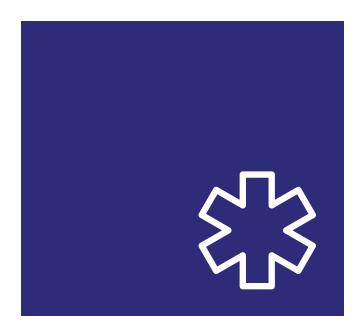


What is Critical National Infrastructure (CNI)?

Its key sectors include:











TRANSPORTATION EMERGENCY SERVICES COMMUNICATIONS FOOD & AGRICULTURE DEFENSE

The risks

of CNI organizations have detected cyber attacks on their OT/ICS environments[®]

of CNI security leaders find that multi-vendor environments make it more challenging to secure their organization.

cited disjointed architecture across OT and IT environments as a top security concern^o

The impact

90%

of critical infrastructure providers in the US, UK, Germany, Australia, Mexico, and Japan have fallen victim to a cyber attack in the past two years

Some recent high-profile attacks on CNI and their consequences:

2020 NTT Communications attack

621 corporate clients' data leaked ⁶

2021 Colonial Pipeline attack

11,000 gas stations left without gas *

2021 JBS Foods attack

\$11 million ransom paid to hackers ⁸

https://www.bridewellconsulting.com/majority-of-cni-organisations-experience-successful-cyber-attacks-despite-strong-confidence-in-security

<u> https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/</u> <u> https://www.firstpoint-mg.com/blog/analysis-of-top-11-cyber-attackson-critical-infrastructure/</u>

CENTRIPETAL

Centripetal CleanINTERNET protects your customers, your partners, and your reputation with real-time, simplified cyber threat intelligence.

Our solution creates a Zero Trust environment for CNI providers, bi-directionally shielding malicious threats to proactively prevent network infiltration and data exfiltration.

Get instant and effortless visibility across your network with Centripetal CleanINTERNET.

To find out more, call us on 571-252-5080 or get in touch with the Centripetal team on our website.