

API security for oil and gas

What current pipeline cybersecurity requirements mean for API visibility and protection, and how one gas utility responded.

The industry requirements

TSA security directives apply to pipeline and LNG owners and operators that TSA has designated critical, and other operators often use them as a baseline. Directive 2021-01 requires a 24/7 cybersecurity coordinator, incident reporting to CISA within 24 hours, and a gap assessment against TSA's Pipeline Security Guidelines. Directive 2021-02 requires a Cybersecurity Implementation Plan covering critical cyber systems, segmentation, access control, continuous monitoring and detection, and risk-based patching, plus an incident response plan and an assessment plan. TSA has also proposed a rule to make surface cyber requirements permanent, and API 1164 extends guidance across industrial automation and control environments. At the same time, acquisitions, new gateways, and IT and OT integration expand the API footprint faster than most teams can inventory it, and operators have little tolerance for controls that add latency or downtime risk to production.

How Salt helps meet the requirements

TSA requirement	How Salt helps
Identify critical cyber systems (2021-02F, III.A)	Continuous API discovery builds a living inventory of managed, shadow, and zombie APIs across gateways, cloud, and the external attack surface, so API-connected systems are not missing from the asset inventory.
Network segmentation policies and controls (2021-02F, III.B)	Posture governance flags APIs that expose internal services or sensitive data, and the external Surface Scan shows what is reachable from outside, helping teams verify that segmentation holds at the API layer.
Access control to prevent unauthorized access (2021-02F, III.C)	Salt validates authentication and authorization on every discovered API, surfaces unauthenticated or over-permissioned endpoints, and detects attempts to abuse them.
Continuous monitoring and detection (2021-02F, III.D)	Runtime protection detects business logic abuse, account takeover, data exfiltration, and anomalous API behavior in real time. Out-of-band deployment adds no latency or downtime risk to production.
Risk-based patching of critical cyber systems (2021-02F, III.E)	Outside Salt's scope, since Salt does not patch operating systems or firmware. Posture findings help prioritize remediation of weaknesses at the API layer.
Report cybersecurity incidents to CISA within 24 hours (2021-01D, II.C to II.E)	Alerts and investigation views show the affected APIs, attacker indicators such as malicious IP addresses, and the data involved, giving responders the details a CISA report calls for.
Incident response plan, assessment plan, and gap assessment against TSA's Pipeline Security Guidelines (2021-02F, 2021-01D II.F)	The Surface Scan and continuous posture reporting give evidence for gap assessments, remediation timelines, and ongoing API risk reporting.

A use case: a regional gas utility

After acquiring operations from another utility, a regional natural gas provider serving millions of customers had to meet a regulatory deadline with no API security solution in place and little tolerance for production risk.

Salt's Surface Scan ran first. It identified APIs and data flows not yet passing through the utility's API gateway and surfaced 1,466 posture gaps, giving the team a starting point without waiting on a long rollout. Deployment begins with net new APIs in the first initiative.

Key benefits

Immediate value The Surface Scan exposed APIs outside the gateway and posture gaps before deployment began, so the team could prioritize early.	Gateway integration Salt integrates with leading API gateways, including Kong, which was a key differentiator for the utility's gateway project.
Lower operational risk Salt's out-of-band deployment model avoids latency and downtime risk to production, which matters in critical infrastructure.	Technical confidence A detailed architecture and deployment review gave the utility's team confidence in Salt's approach.

Key takeaway

Regulatory expectations for pipeline operators keep evolving, and acquisitions expand the API footprint faster than most security teams can track. The first step is visibility: knowing which APIs exist, how they are authenticated, and where controls are missing. From there, teams can prioritize and close gaps without waiting on a long rollout and without putting production availability at risk. Salt complements, and does not replace, OT network monitoring and incident response processes.

Want the same visibility? Request a Surface Scan | saltsecurity.com