FortiDeceptor For OT

Deceive | Expose | Eliminate Threats

Moshe Ben-simon

VP Product Management, ATP Group

May 1, 2022

Agenda

01

OT Security challenges

02

Why Deception?
Why Now?

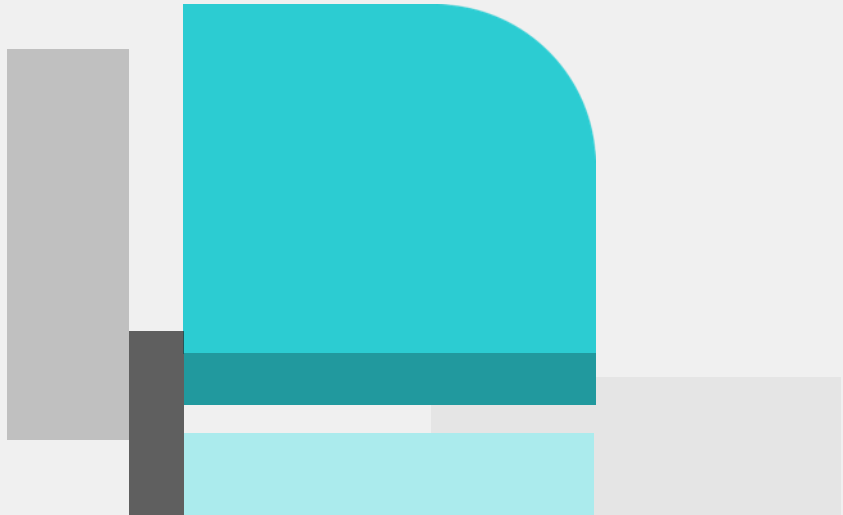
03

FortiDeceptor Technology

04

Deception as part of the Fabric / ECO system

OT Security Challenges



The Industry Agrees…

IT / OT Convergence

“OT environments that were traditionally separated are no longer completely isolated. They now have direct connections for business, OEMs and other third parties.”

Gartner, Reduce Risk to Human Life by Implementing This OT Security Control Framework published 17 June 2021

Long Lifespan

“The automation hardware in a process automation system is often capable of running 20 to 30 years.”

Automation’s Life Cycle Management of Processing Automation Control Systems, published April 2021

Incidents Underreported

“15% of survey respondents have experienced a security incident last year that crippled operational or mission-critical systems.”

Gartner, Emerging Technologies: Critical Insights for Operational Technology Security published November 10, 2021

Connectivity Driving Risk

“Connectivity to external systems continues as the overwhelming root cause of incidents, an indications that organizations still fail to follow network segmentation best practices.”

SANS *2021* Survey: OT/ICS Cybersecurity, published August 2021

Mixing legacy and modern tech

“Technical integration of legacy and aging OT technology with modern IT systems is the biggest challenge facing securing OT technology and process.”

SANS 2021 Survey: OT/ICS Cybersecurity, published August 2021

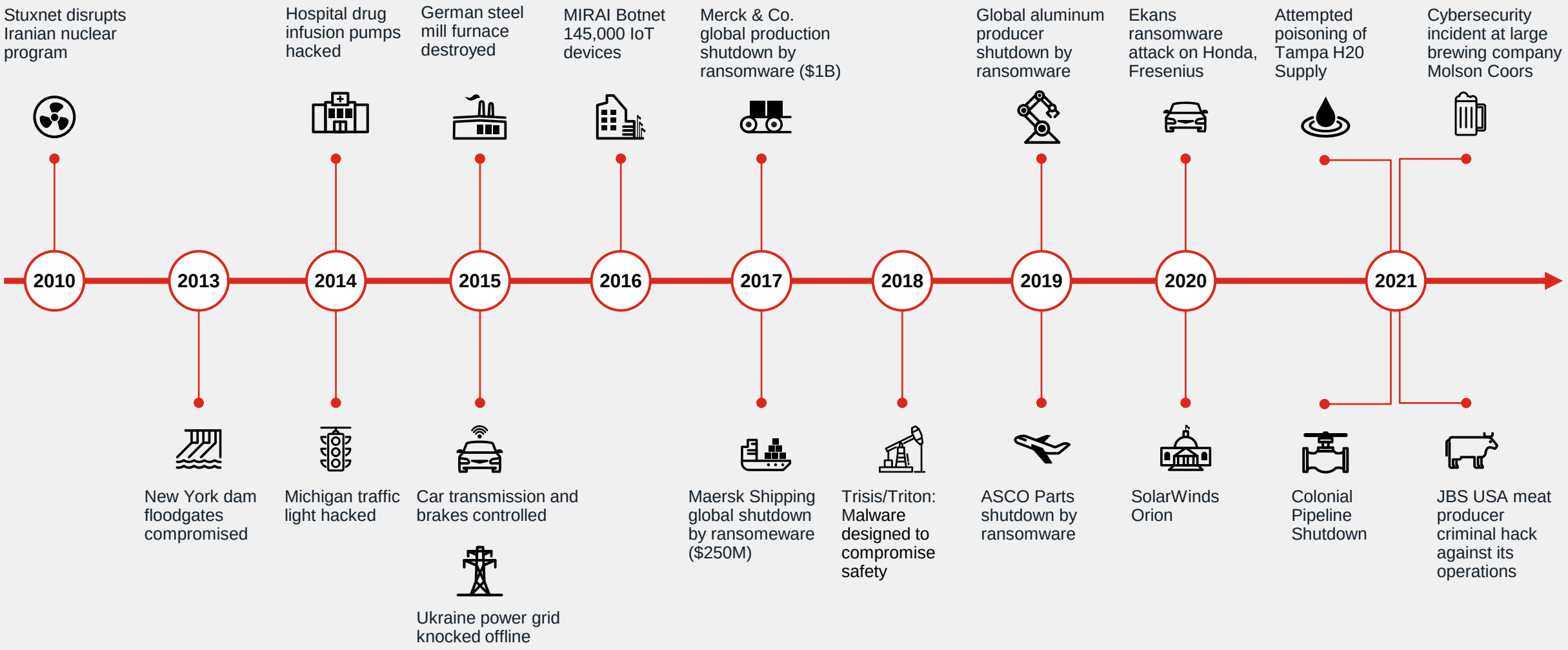
Insecure Remote Access

“42% indicate that their control systems had direct connectivity to the internet up from 12% in 2019.”

SANS 2021 Survey: OT/ICS Cybersecurity, published August 2021

OT Infrastructure Attacks Are Getting Worse

Attacks are increasing in frequency and impact



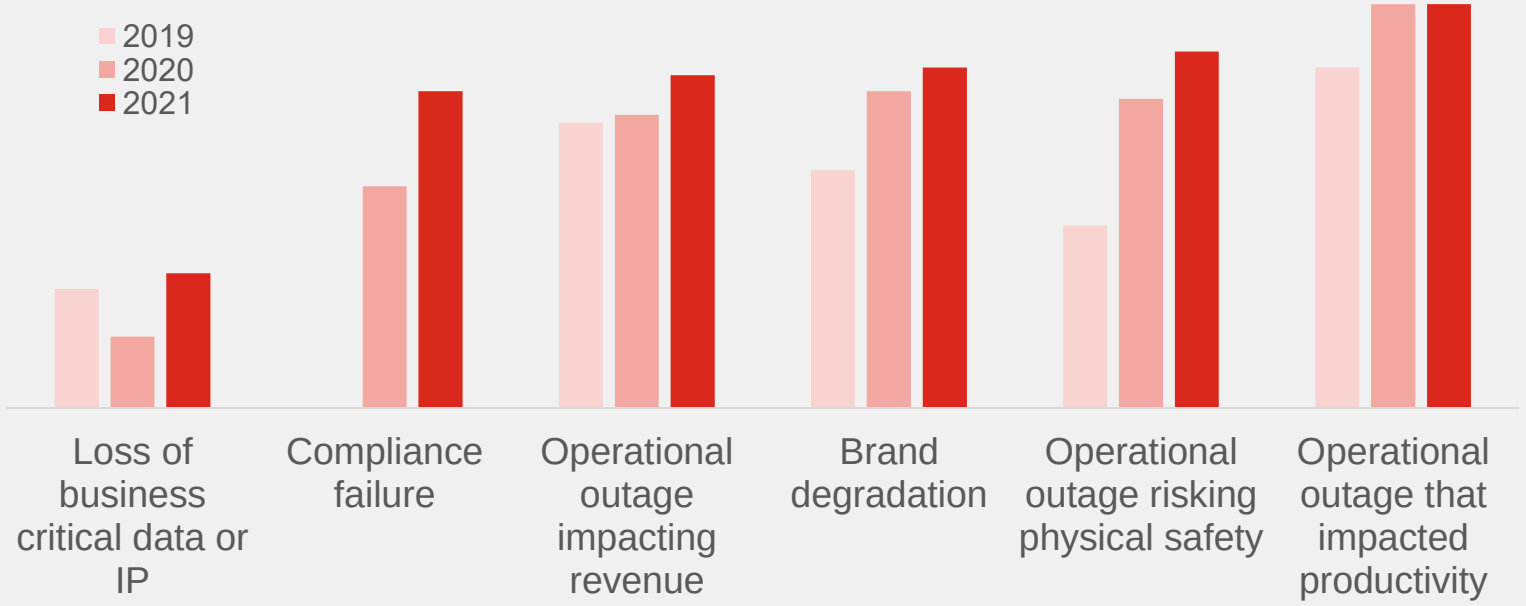
OT Risk Is Proportional to OT Connectivity

Yet inversely proportional to the integration of IT/OT security management

9 out of 10

OT organizations experienced at least one intrusion in the past year and **63% had 3 or more intrusions**, which is similar to the results in 2020.

Impact on organization



Top-tier organizations are…

…likely to use **orchestration and automation** and have **security tracking and reporting** in place.

100% **centralized visibility** in their security operations center.

Data is from Fortinet's **2021 State of Operational Technology and Cybersecurity Report**

Source: Fortinet's 2021 State of Operational Technology and Cybersecurity Report

Why Deception Now?
Well-defined and Proven Technology

Cyber Deception Technology is recognized by Gartner as the most effective method to detect advanced threats

"Prioritize deception-based detection approaches for environments that cannot use other security controls due to technical reasons (for example, IoT, SCADA or medical environments) or due to economic reasons (for example, environments with highly distributed networks)."

- Gartner Hype Cycle for Threat-Facing Technologies, 2018

"Security organization dealing with skill-set shortages are prioritizing low friction approaches such as Deception over resource intensive approaches such as SIEM, UEBA, EDR or NTA".

- Gartner Hype Cycle for Threat-Facing Technologies, 2018

FortiDeceptor Technology

FortiDeceptor: Overview

An advanced threat deception designed to DECEIVE, EXPOSE, and ELIMINATE external and internal threats early in the attack kill chain and proactively block these threats before any significant damage occurs.

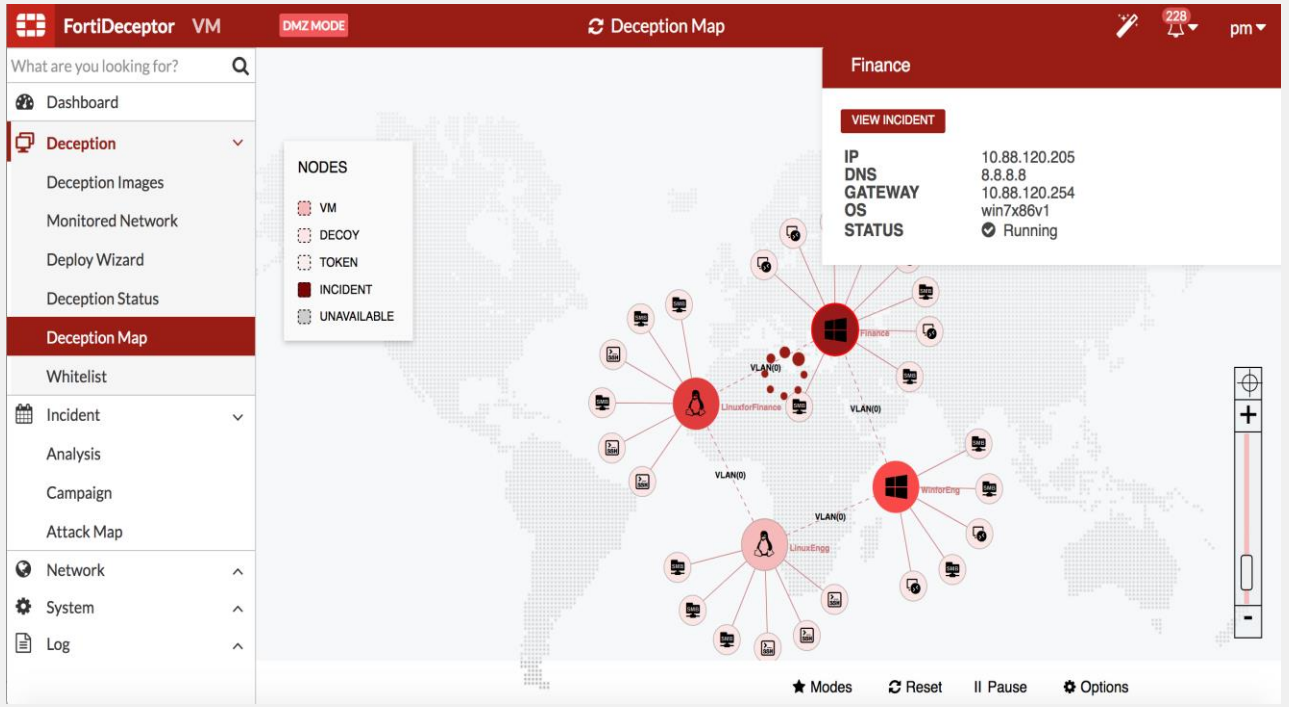
FortiDeceptor
Advanced Threat Deception

HW Appliance

Virtual Appliance

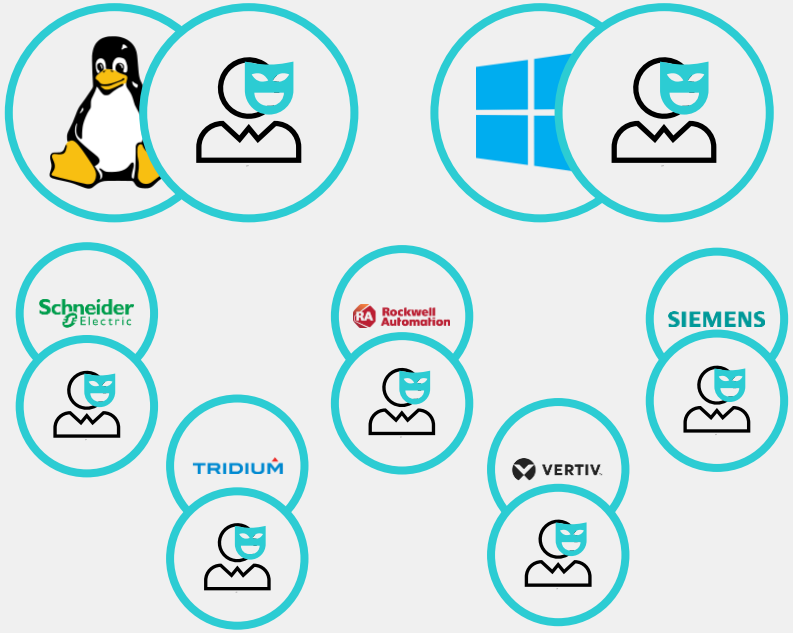
Security Fabric Integrations:

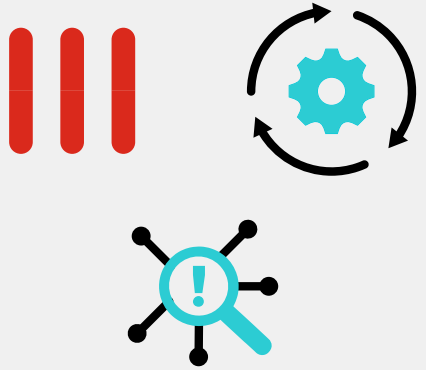
- **FortiGate**
- **FortiSIEM**
- **FortiSOAR**
- **FortiNAC**
- **FortiAnalyzer**



FortiDeceptor Vision & Benefits

DECEIVE | EXPOSE | ELIMINATE





- Deception Decoys & Lures
- Learn Your Adversaries
- Expose Attackers
- PLC Decoys

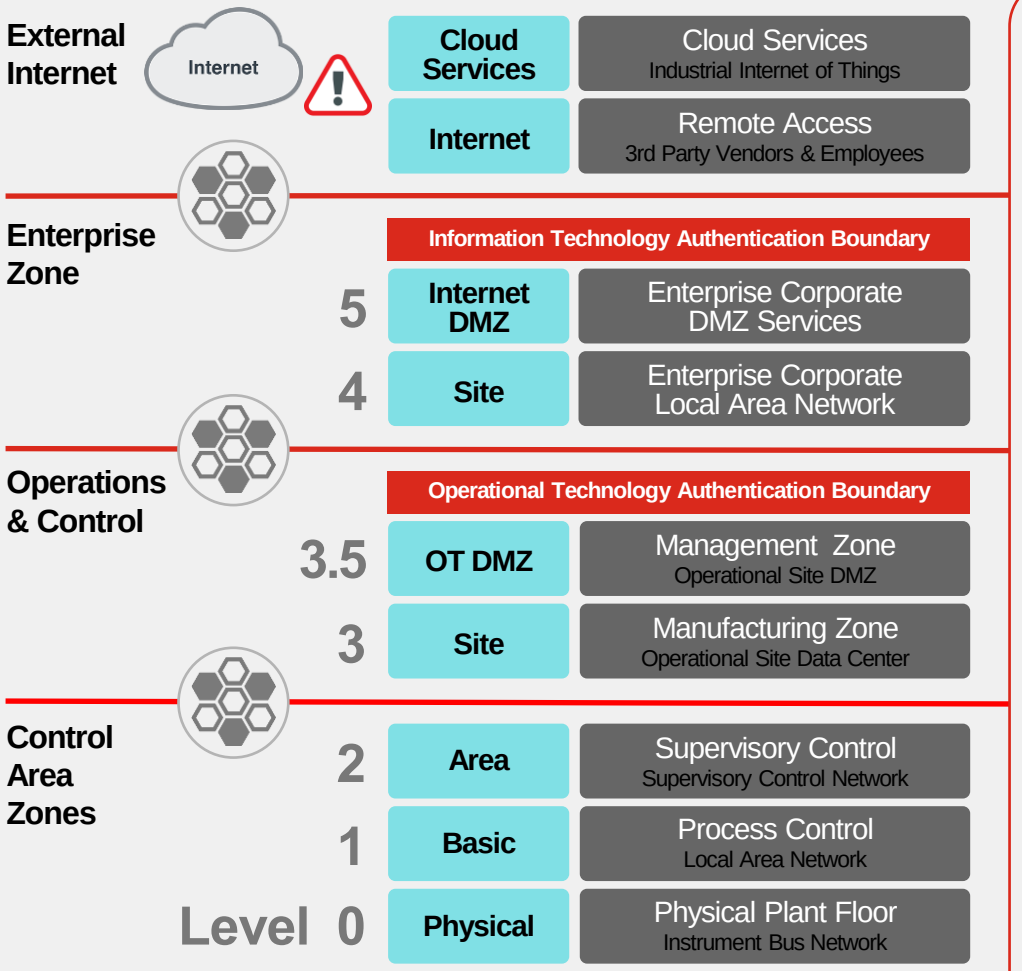
- Few & Accurate Alerts
- Increase Cost of Attackers
- Cut Down Breach Detection Time

- Auto Quarantine
- Improve SIEM Visibility
- Dynamic Deception Operation

Protecting OT – Based on the Purdue Model

with the Fortinet Security Fabric

- Access Layer Segmentation
- L2/L3 NGFW Segmentation
- Web Server Protection
- Authentication and VPN
- Threat Protection
- Application Control
- Endpoint Protection
- Deception
- Sandboxing
- NOC/SOC



1. Lure malicious actors away from the critical assets
2. Reduce the risk of them harming the real network.

FortiDeceptor As a Part of The Fortinet Security Fabric

Fortinet Security Fabric

Broad

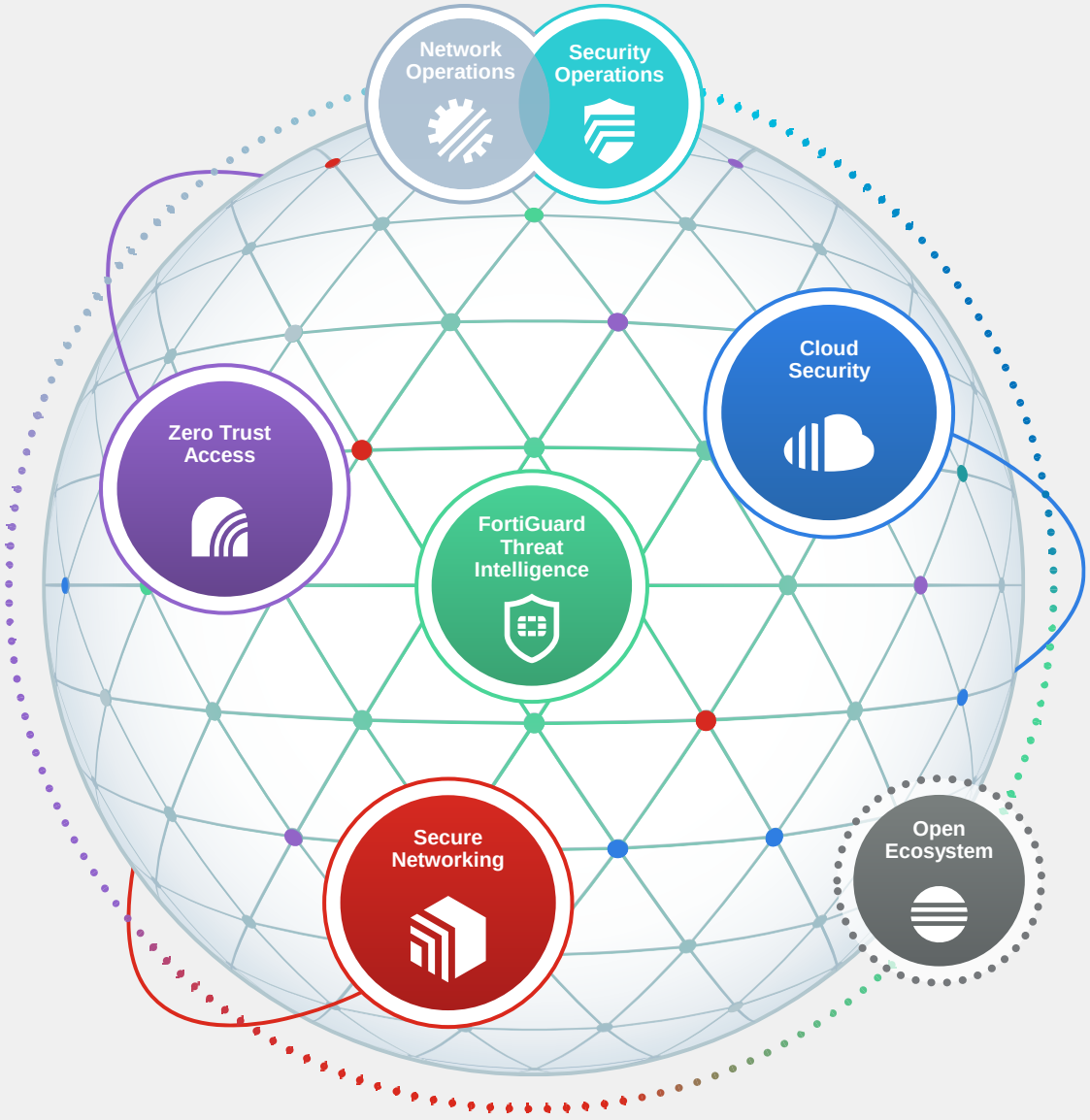
visibility and protection of the entire digital attack surface to better manage risk

Integrated

solution that reduces management complexity and shares threat intelligence

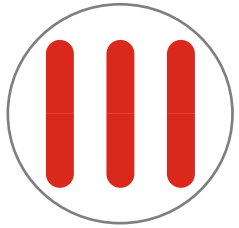
Automated

self-healing networks with AI-driven security for fast and efficient operations



Part of the Fortinet Security Fabric

FortiGate



- Dynamic rule blocking based on attack Trigger
- OT/IoT Threat Detection Capabilities
- Quarantine attacker / malware (TIC IOC)

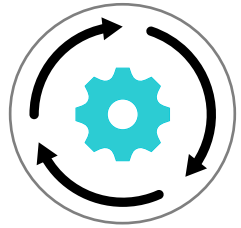
FortiNAC

- Endpoint/devices isolation automation based on attack trigger
- OT/IoT Threat Detection Capabilities

FortiSIEM

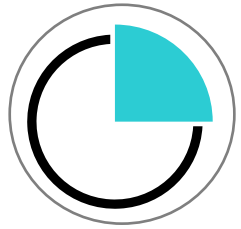
- Correlation rules detection based on false data (Token)
- Enrich the insider threat detection capabilities
- Reduce FP alerts to improve team efficiency

FortiSOAR



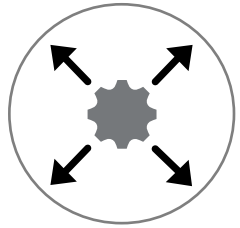
- Orchestrate mitigation & remediation response based on attack trigger.
- Enrich the MDR workflow with threat intelligence IOC's

FortiAnalyzer



- Enrich the threat detection with attack IOC's
- Built-in security and analytics reporting

Third-Party



- Generic REST-API wizard builder to integrate with any third part tools for Mitigation & Remediation

FortiDeceptor enhances threat detection within the Fortinet Security Fabric

Summary

- Manufacture & Utilities are high profile targeted industries
  - Security often has limited investment and resources
- Motivated threat actors will find a way in
  - Focusing protection at the perimeter is not sufficient
  - “Trusted” devices are not secure and highly vulnerable
- OT Devices threats need to be treated with highest priority
  - Once OT device get compromised, threat actors have little to no limits
- Deception provides unique visibility and disorientates attackers
- Full OS and Emulation Decoys
  - Rockwell & Siemens PLC,BACNET, IPMI, Industrial automation platform (windows OS Custom Decoy) and many more.