



FROST & SULLIVAN  
INSTITUTE

# Digitalization And Real-Time Visibility Transforming The Global Critical Infrastructure Cyber Security Market

Related Thought Leadership: Security



# Digitalization And Real-Time Visibility Transforming The Global Critical Infrastructure Cyber Security Market

Today's evolving cyber security threat landscape has left no system or network impervious to changing risk profiles. While corporate and consumer businesses remain popular marks for cyber-attacks, critical infrastructure facilities have become increasingly popular threat targets; they are highly vulnerable to major operational disruptions and cyber-incidents that can lead to real-world peril. Despite the ever-increasing threat landscape and their incredibly high risk profile, critical infrastructure organizations remain far behind where they should be in their cyber-maturity and digital resilience strategies, necessitating a rapid push to fortify cyber-defenses and manage their cyber-risk profiles. As the security industry is seeing increasing convergence between the physical and digital security domains, critical infrastructure organizations highlight how a cyber security attack affecting organizational networks could result in a physical disaster in society. Critical infrastructure organizations need to focus their cyber security strategies on the twofold task of maintaining regulatory compliance and uninterrupted operations while at the same time building up their digital resiliency strategies. They can do this by adopting solutions that will monitor, inventory, analyze, and assess all connected assets, networks, and systems to determine any pertinent vulnerability; to assess risks; and to enact mitigation, remediation, or quarantine policies to protect their operational networks without disrupting services.