network perception

10 BUILDING BLOCKS TO PREVENTING OT NETWORKS FROM CYBER ATTACKS

From the last few years, it is clear that cyber threats are increasingly common, getting more sophisticated, and expensive.

The majority of organizations still lack proper visibility to efficiently defend themselves. The urgency to improve the situation is heightened in the case of operational technology (OT) networks where cyber attacks could cause heavy damage to industrial equipment, disruption to the utilities many rely on, or even loss of life.

How to **solve this?**

To be proactive and reduce risk, OT network operators need to develop cyber resiliency, which means the ability to keep running mission-critical operations despite being under threat.

Security and risk management leaders need to partner with other departments to prioritize digital supply chain risk and put pressure on suppliers to demonstrate security best practices.[5]

These best practices are part of the NIST Special Publication 800-160 on Developing Cyber-Resilient Systems aim to help organizations reach the capability to anticipate, withstand and recover from, and adapt to adverse conditions.

Cyber Resiliency Building Blocks

Visibility and Understanding

1 Analytic Monitoring
Monitor and detect adverse actions and conditions in a timely and actionable manner.

2 Dynamic Representation
Keep representation of the network current. Enhance understanding of dependencies.

3 Substantiated Integrity
Ascertain whether critical system elements have been corrupted.

93% Cybercriminals can penetrate 93% of company networks[3]

35% Roughly 35% of attacks on the energy industry were attempted data theft and leaks.[4]

70% The latest report from Dragos determined that 70% of service engagements have a lack of visibility across OT networks.[1]

45% Gartner predicts that by 2025, 45% of organizations worldwide will have experienced attacks on their software supply chains, a three-fold increase from 2021.[2]

Defense-in-Depth

4 Coordinated Protection
Implement a defense-in-depth strategy, so that adversaries must overcome multiple obstacles.

5 Redundancy
Provide multiple protected instances of critical resources.

6 Diversity
Use heterogeneity to minimize common mode failures, particularly attacks exploiting common vuln.

Least Privilege Principle

7 Segmentation
Define and separate system elements bases on criticality and trustworthiness.

8 Privilege Restriction
Restrict privileges based on attributes of users and system elements as well as on environmental factors.

9 Realignment
Minimize the connections between mission-critical and noncritical services.

10 Non-Persistence
Generate and retain resources as needed or for a limited time. Reduce exposure to compromise.

Core Challenge:

A significant volume of geographically-dispersed OT devices are vulnerable to cyber risks.

50% of organizations have improper network segmentation (Dragos)

70% of organizations lack OT network visibility (Dragos)

21 DAYS
Average downtime due to ransomware attacks
(Coveware)

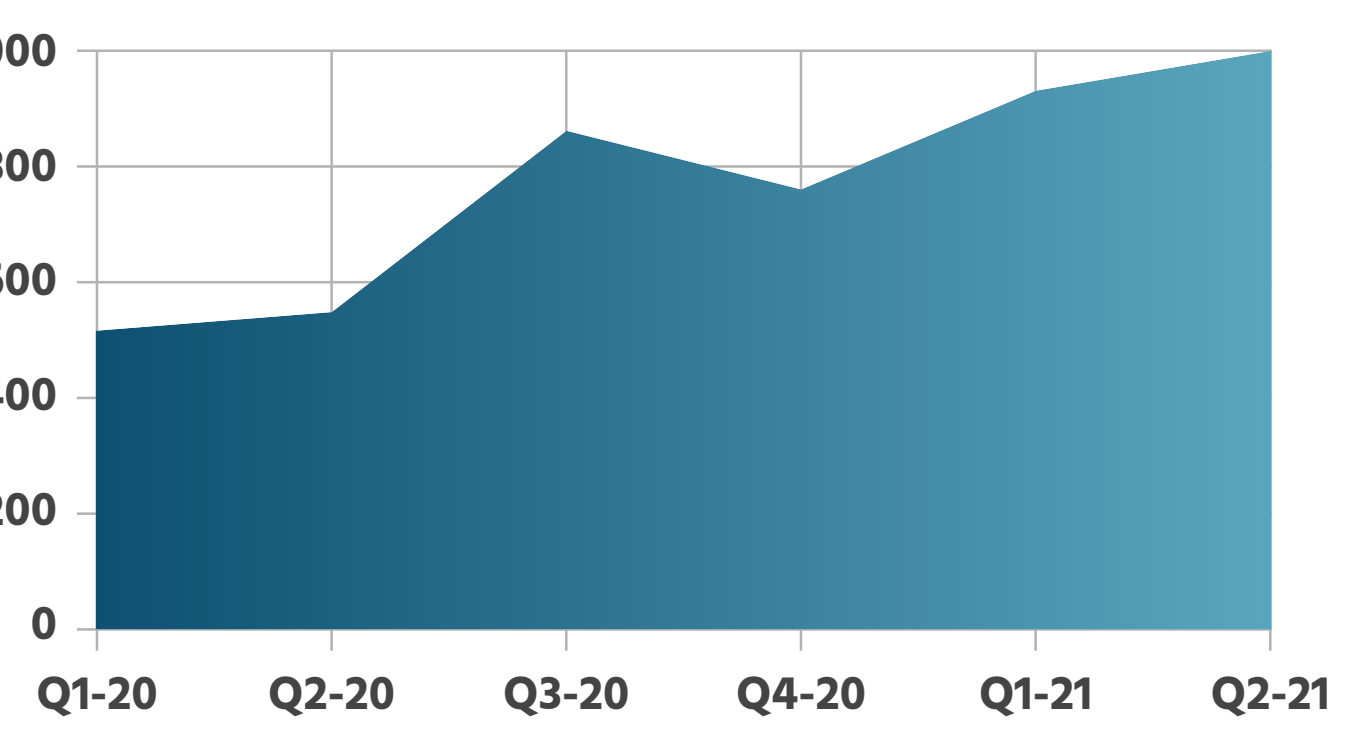
287 DAYS
Average days it takes a business to fully recover from an attack
(Emsisoft)

$350 MILLION
Victims paid in ransom in 2020 - a 311% increase over the prior year
(Chainalysis)

$312 THOUSAND
The average payment in 2020 - A 171% increase compared to 2019
(Palo Alto Networks)

Weekly Amount of Organizations Impacted by Ransomware

(2020-2021)



Increasing Ransomware Threat

350%
Number of ransomware attacks jumped by 350% since 2018

100%+
Average ransom payment increased by 100%+ this year so far

The energy sector is becoming a prime target next to healthcare

Network visibility is paramount to gain situational awareness and reduce the exposure of our critical assets. There is no doubt that to become cyber resilient, organizations have to eliminate all blind spots through a comprehensive network visibility program.

Understanding the complex architecture of multi-layer networks can be extremely challenging. The Network Perception solution NP-View has been designed to address this challenge by enabling real-time visibility into network assets and access paths.

NP-View can directly assist security and compliance teams by providing the following turn-key solutions:

- Correct implementation and verification of network segmentation
- Offline desktop access that doesn't write to the network to promote velocity
- Generate automatically network architecture diagram to increase visibility

network perception

See how Network Perception can help you stay proactive, reduce risk, and prevent cyber attacks from impacting your OT networks.

Contact us today

+1 (872) 245-4100 info@network-perception.com https://network-perception.com

SOURCES:
1 - https://www.dragos.com/year-in-review/
2,5 - https://www.gartner.com/en/articles/7-top-trends-in-cybersecurity-for-2022
3 - https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=9b2a3766b616
4 - https://securityintelligence.com/articles/energy-utility-data-breaches-2021/