Readiness Against the Rising Tide of Industrial Cyber Attacks

Steven Dahlin – Region Director

Fortinet

Welcome and Agenda

- State of the Industry
- Industry Research | Top Cybersecurity Findings
- How can Fortinet help?
- How are Hackers Getting into your Network?
- Best Practices for Securing SCADA Systems
- Take the Next Step | Grant Funding
- Q&A

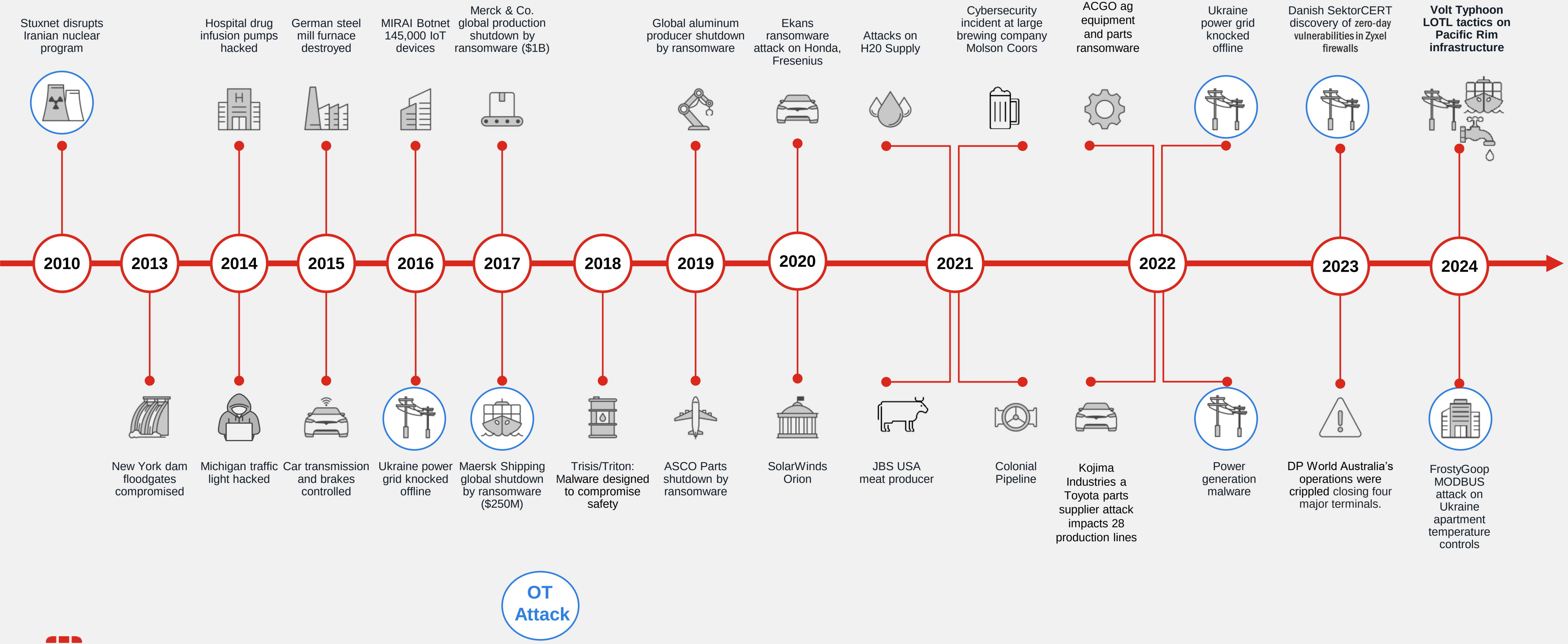
State of the Water Segment

Water and Wastewater Industry Risk and Insights

Known or perceived risk within the industry

OT Infrastructure Attacks Are Getting Worse

Attacks are increasing in frequency and impact



2010

Stuxnet disrupts Iranian nuclear program

2013

New York dam floodgates compromised

2014

Hospital drug infusion pumps hacked

Michigan traffic light hacked

2015

German steel mill furnace destroyed

Car transmission and brakes controlled

2016

MIRAI Botnet 145,000 IoT devices

Ukraine power grid knocked offline

2017

Merck & Co. global production shutdown by ransomware ($1B)

Maersk Shipping global shutdown by ransomware ($250M)

2018

Trisis/Triton: Malware designed to compromise safety

2019

Global aluminum producer shutdown by ransomware

ASCO Parts shutdown by ransomware

2020

Ekans ransomware attack on Honda, Fresenius

SolarWinds Orion

2021

Attacks on H20 Supply

Cybersecurity incident at large brewing company Molson Coors

JBS USA meat producer

Colonial Pipeline

2022

ACGO ag equipment and parts ransomware

Ukraine power grid knocked offline

Kojima Industries a Toyota parts supplier attack impacts 28 production lines

Power generation malware

2023

Danish SektorCERT discovery of zero-day vulnerabilities in Zyxel firewalls

DP World Australia's operations were crippled closing four major terminals.

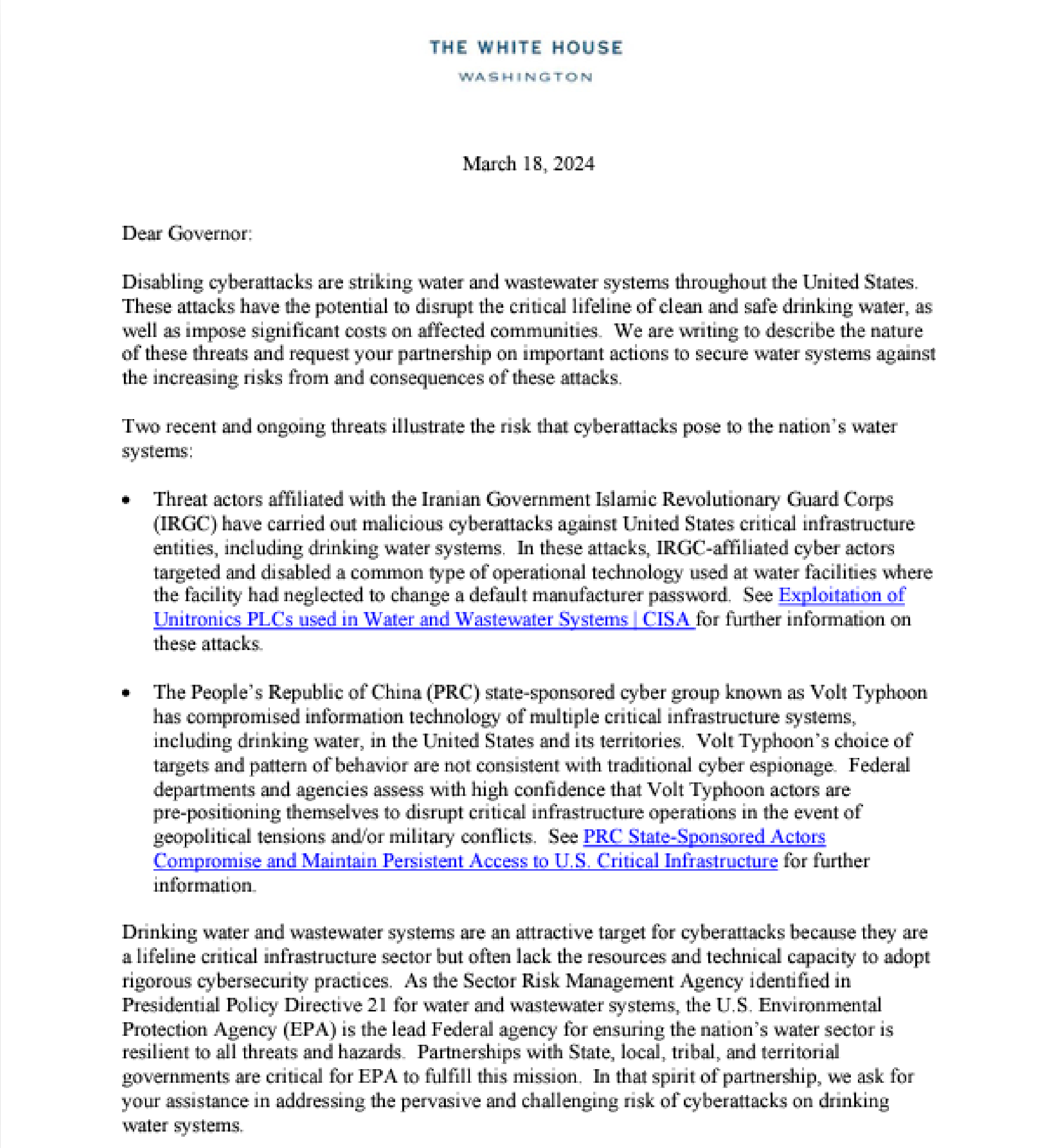
2024

Volt Typhoon LOTL tactics on Pacific Rim infrastructure

FrostyGoop MODBUS attack on Ukraine apartment temperature controls

OT Attack

2024 | Letter to Governors



THE WHITE HOUSE
WASHINGTON

March 18, 2024

Dear Governor:

Disabling cyberattacks are striking water and wastewater systems throughout the United States. These attacks have the potential to disrupt the critical lifeline of clean and safe drinking water, as well as impose significant costs on affected communities. We are writing to describe the nature of these threats and request your partnership on important actions to secure water systems against the increasing risks from and consequences of these attacks.

Two recent and ongoing threats illustrate the risk that cyberattacks pose to the nation's water systems:

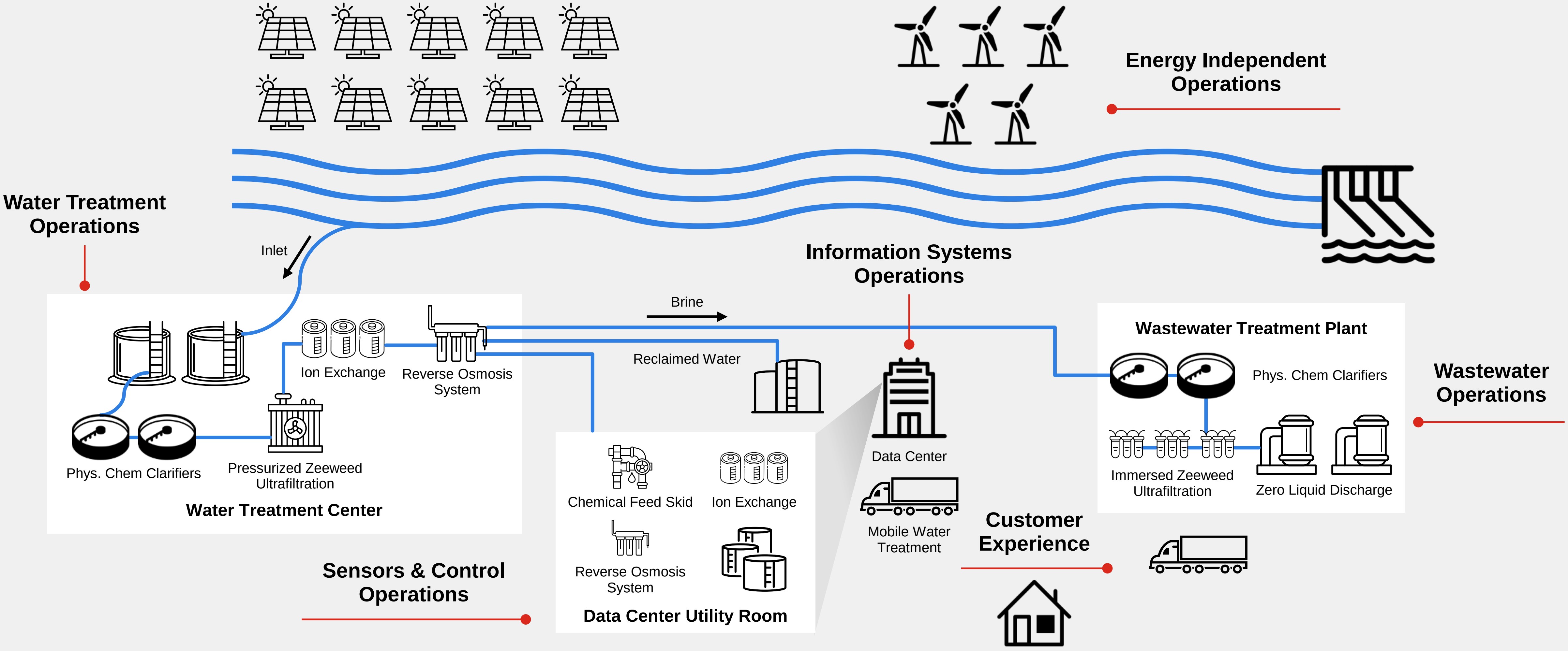
- Threat actors affiliated with the Iranian Government Islamic Revolutionary Guard Corps (IRGC) have carried out malicious cyberattacks against United States critical infrastructure entities, including drinking water systems. In these attacks, IRGC-affiliated cyber actors targeted and disabled a common type of operational technology used at water facilities where the facility had neglected to change a default manufacturer password. See Exploitation of Unitronics PLCs used in Water and Wastewater Systems | CISA for further information on these attacks.
- The People's Republic of China (PRC) state-sponsored cyber group known as Volt Typhoon has compromised information technology of multiple critical infrastructure systems, including drinking water, in the United States and its territories. Volt Typhoon's choice of targets and pattern of behavior are not consistent with traditional cyber espionage. Federal departments and agencies assess with high confidence that Volt Typhoon actors are pre-positioning themselves to disrupt critical infrastructure operations in the event of geopolitical tensions and/or military conflicts. See PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure for further information.

Drinking water and wastewater systems are an attractive target for cyberattacks because they are a lifeline critical infrastructure sector but often lack the resources and technical capacity to adopt rigorous cybersecurity practices. As the Sector Risk Management Agency identified in Presidential Policy Directive 21 for water and wastewater systems, the U.S. Environmental Protection Agency (EPA) is the lead Federal agency for ensuring the nation's water sector is resilient to all threats and hazards. Partnerships with State, local, tribal, and territorial governments are critical for EPA to fulfill this mission. In that spirit of partnership, we ask for your assistance in addressing the pervasive and challenging risk of cyberattacks on drinking water systems.

- Iranian's (IRGC) attacked US drinking water systems and disabled Unitronic PLCs. Simply because a default username and password wasn't changed.
- China's sponsored cyber group Volt Typhoon is embedding threats into our nation's infrastructure – laying in wait for a future attack.
- How do you know that they aren't in your network right now?

Digitizing the Water and Wastewater Operations

From engagement to delivery of water and services



Water and Wastewater Cybersecurity Principles

Safety & Operations First

Safety-critical and operational-critical functions needs the highest protection

Cohesive, Purpose-based Zoning

Zones impose security service requirements to the functions/devices/components

Asset Assumed Vulnerable

Field digitalization will rise exponentially

Consequences

What happens if Water and Wastewater public providers do not act:

A Regional or National Emergency

Service Disruption

Customer Harm

Economic Impact

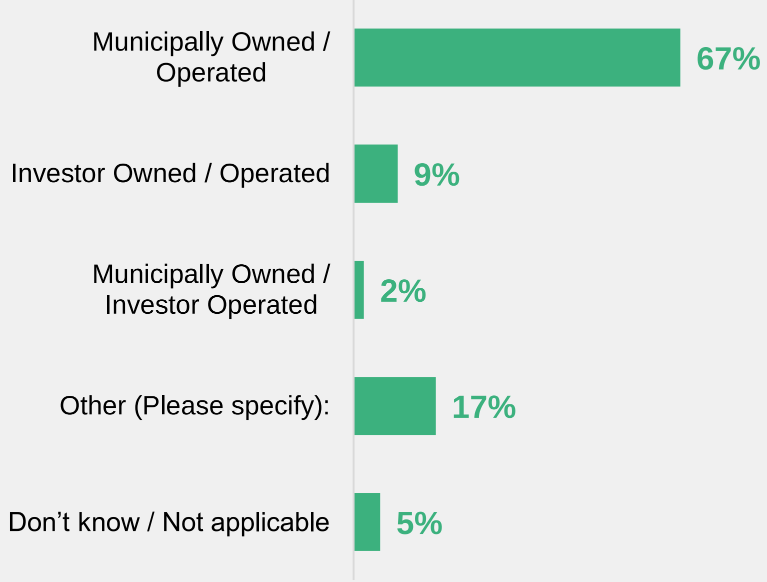
Negative Media Exposure

Recent Research

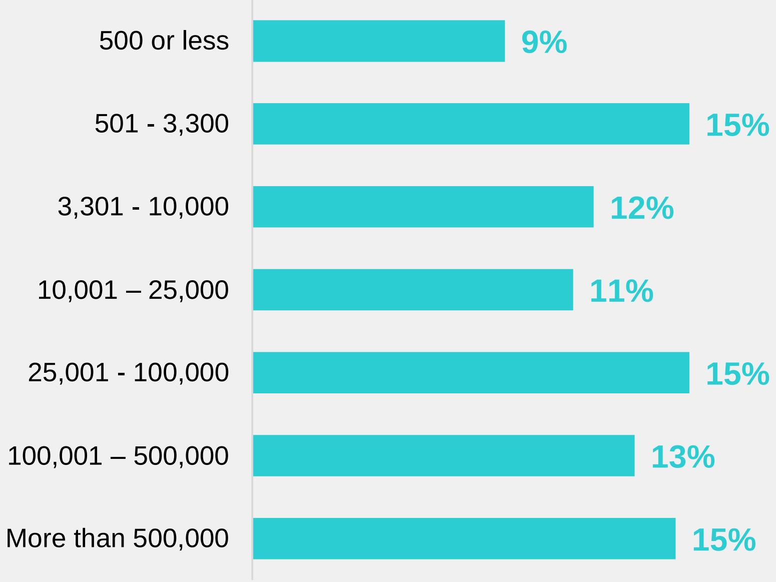
Water World and Wastewater Digest

Recent Research | Water World and Wastewater Digest

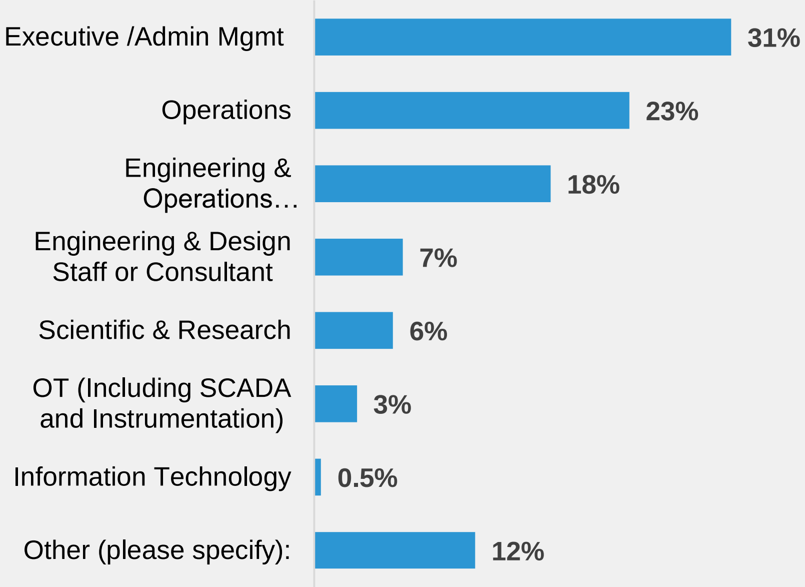
OWNERSHIP



POPULATION



JOB ROLE

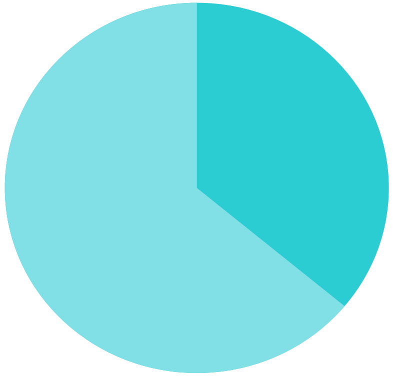


Base: 2024 Respondents (n=410)

Cybersecurity in Water Management Facilities

Research Findings

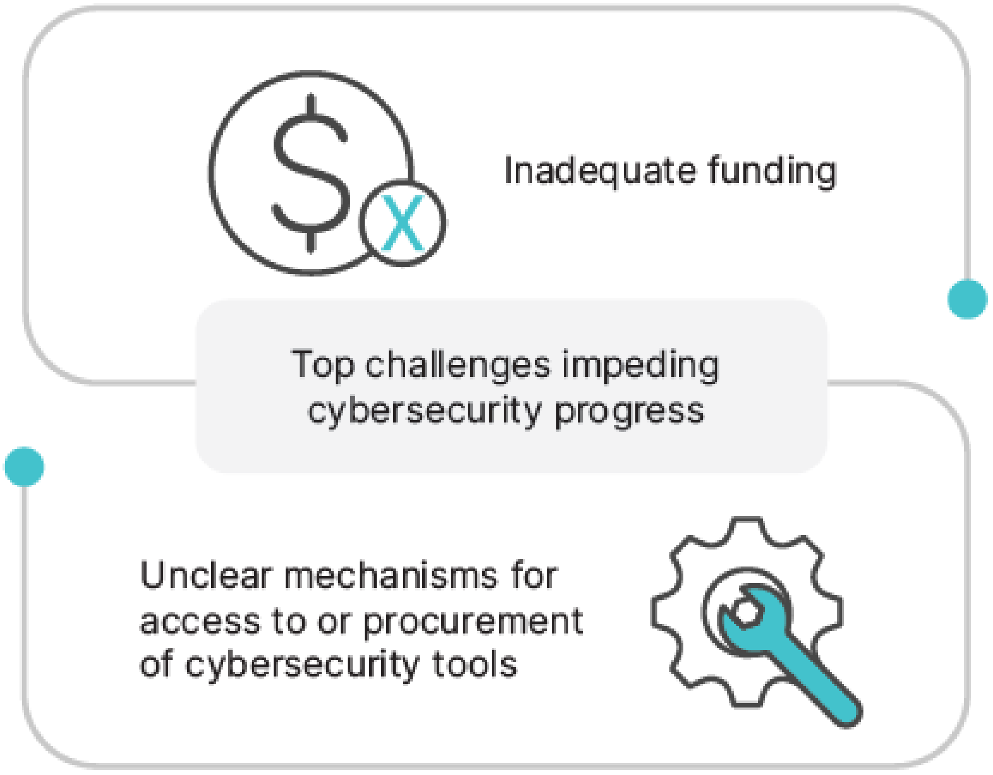
1 INCREASE IN CYBERATTACKS



33%

Of respondents reported **at least one** cyberattack in the last 12 months.

2 TOP CHALLENGES IMPEDING CYBERSECURITY PROGRESS



Inadequate funding

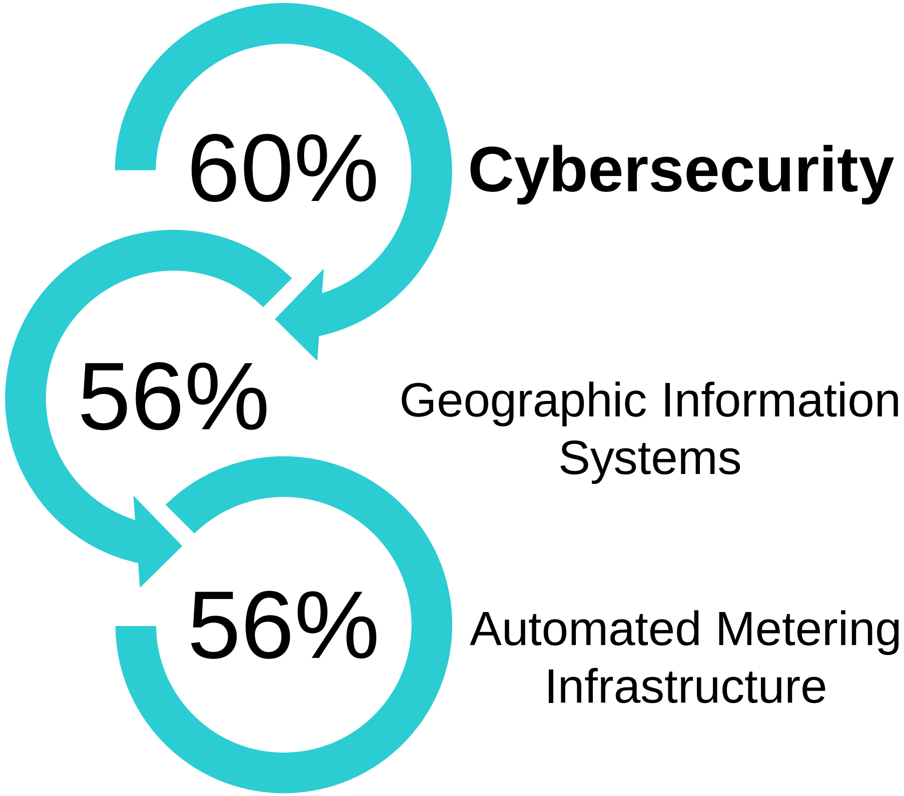
Top challenges impeding cybersecurity progress

Unclear mechanisms for access to or procurement of cybersecurity tools

Cybersecurity in Water Management Facilities

Research Findings, cont.

3 PLANNED INVESTMENTS OVER NEXT 24 MO.

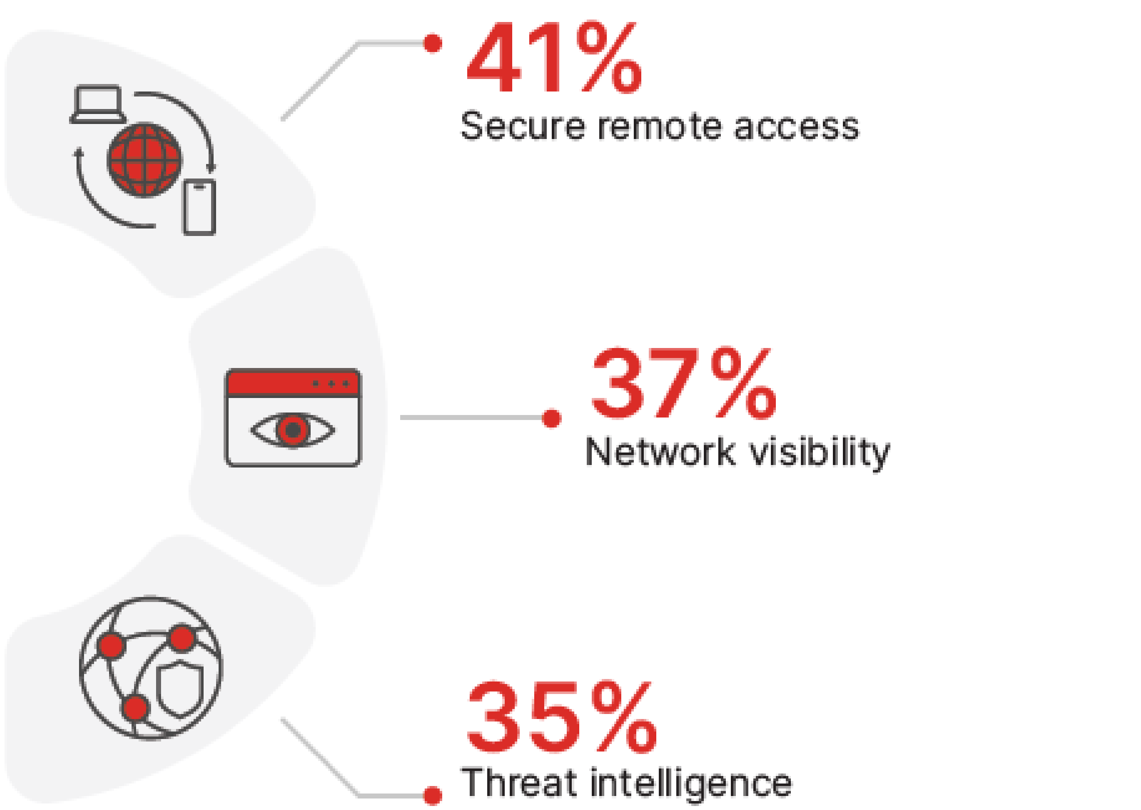


60% **Cybersecurity**

56% Geographic Information Systems

56% Automated Metering Infrastructure

4 CYBERSECURITY PRIORITIES NEXT 12 MO.



41% Secure remote access

37% Network visibility

35% Threat intelligence

Cybersecurity in Water Management Facilities

5 MATURING AND ADOPTING CYBERSECURITY MEASURES

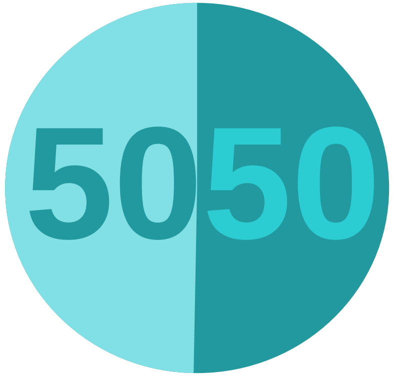
20%
Visibility and Segmentation established

50%
Access control established

Water Utilities maturing cybersecurity measures.

13%
Predictive behavior established

4%
Leveraging orchestration and automation



Of respondents believe increased regulations and compliance will impact water / wastewater utilities within 2-5 years.

How can Fortinet help?

2023

Leader

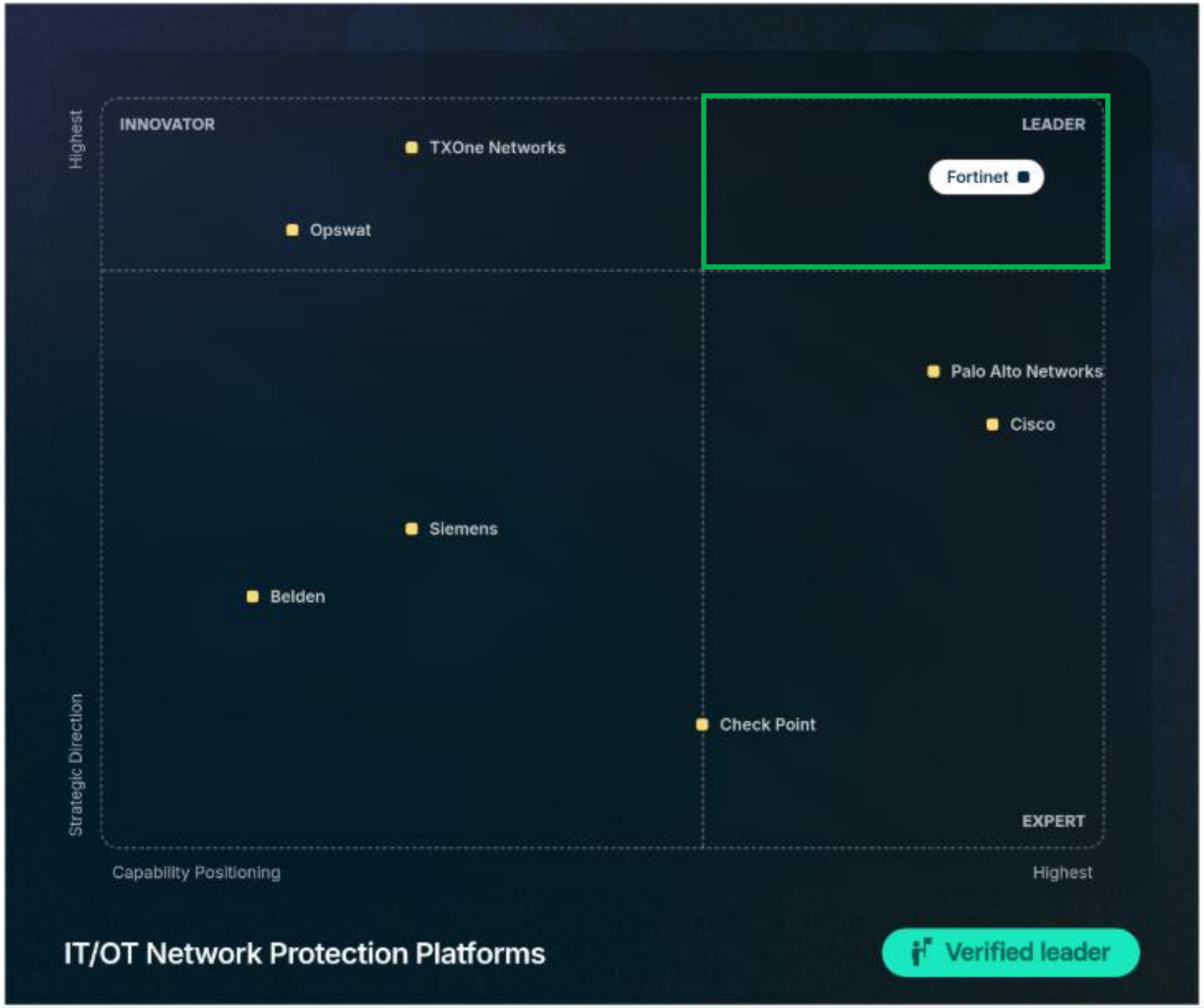
IT/OT Network Protection Platforms

Fortinet

IRWA

ILLINOIS RURAL WATER ASSOCIATION

IT/OT Network Protection Platforms



Fortinet is one of the largest cybersecurity companies in the world.

Founded: **October 2000**

Founded by: **Ken Xie and Michael Xie**

Headquarters: **Sunnyvale, CA**

Fortinet IPO (FTNT): **November 2009**

Listed in both: **NASDAQ 100 and S&P 500 Indices**

Member of: **2023 Dow Jones Sustainability World and North America Indices**

Global Customer Base
830K+
Customers

>50%
Global Firewall Shipments

2024 Billings
$6.5B+
(as of Dec. 31, 2023)

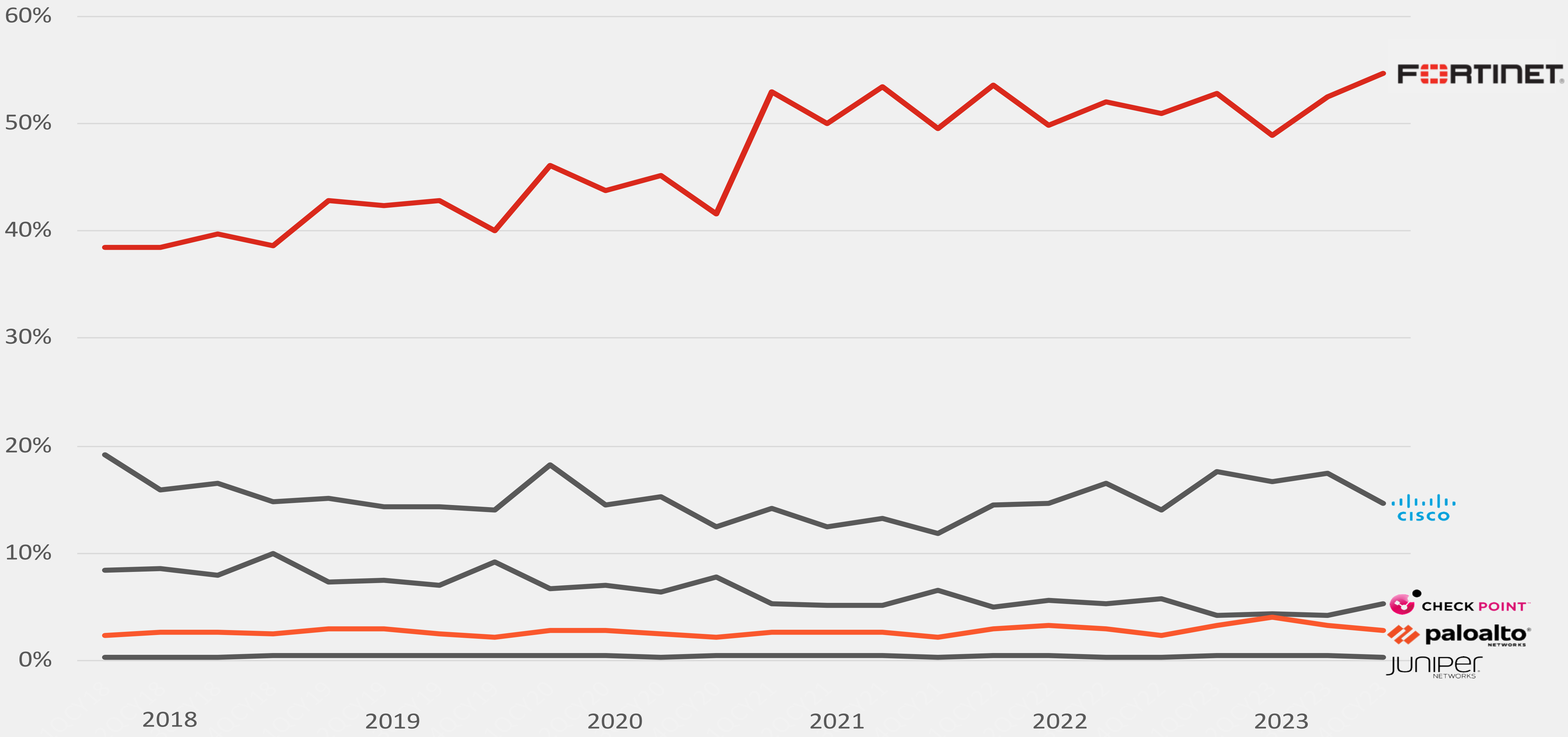
~$2.5B+
Investment in Innovation since 2017, with 91% R&D
(as of Dec. 31, 2023)

Market Capitalization
$85.5B
(as of Feb. 14th , 2025)

Security Investment Grade Rating:
BBB+ Baa1

The Most Trusted Security Vendor for Network Firewalls

More than 50% of all firewalls shipped worldwide are FortiGate NGFWs



Source: 650 Group, March 2024

564 West Randolph Street

Investing in Illinois

Building Size
102,700 sq. ft. gross, 93,700 sq. ft. usable
(28% is leased)

Purchase Price
$20.8M (February 1, 2022)

Renovation costs
~$10M

Total Fortinet investment
+$33M

Head Count Capacity
Fortinet’s used portion of building: 137
Current Chicago Headcount: 57

Breakdown of Chicago Jobs
40% R&D, 45% Sales

Chicago Job Growth
Grown jobs by over 70% since 2021

Chicago Job Openings
Roles in Sales and R&D

Free Educational Services for IL

Academic Partner Program

- **Academic Partner Program**
  - Free Curriculum for all Uni, College, & Tech Schools
  - Free Hosted Lab access
  - Free products in VM format and on line
  - Free certifications for all students

- **K-12 Free Cybersecurity Awareness Training**
  - Customized for School Districts
  - Age-specific content modules
  - Included administration and Management
  - Active Monitoring and Reporting
  - Certificate of Completion

- **Water/Wastewater Cyber Awareness Training**
  - Providing Cyber Awareness training statewide via the IRWA
  - Free Threat Assessment Service offered to Industrial environments

Amazing Customers

"If I am looking for a particular device, one search turns it up. And the ability to manage the switches remotely is a huge efficiency benefit, which is crucial since we have 26 locations and only one network engineer." – Bill Sadlick

The result is a substantially lower total cost of ownership for the network. "With our previous vendor, the total cost of ownership amounted to $5 million over five years," Pegues says. **"We have successfully achieved cost savings and avoidance totaling millions of dollars."**

FORTINET

CASE STUDY

It Takes a Village: How Fortinet Helps Keep the Village of Schaumburg Secure

Located 30 miles northwest of Chicago and 11 miles west of O'Hare International Airport, the Village of Schaumburg bills itself as the "premier suburban business destination in Illinois." Over the past several decades, Schaumburg has transformed from a small farming community into a thriving economic center that houses more businesses than any other Illinois community except Chicago. The village also prides itself on the Woodfield Mall, which was once the nation's largest shopping center.

The Schaumburg village government supports residents and businesses using many of the same services as other municipalities. "Our core solutions include ERPs [enterprise resource planning systems], permitting systems, payment systems, and water billings systems," says Chris Westgor, technical services manager. "We have OT systems in our utility division. We also own a hotel, airport, and ballpark. We help manage the train station and run community facilities such as a teen center and senior center."

All told, the village government has 26 locations. Protecting those sites from cyberattack falls to Westgor and Network Administrator William Sadlick. "A cyberattack or data breach could cause massive challenges," Sadlick says. "Our service to village residents could certainly be impacted. Even water delivery might be affected by a successful attack."

VILLAGE OF SCHAUMBURG
PROGRESS THROUGH THOUGHTFUL PLANNING

"The Fortinet solutions have improved security throughout the village by enabling us to monitor things more closely and find issues more quickly. We have a better understanding of potential vulnerabilities, and we can respond and remediate issues much faster than ever before."

Chris Westgor
Technical Services Manager,
Village of Schaumburg

FORTINET

CASE STUDY

How Fortinet Saved the Second-Largest City in Illinois Millions of Dollars on Networking and Security

Located about 41 miles west of Chicago, Aurora is the second-largest city in Illinois, "But I would say we are second to none," proclaims Michael Pegues, Aurora's Chief Information Officer. The city has a long history as an industrial hub, home to companies such as Caterpillar and Burlington Northern. It is known as the "City of Lights" because it was one of the first cities in the United States to install electric streetlights.

Recently, Aurora has gained recognition as a pivotal technology hub within the Illinois Technology and Research Corridor, largely due to the proliferation of data centers.

When Mayor Richard Irvin was elected in 2017, he welcomed Pegues back home. An Aurora native, Pegues had been working abroad in IT and cybersecurity for Fortune 500 companies for decades. "Mayor Irvin said, 'I want you to transform the city of Aurora in terms of innovation and technology,'" he reports. "The three pillars of his government are public safety, education, and economic development. He wanted technology to be the foundation underpinning all three of those main pillars, and

AURORA
CITY OF LIGHTS

"In my experience, the big difference between Fortinet and its competitors is that Fortinet streamlines network management. Fortinet solutions are very efficient to manage because the interfaces are easy to use."

Keith Wouk
Director of IT Operations,
City of Aurora

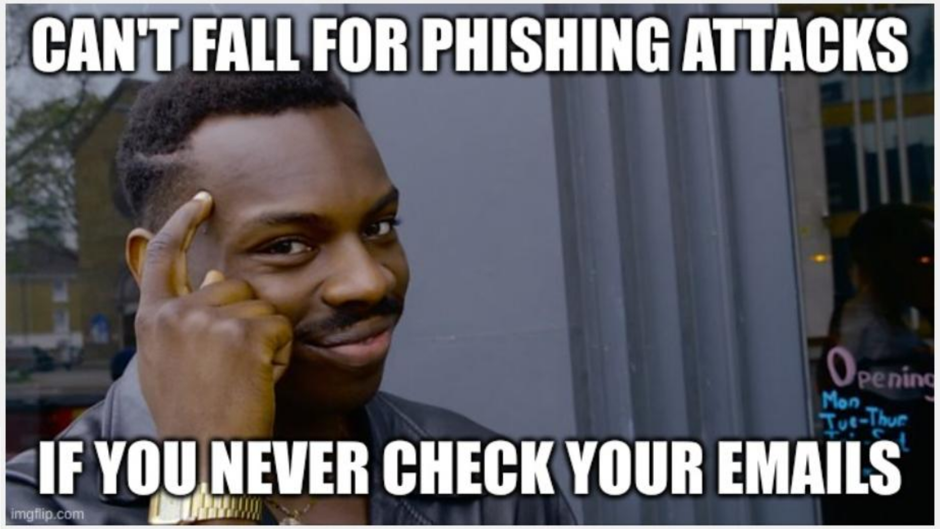
How are Hackers Gaining Access to your Network?

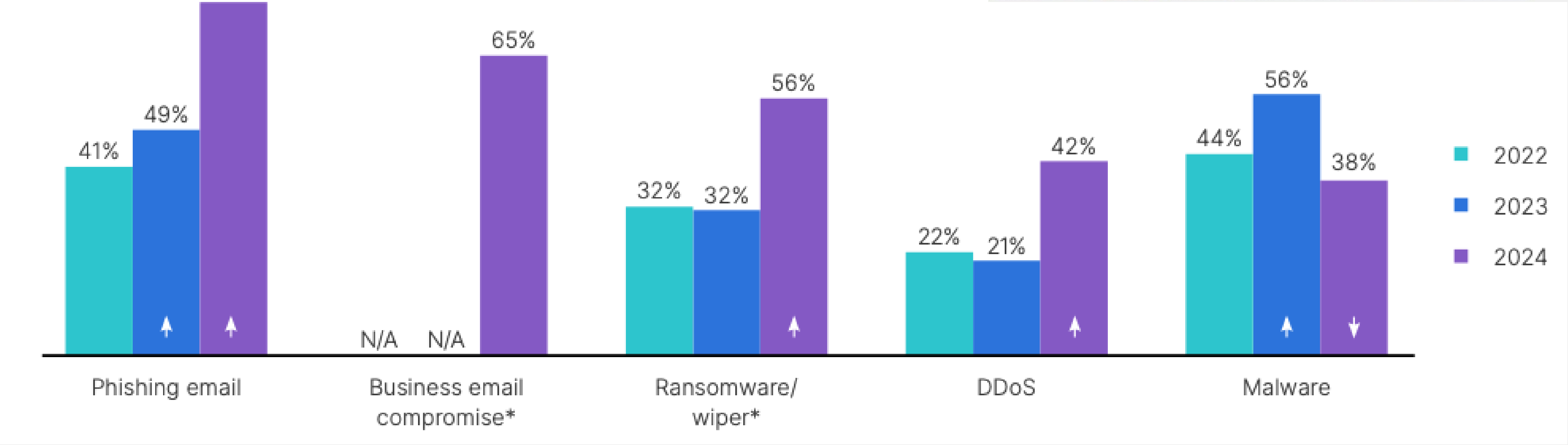
Common Challenges

Cyber Threat Categories

- Social Engineering
- Malicious Software
- Unauthorized Access to physical places or systems
- System Design Failure

What types of intrusions are most common in OT?


CAN'T FALL FOR PHISHING ATTACKS
IF YOU NEVER CHECK YOUR EMAILS
imgflip.com



Phishing

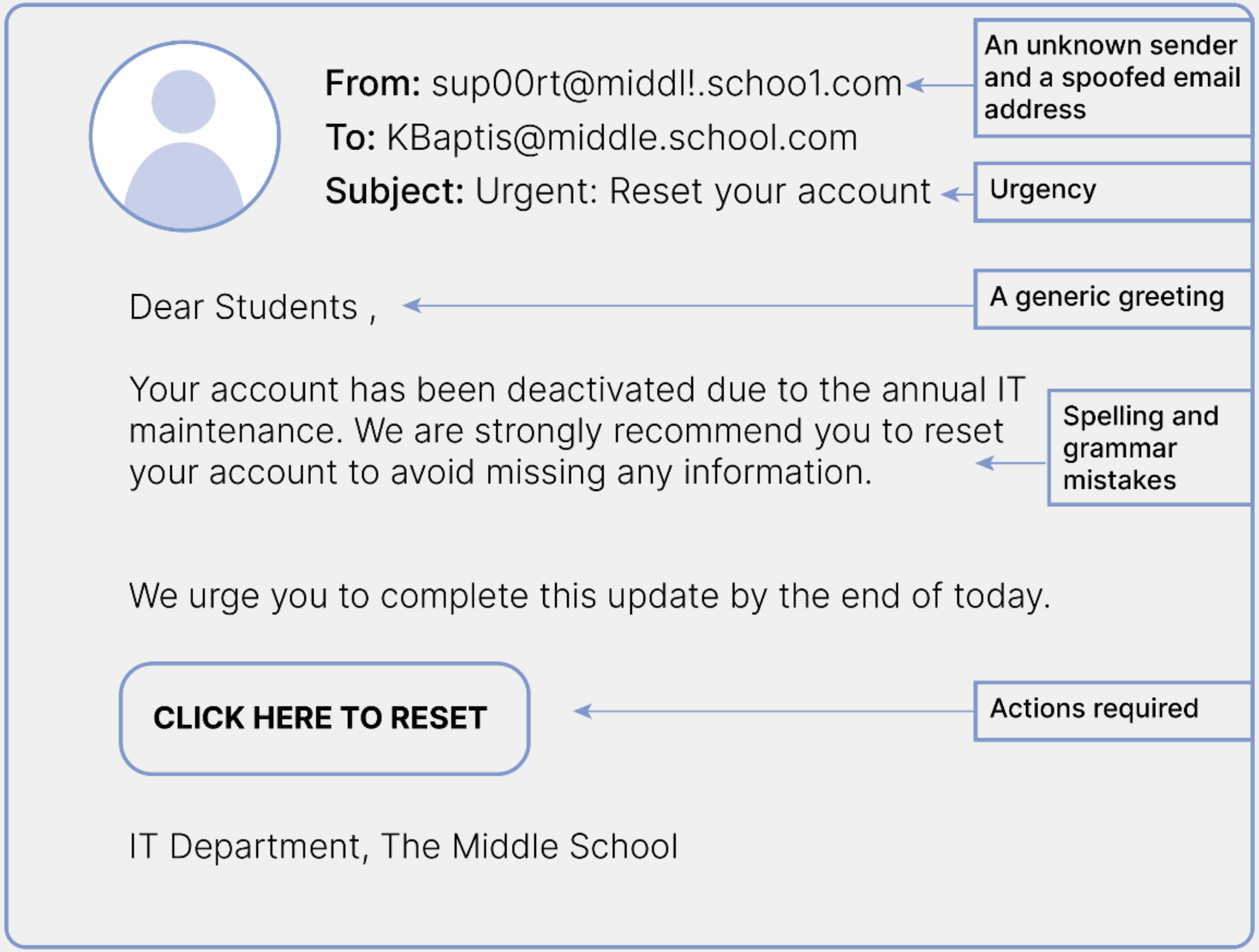
- One of the most common attack vectors
- 9 out of 10 cyber attacks are launched using phishing emails
- Game of numbers for bad actors. They send out thousands of emails
- Statistically 1 in 20 people will fall for a phishing email.
- It only takes 1 and then malware can be deployed into the network
- Can be manipulative and very real looking

© Fortinet Inc. All Rights Reserved.

How to spot a phishing email

- AI has made phishing attacks even harder to spot
- Personalization has become easier with information about you available online
- Is the message trying to get you to feel fear urgency or excitement
- Is the message trying to get you to take action by clicking a link, entering information, or opening an attachment?
- Do you know the sender, does it seem weird that they sent you this message?
- Were you expecting this message or was this request out of the blue?
- Bad writing, spelling, or grammar?
- Does the message ask for payment or money transfer?

Answers



From: sup00rt@middl!.schoo1.com

To: KBaptis@middle.school.com

Subject: Urgent: Reset your account

Dear Students ,

Your account has been deactivated due to the annual IT maintenance. We are strongly recommend you to reset your account to avoid missing any information.

We urge you to complete this update by the end of today.

CLICK HERE TO RESET

IT Department, The Middle School

An unknown sender and a spoofed email address

Urgency

A generic greeting

Spelling and grammar mistakes

Actions required

Malware

- Malicious Software
  - Program that runs on your devices and is meant to cause you harm
  - Spy on your activities
  - Expose your data
  - Trick you into giving away private information
  - Disrupt how your devices work
  - Spread to other devices

- Types of Malware - **350K new variants discovered every day!**
  - Trojan aka – Troy Trojan horse used by the Greeks. Installing a backdoor
  - Spyware gain info on you to steal/sell, or use to access your accounts
  - Worm – Make copies of itself and spreading to other devices
  - Ransomware – Encrypts your data and requests $ to unlock

Reminders! How to avoid phishing & malware

- Be smart and stay cautious online
- Don’t click suspicious links
- Have AV installed
- Practice good password hygiene
  - All accounts use strong unique passwords
- Use VPN on public wifi
- Backup critical data & have a 3rd copy off site

FORTINET

Best Practices for Securing SCADA Systems

Case Studies

Basic Principles of the Cybersecurity Solution

Protect Users

Security at the Edge to protect and secure all the infrastructure that runs the system from back office to laptops, SCADA and operators

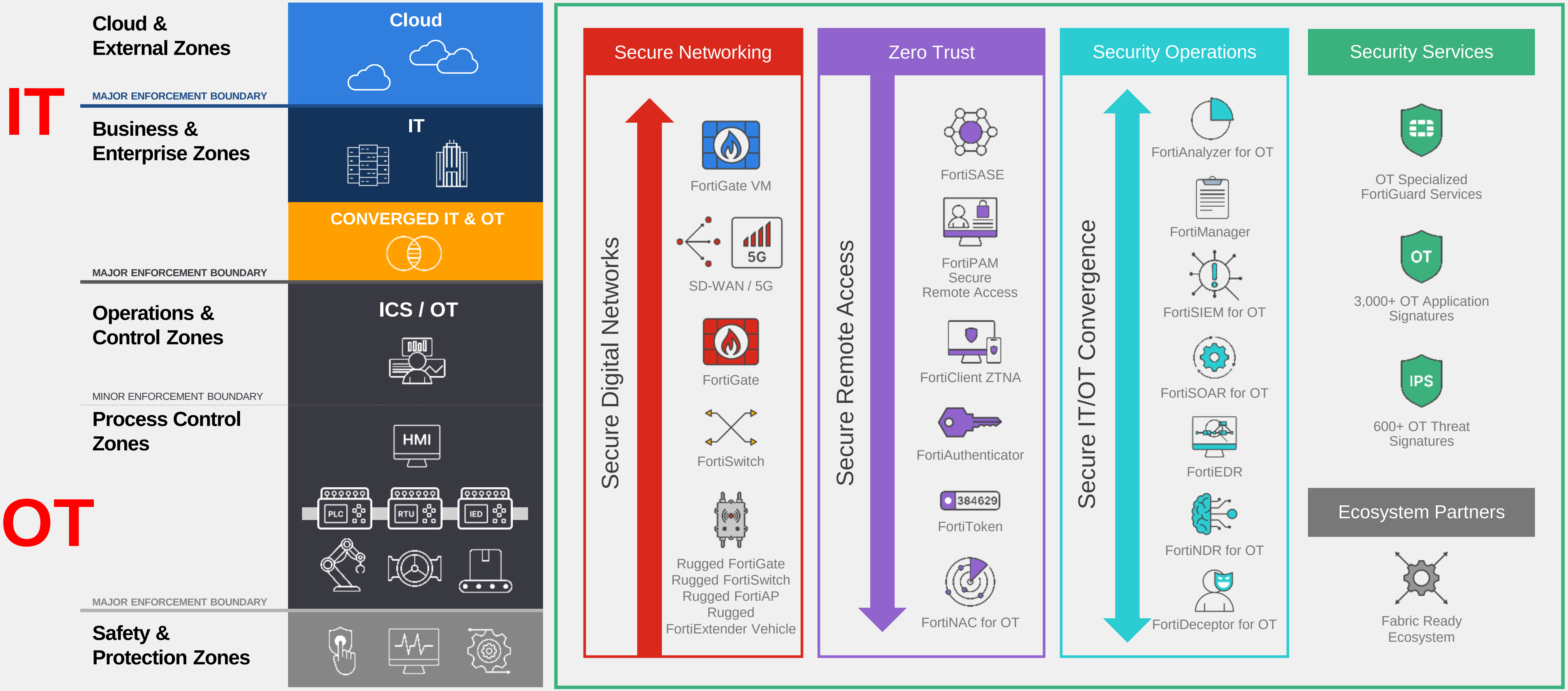
Protect the Network

Protect and secure all communication equipment from sensors to PLCs

Protect the Servers

Protect and secure everything that serves employees and facilities

OT Security Platform



IT

Cloud & External Zones

Cloud

MAJOR ENFORCEMENT BOUNDARY

Business & Enterprise Zones

IT

CONVERGED IT & OT

MAJOR ENFORCEMENT BOUNDARY

Operations & Control Zones

ICS / OT

MINOR ENFORCEMENT BOUNDARY

Process Control Zones

HMI

PLC RTU IED

OT

MAJOR ENFORCEMENT BOUNDARY

Safety & Protection Zones

Secure Networking

Secure Digital Networks

- FortiGate VM
- SD-WAN / 5G
- FortiGate
- FortiSwitch
- Rugged FortiGate
Rugged FortiSwitch
Rugged FortiAP
Rugged FortiExtender Vehicle

Zero Trust

Secure Remote Access

- FortiSASE
- FortiPAM Secure Remote Access
- FortiClient ZTNA
- FortiAuthenticator
- FortiToken
- FortiNAC for OT

Security Operations

Secure IT/OT Convergence

- FortiAnalyzer for OT
- FortiManager
- FortiSIEM for OT
- FortiSOAR for OT
- FortiEDR
- FortiNDR for OT
- FortiDeceptor for OT

Security Services

- OT Specialized FortiGuard Services
- 3,000+ OT Application Signatures
- 600+ OT Threat Signatures

Ecosystem Partners

- Fabric Ready Ecosystem

Recommended Best Practices for OT

Segmentation

Visibility & Compensating Controls

Security Operations Center & IR

Platform Approach

OT Threat Intelligence

Safeguarding OT

Specialized OT Solutions and Teams

Specialized Solutions

FortiGate Rugged

FortiSwitch Rugged

FortiAP IP-rated

Industrial-grade firewalls, switches and APs

Most deployed IT/OT next-gen firewall worldwide

OT-specific SIEM, EDR, Sandbox, and Deception capabilities

Specialized Threat Information

DPI for 70+ OT protocols

Up to payload level visibility and control

Vulnerability shielding for OT assets

More IPS signatures than any other cybersecurity vendor

Specialized Talent

Industry validated and referenced solutions

Experienced OT professionals

Specialized OT integrators

1000+ professional services engineers

Specialized Ecosystem

Extensive solution integration platform

500+ Security Fabric ecosystem integrations

Out-of-the-box integrations with leading OT security solutions

OT Ecosystem: +370 Partners, +700 Integrations and Growing

Best-in-class integrated solutions for comprehensive protection

FORTINET FABRIC-READY

OT TECHNOLOGY PARTNERS

Visibility and Threat Intelligence

DRAGOS
NOZOMI NETWORKS
CLAROTY
ARMIS
ordr
np network perception
CYBERX BATTLE-TESTED INDUSTRIAL CYBERSECURITY
SCADAfence
INDUSTRIAL DEFENDER
tenable

Security Operations Management

OTORIO
splunk>
tdi technologies
rubrik
BACKBOX
SKYBOX SECURITY
servicenow.

Other

SIEMENS RUGGEDCOM
FORESCOUT
OWL Cyber Defense
radiflow
HIGHWAY 9 NETWORKS
DARKTRACE
RAD

SOLUTION VENDORS AND SYSTEMS INTEGRATORS

Industrial Control System Vendors

Schneider Electric
ABB
SIEMENS Ingenuity for life
GE
Rockwell Automation
Honeywell
EMERSON
SEL SCHWEITZER ENGINEERING LABORATORIES
HIRSCHMANN A BELDEN BRAND
YOKOGAWA
SAMSUNG SAMSUNG HEAVY INDUSTRIES
HITACHI

Global System Integrators

Hewlett Packard Enterprise
IBM
Capgemini CONSULTING. TECHNOLOGY. OUTSOURCING
Orange Cyberdefense
HCL
Atos
NTT
accenture

Other

Baker Hughes
T · · Systems ·
Johnson Controls
Eleven Paths A Telefonica COMPANY
World Wide Technology, Inc.

OT Security Focus Areas

Best Practices to Guide Strategy

Asset Management

- Include offsite or remote devices
- Discover and profile OT devices
- Identify high and critical vulnerabilities (Virtual Patching)
- OT Protocol visibility (Modbus, DNP3, Ethernet IP)

OT Network Segmentation

- Enabled secure communications through DMZ
- North-South network traffic monitoring and threat inspection (Inter VLAN)
- East-West traffic monitoring (intra VLAN inspect

Endpoint Security

- Endpoint Detection & Response Solution
- Malware and Viruses Detection
- OT Application Whitelisting (Historian, SCADA, HMI)
- Integration with Incident Response
- Support Legacy & Modern Operating Systems (XP)

Secure Remote Access

- Enable MFA and Role Based Access Control
- Provide access to required devices only
- Session Management (Start/Stop), MFA, Password Management, session recording and secure file transfer

Virtual Patching / Vulnerability Shielding

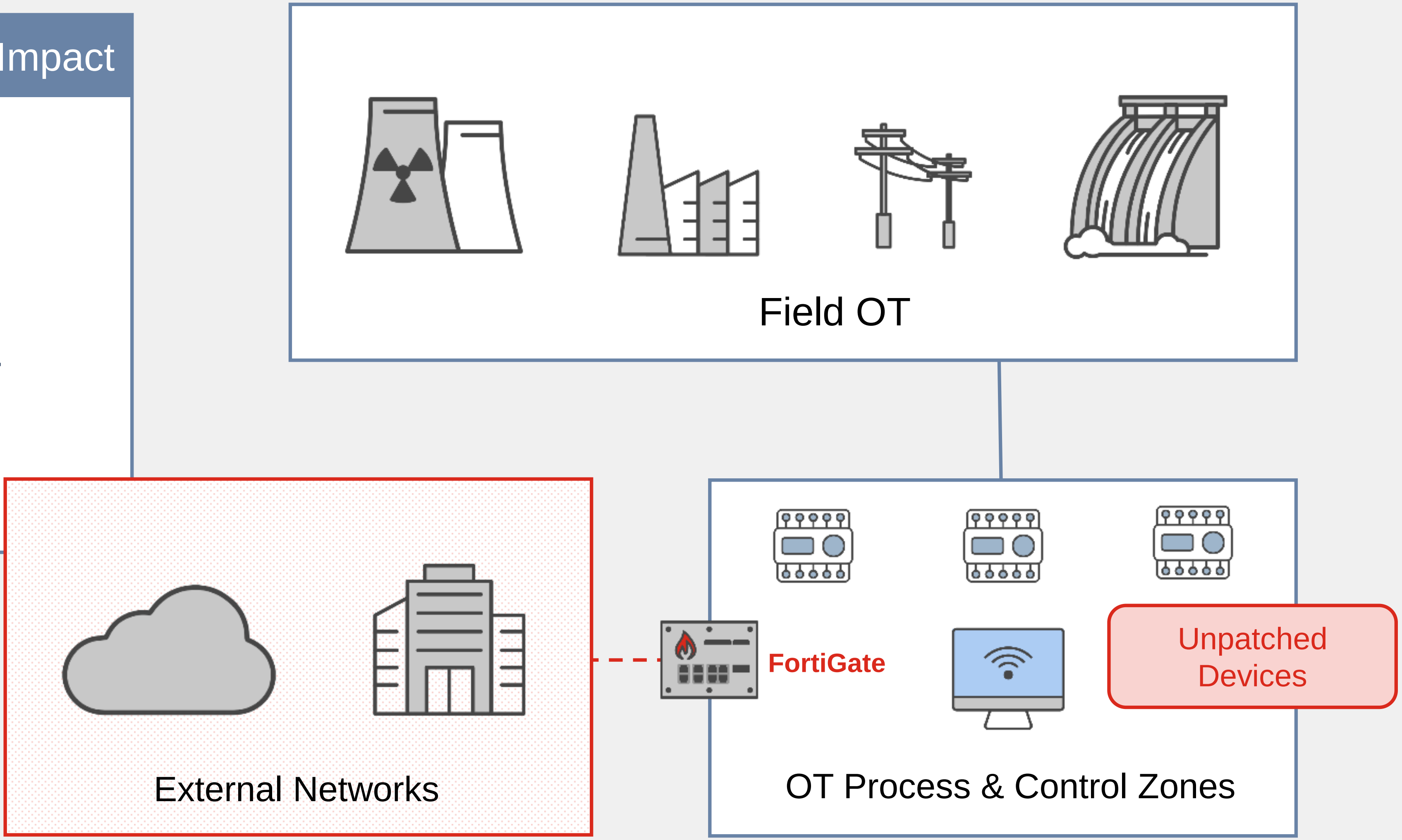
Protect Legacy Devices without Impact

Detect OT/IoT Network Assets

Query for vulnerabilities

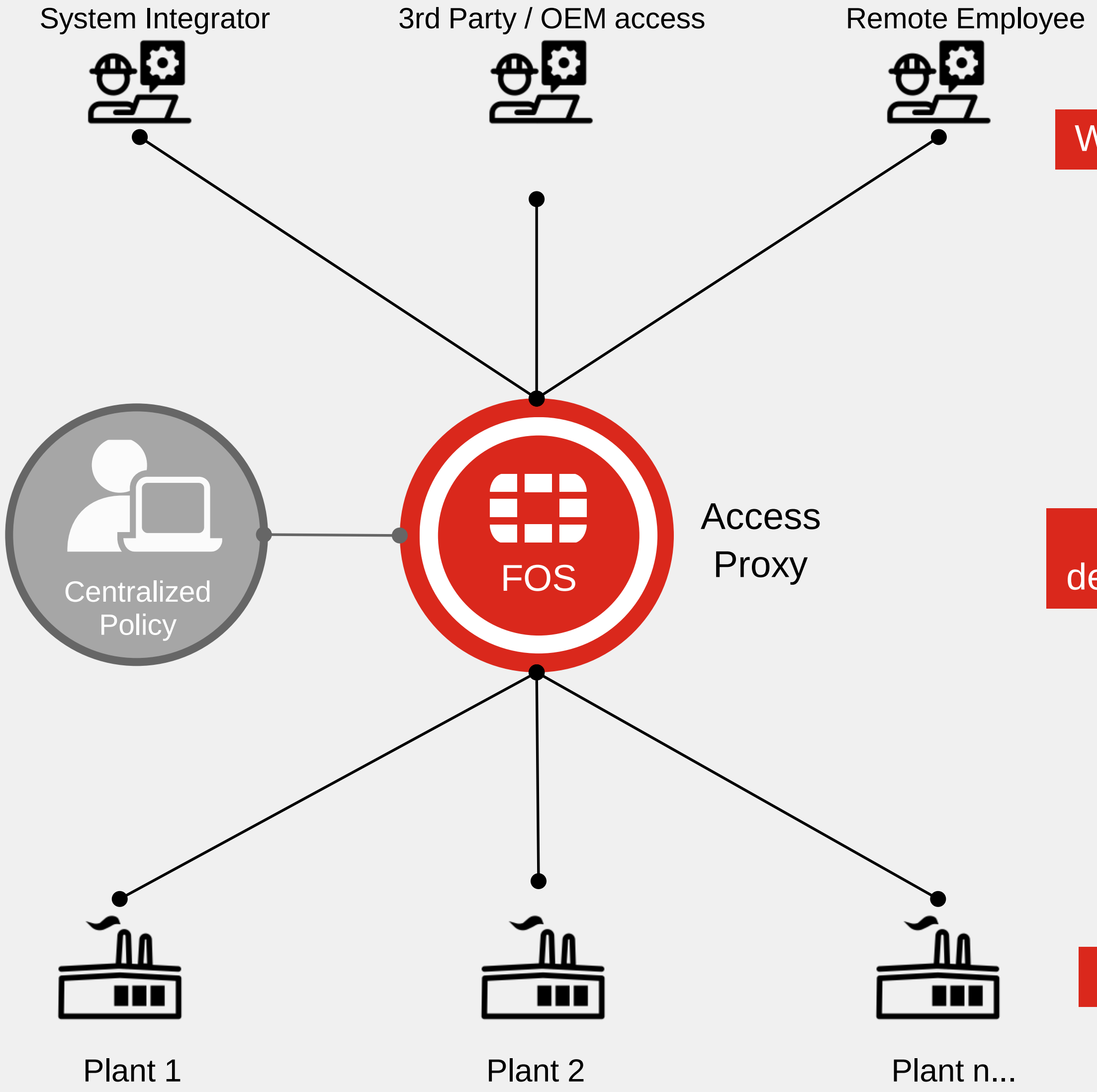
Populate FOS Asset Identity Center

Deploy Virtual Patching



Secure Remote Access

- **Session Management** (Start/Stop), MFA, Password Management, **session recording**, etc
- **Role based** access and least privilege. Provide access (read/write) to **only target devices**
- Remote users require different **level of Access** to run specialized tools (e.g. Web based and thick clients). HTTPS, VNC, SSH, etc
- Require **File Transfer** capabilities (e.g. firmware upgrades, config / programing, compliance reports, diagnostics, etc)
- User friendly and **immediate access** (seconds not minutes)



Wherever the user is located

Verified user identity and device posture prior to access

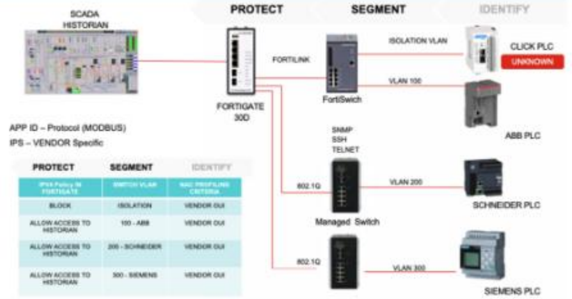
Industrial asset location

Network Segmentation and Micro-segmentation 1

- □ Segmentation provides important security controls for your network using FortiGates, FortiSwitches, and FortiAPs
- □ Integrations with leading OT IDS and other technology vendors
- □ DIN rail, DEC powered version
- □ Transparent mode, HA fail-over, bypass ports
- □ (The only) Ruggedized SD-WAN NGFW
- □ Centralized switch / AP management with NAC integration

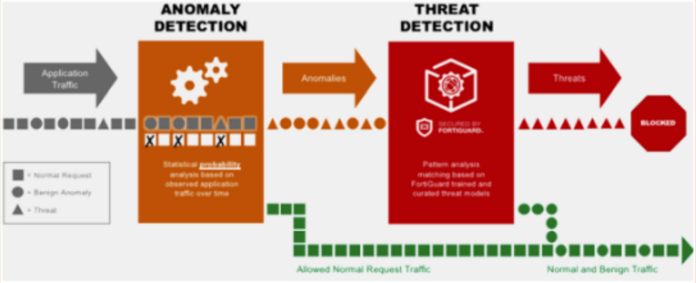
Network Access Control - FortiNAC 2

- □ Detect, identify, and profile devices as they connect to the network
- □ Apply network access control policies to the devices on the network
- □ Alert and notify network access control policy violations
- □ Automate remediation actions for policy violations
- □ Network device classification per location in Purdue Levels
- □ Access policies can be applied based on Purdue Levels
- □ Multi-vendor device support

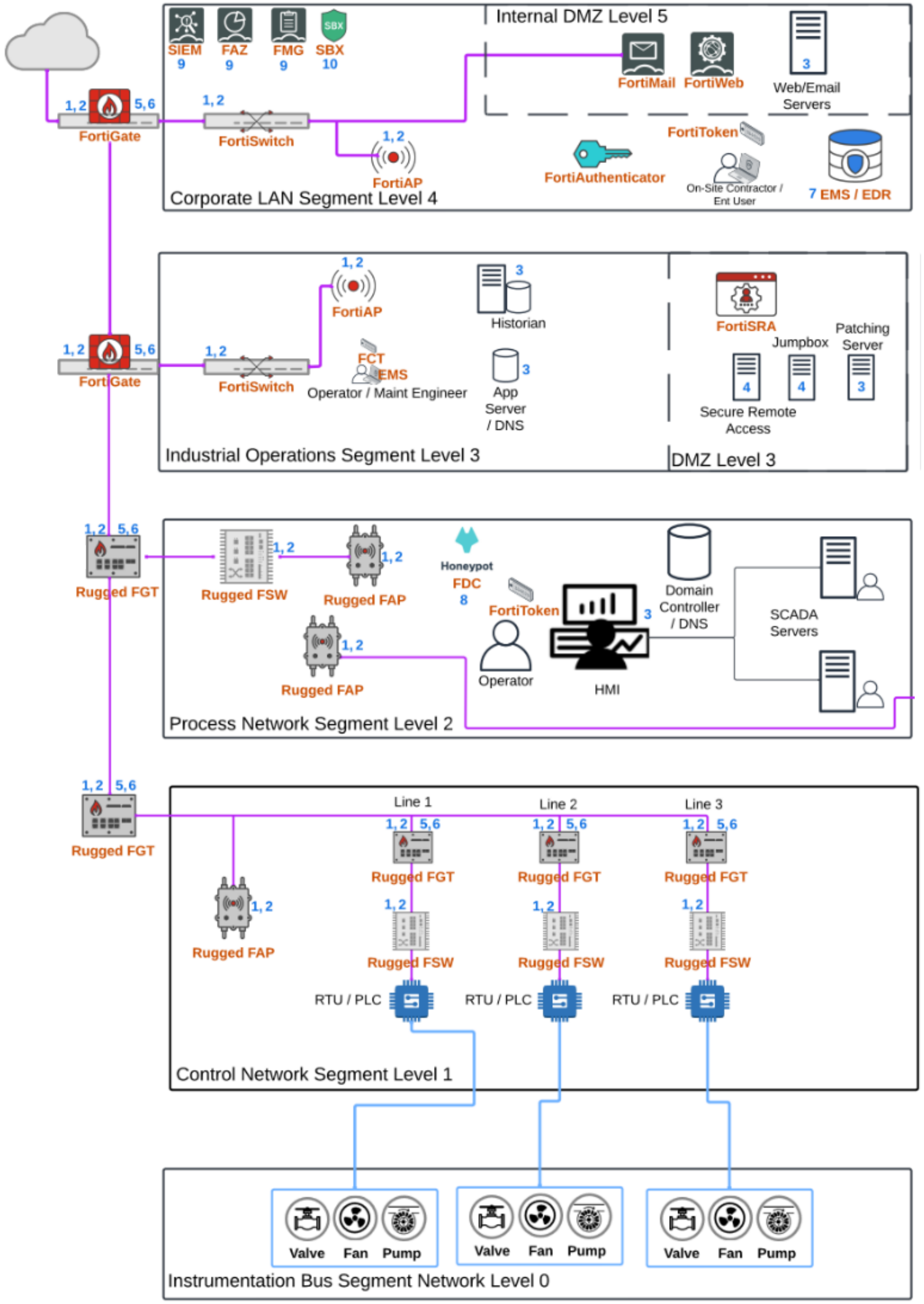


Web Server Protection - FortiWeb 3

- □ Secure web-based HMIs and Historians
- □ Apply web application and API security
- □ Identify and block malicious web application attacks
- □ Prevent web services from exploitation
- □ Protects against OWASP top 10 threats (SQL injections, XSS, CSRF, etc)
- □ DDoS mitigation, Bot management, DLP, Virtual Patching

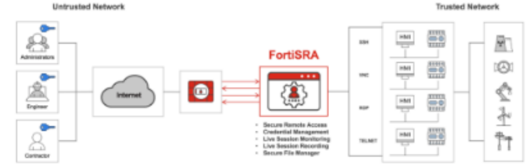


ANOMALY DETECTION
THREAT DETECTION
Application Traffic
Anomalies
Threats
BLOCKED
■ = Normal Request
● = Benign Anomaly
▲ = Threat
Statistical probability analysis based on observed application traffic over time
SECURED BY FORTIGUARD.
Pattern analysis matching based on FortiGuard trained and curated threat models
Allowed Normal Request Traffic
Normal and Benign Traffic



Secure Remote Access - FortiClient and FortiSRA 4

- □ FortiClient VPN client with MFA support
- □ FortiClient monitors and protects endpoints
- □ Endpoint telemetry, vulnerability management
- □ Malware prevention
- □ Web and application filtering
- □ FortiAuthenticator authenticates users with MFA including PKE and OTP
- □ FortiSRA - Agent-less secure remote access w/ session recording
- □ ZTNA - Change remote access to explicitly allow application access



Threat Protection and AI 5

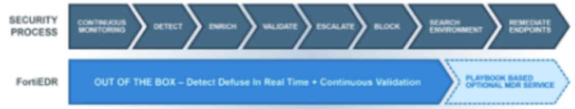
- □ Detect known malware and intrusion attempts
- □ Monitor, block or quarantine actions when policy violation or malicious traffic is detected
- □ 400+ IPS signatures for OT applications and protocols
- □ IPS/ Virtual Patching for OT - 7 technologies, RSLogix, Siemens, Eaton, GE, Broadwin, Rockwell Automation, MOXA, IntelliCom, Sunway, TeeChart, VxWorks, Wellintech, Yokogawa, etc....

Application Control 6

- □ 1,800+ application control signatures for OT protocols
- □ 3,900+ total application control signatures for IT
- □ Deep packet inspection for 50+ OT protocols
- □ Granular options for application monitoring and control
- □ OT protocols and Applications - ADDP, BACnet, CIP, CN.IP, DNP3, Elcom, EtherCat, EtherNET/IP, TriStation, Heart, IEC, Modbus, MMS, ICCP, OPC, etc....

Endpoint Protection - fortiEDR + FortiClient EMS 7

- □ EDR for critical systems
- □ Compatible with legacy OS
- □ Air-gapped on-premises options
- □ Block external devices like USB sticks
- □ Allow / deny applications and communication paths

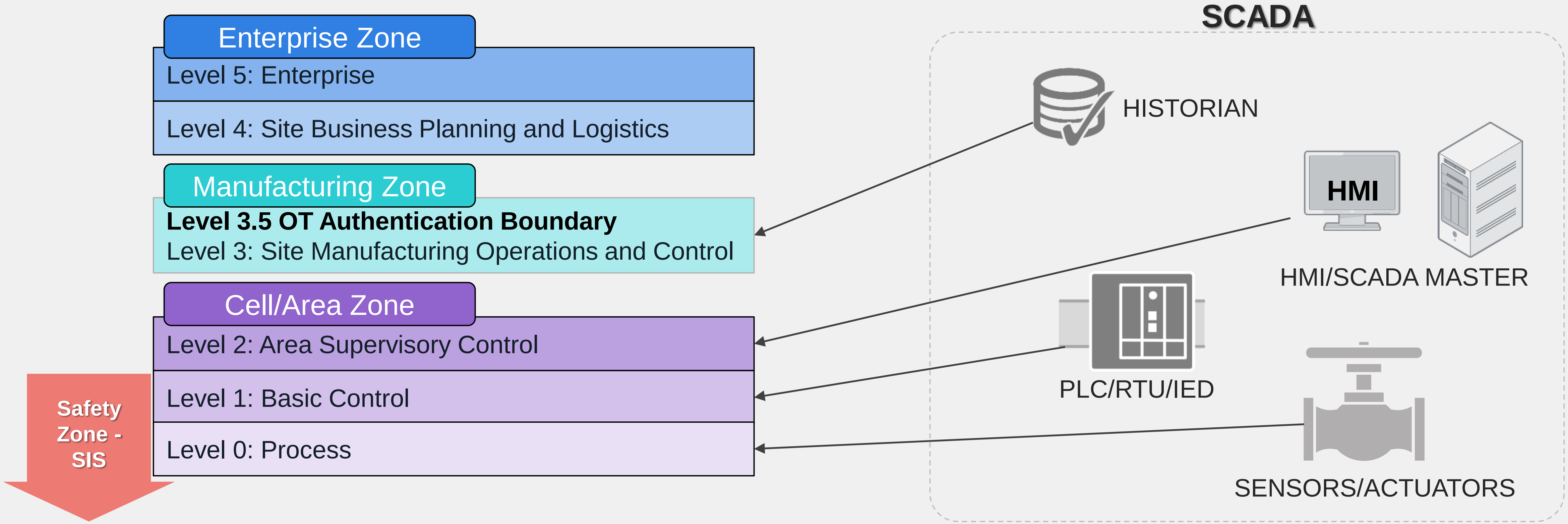


Honeypot - FortiDeceptor 8

- □ Mimic servers such as Jumpboxes and VPN services for OT & IT
- □ Mimic OT assets such as HMIs, PLCs, and OT protocols
- □ Integrations into FGT and FortiSIEM and security fabric
- □ Decoy supported protocols - MODBUS, S7COMM, BACNET, IPMI, TRICONEX, GUARDIAN-AST, IEC104, DNP3, Trinix, HTTPS, FTP, TFTP, SNMP, etc....

Purdue Model For Industrial Control Hierarchy

- Industry standard framework for OT cybersecurity
- Segment OT assets into security zones and conduits
- Increasing Security Levels to enhance security posture
- Validated Security Controls for protecting OT assets



Enterprise Zone

Level 5: Enterprise

Level 4: Site Business Planning and Logistics

Manufacturing Zone

Level 3.5 OT Authentication Boundary

Level 3: Site Manufacturing Operations and Control

Cell/Area Zone

Level 2: Area Supervisory Control

Level 1: Basic Control

Level 0: Process

Safety Zone - SIS

SCADA

HISTORIAN

HMI

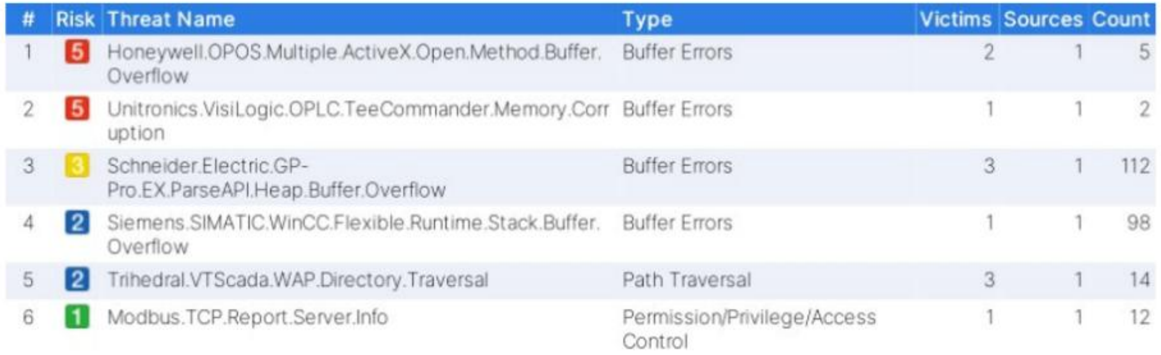
HMI/SCADA MASTER

PLC/RTU/IED

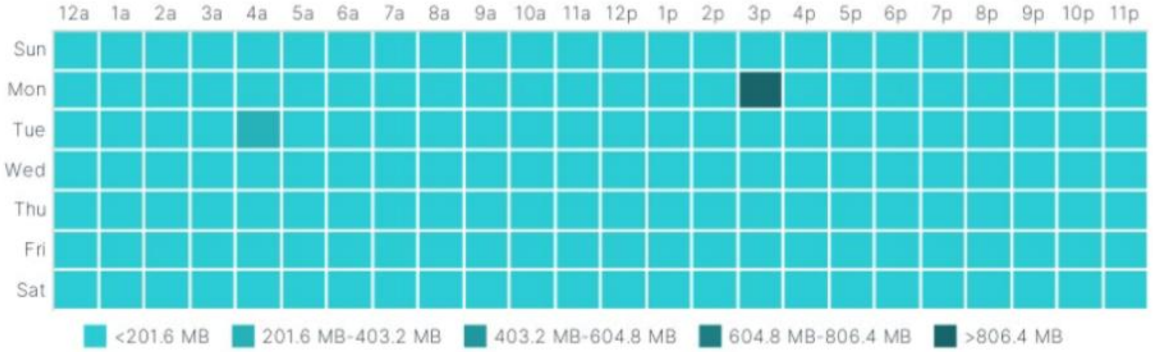
SENSORS/ACTUATORS

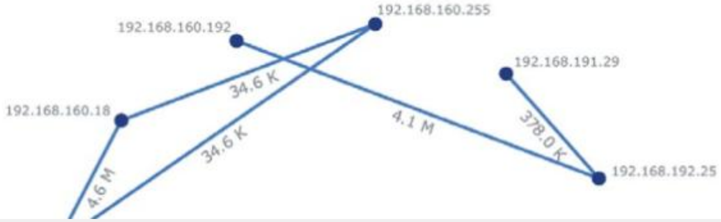
Free Cyber Operational Technologies Threat Assessment

- **Security and Threat Prevention** – How effective is your current network security solution? Learn more about application vulnerabilities are attacking your network, which malware/botnets were detected and even pinpoint “at risk” devices within your network. Make sure your existing security solution isn’t letting anything slip through the cracks by leveraging FortiGuard Labs’ award-winning content security.
- **OT/IT Application Usage** – What steps are you taking to monitor traffic flows in your network? Improve your visibility to traffic and most used applications within your OT environment. Monitor traffic patterns to identify network anomalies whether accessing on-site or via remote access.
- **Network Utilization and Performance** – How should your network security solution be optimized for performance? Find out more about your throughput, session and bandwidth requirements during peak hours. Ensure your security solution is sized and optimized properly based on your actual usage.

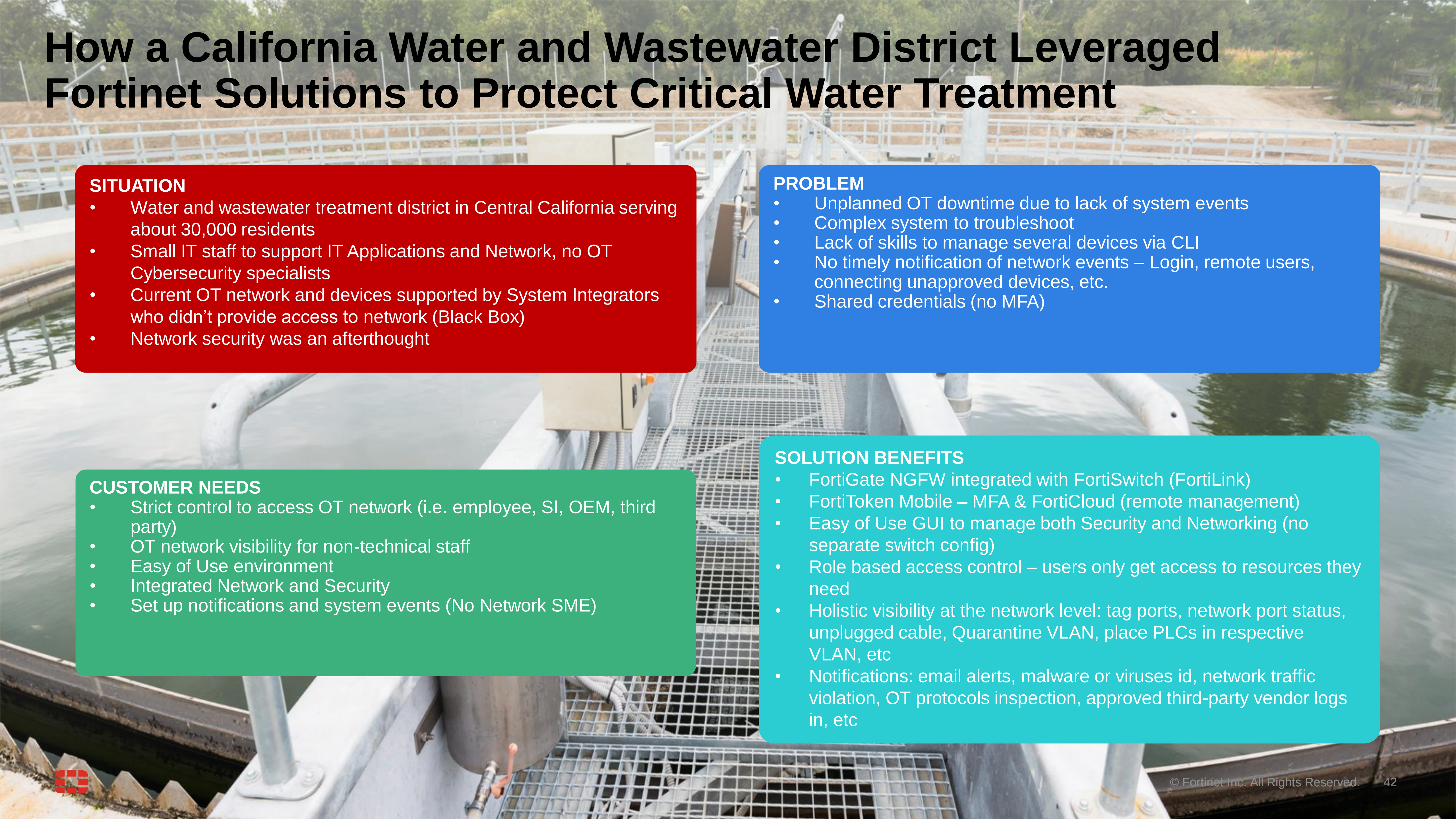


#	Risk	Threat Name	Type	Victims	Sources	Count
1	5	Honeywell.OPOS.Multiple.ActiveX.Open.Method.Buffer.Overflow	Buffer Errors	2	1	5
2	5	Unitronics.VisiLogic.OPLC.TeeCommander.Memory.Corruption	Buffer Errors	1	1	2
3	3	Schneider.Electric.GP-Pro.EX.ParseAPI.Heap.Buffer.Overflow	Buffer Errors	3	1	112
4	2	Siemens.SIMATIC.WinCC.Flexible.Runtime.Stack.Buffer.Overflow	Buffer Errors	1	1	98
5	2	Trihedral.VTScada.WAP.Directory.Traversal	Path Traversal	3	1	14
6	1	Modbus.TCP.Report.Server.Info	Permission/Privilege/Access Control	1	1	12





How a California Water and Wastewater District Leveraged Fortinet Solutions to Protect Critical Water Treatment



SITUATION

- Water and wastewater treatment district in Central California serving about 30,000 residents
- Small IT staff to support IT Applications and Network, no OT Cybersecurity specialists
- Current OT network and devices supported by System Integrators who didn’t provide access to network (Black Box)
- Network security was an afterthought

PROBLEM

- Unplanned OT downtime due to lack of system events
- Complex system to troubleshoot
- Lack of skills to manage several devices via CLI
- No timely notification of network events – Login, remote users, connecting unapproved devices, etc.
- Shared credentials (no MFA)

CUSTOMER NEEDS

- Strict control to access OT network (i.e. employee, SI, OEM, third party)
- OT network visibility for non-technical staff
- Easy of Use environment
- Integrated Network and Security
- Set up notifications and system events (No Network SME)

SOLUTION BENEFITS

- FortiGate NGFW integrated with FortiSwitch (FortiLink)
- FortiToken Mobile – MFA & FortiCloud (remote management)
- Easy of Use GUI to manage both Security and Networking (no separate switch config)
- Role based access control – users only get access to resources they need
- Holistic visibility at the network level: tag ports, network port status, unplugged cable, Quarantine VLAN, place PLCs in respective VLAN, etc
- Notifications: email alerts, malware or viruses id, network traffic violation, OT protocols inspection, approved third-party vendor logs in, etc

OT Customer Profile: Water Treatment

Bloomington Normal Water Reclamation District

COMPELLING EVENT

- Need for consolidation of products in environment
- Desire to improve security posture
- Lack of visibility across end points
- Needed OT security monitoring

CUSTOMER NEEDS

- SD-WAN capabilities
- Consolidate management of security and networking
- Ease of Use and management – GUI
- Single vendor to call for support
- Network visibility and user/device restrictions

SOLUTION

- FortiGate 100Fs & 60Fs
- FortiSwitch 1024D, 124F, 108F, 148F, Rugged 112D-POE
- FortiAP 231F
- FortiAnalyzer
- FortiManager
- FortiDeceptor
- FortiNAC

OUTCOME

- Single Pane of Glass Management
- 100% Visibility of Network and Security
- Attack surface reduced
- Single vendor environment
- Potential next steps are SIEM, EDR, and Mail protection

OT Customer Profile: Water Treatment

SANGAMON COUNTY WATER RECLAMATION DISTRICT

COMPELLING EVENT

- Desire to improve security posture after ransomware attack
- Lack of visibility across end points
- Need for consolidation of products in environment
- Needed OT security monitoring
- Needed network segmentation

CUSTOMER NEEDS

- Consolidate management of security and networking
- Ease of Use and management – GUI
- Single vendor to call for support
- Network visibility and user/device restrictions
- End point monitoring and threat correlation

SOLUTION

- FortiGates 501E, 600E and others
- FortiAnalyzer
- FortiManager
- FortiEDR
- FortiExtender
- FortiClient
- FortiDeceptor

OUTCOME

- Single Pane of Glass Management
- 100% Visibility of Network and Security
- Attack surface reduced
- Single vendor environment for security and networking
- Potential next steps are FortiVoice and FortiSwitch

Take the Next Step

Talk to an expert about your cybersecurity needs and strategy

Funding for Cyber Resilience and Protection

- Clean Water State Revolving Fund (CWSRF) | US EPA
- Drinking Water State Revolving Fund (DWSRF) | US EPA
- State and Local Cybersecurity Grant Program (SLCGP) | CISA
- WaterSMART | USBR

Over $3B amongst these four programs

Grants Support Program

Bringing Technology Funding Home for Public Sector Agencies

Get Started by emailing

SLED@Fortinet.com

Get the Report

Sponsored by

FORTINET

2024 Cybersecurity in Water Management Facilities Report

Addressing the growing threat of cyberattacks on America's water supply and wastewater utilities

WASTEWATER DIGEST

WaterWorld

Public Service Announcement

Q&A

Thank you!

More info | www.fortinet.com/OT
Email | OT@fortinet.com

FORTINET