives Plant Operators by **FORGING** Reported State of Critical Systems

SEVERE DAMAGE!

ONCE INSIDE, AN ATTACKER CAN CREATE SEVERE DAMAGE:

INSIDER THREATS

Rogue employees were responsible for **63%** of incidents in 2015

Australian wastewater company contractor disabled scada functions, allowing **800,000** Liters Of Untreated Sewage to Spill

STATE-SPONSORED AGENTS

Ukraine's power grid breached, leaving a quarter **million people in the dark**

North Korea accused of breaching South Korea's **public transportation systems**

Iran accused of **breaching the control system** of a dam in NY State

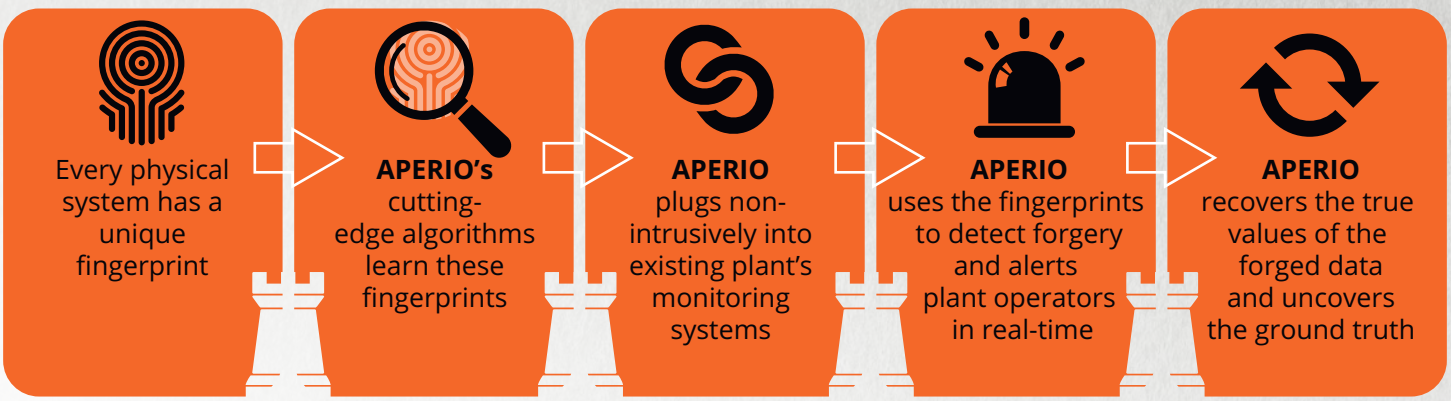
TERRORISTS, CYBERCRIMINALS & HACKTIVISTS

Al Qaeda member worked at five different U.S. nuclear power plants

Syrian hacktivists accused of breaching U.S. water purification plant, modifying amounts of chemicals in water

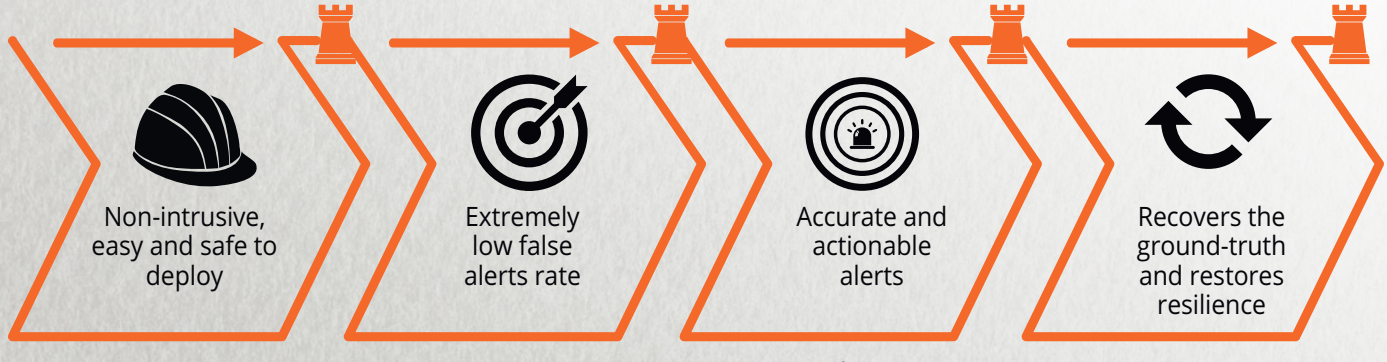
APERIO
Critical System Resilience

APERIO SYSTEM'S SOLUTION:
DATA FORGERY PROTECTION™(DFP)



APERIO SYSTEMS RESTORES CRITICAL SYSTEMS' RESILIENCE

APERIO SYSTEMS' ADVANTAGES:



Energy | Oil and Gas | Water and Waste Control | Pharma | Manufacturing | Transportation

To request a demo, please contact us at: **info@aperio-systems.com**
www.aperio-systems.com