BES Network Cyber Security & NERC CIP Version 6 Continuous Compliance Using Tufin Orchestration Suite™

Solution Brief

Cybersecurity is a tremendous challenge for today's power grid critical infrastructure. Recent government-sponsored research concluded that "cyber threats to the electricity systems are increasing in sophistication, magnitude, and frequency" and the electricity system "faces imminent danger" from cyber-attacks. The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards evolved after the Great Northeast Blackout of 2003 that affected over 50 million people. Now there is an urgent and evolving need for more stringent standards to protect the Bulk Electric System (BES) of the North American power grid. NERC CIP v6 is the most recent version of policy guidelines by which critical cyber assets must be protected.

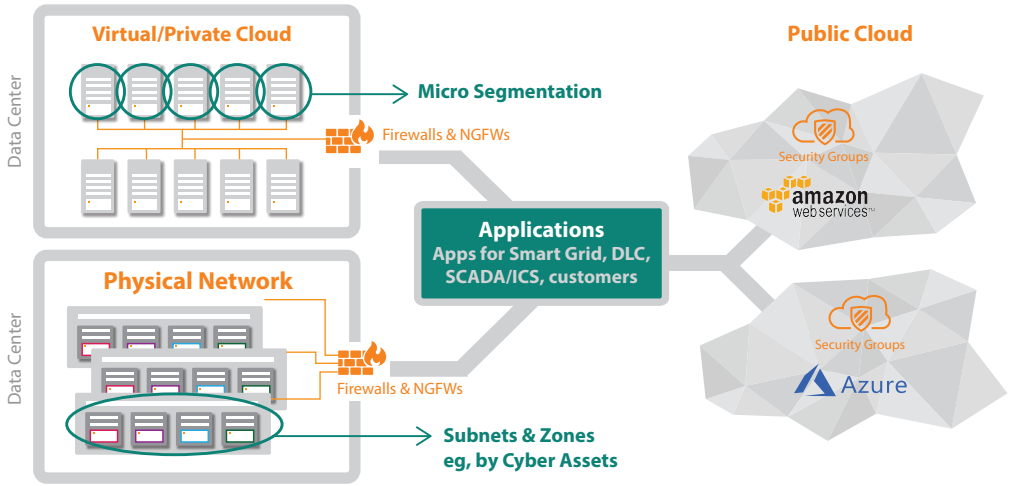
The Challenge: Transitioning to NERC CIP V6 Compliance

The challenge for BES networks transitioning to and complying with NERC CIP V6 is multi-faceted, requiring:

- More stringent regulations than previous standards regarding policies, Asset Coverage, new Grouping of Cyber Assets (BES Cyber Systems), and Impact Ratings
- Extensive change management processes and sensitive risk analysis
- More auditable evidence for demonstrating compliance
- Violations of compliance costing up to $1 million penalty per day
- Enforcement of security policies across networks supporting today's BES power grid comprised of multi-vendor, multi-technology heterogeneous IT environments that span physical and hybrid networks, and the cloud
- Application connectivity management for Smart Grid; Dynamic Load Control (DLC) systems; Supervisory Control and Data Acquisition (SCADA) / other Industrial Control Systems (ICS); advanced metering software; load modeling; electric grid monitoring; transmission assessment; risk analysis; and other critical applications for running the utility business
- Develop and implement methods to deter, detect, or prevent malicious code via transient assets, and provide proof of those methods.
- Meet deadlines that significantly vary across NERC CIP versions

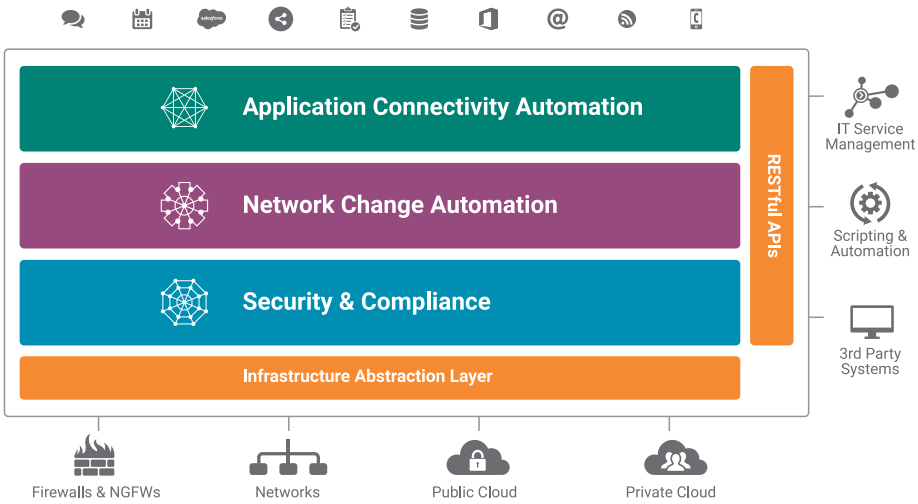
Highlights and Benefits:

- Manage and control network security for BES Cyber Systems from a single console
- Gain security visibility across physical networks and public and private clouds
- Ensure continuous policy and NERC CIP regulatory compliance and auditability
- Increase agility for network security infrastructure changes
- Support multi-vendor, multi-technology IT infrastructures with end-to-end centralized management



The BES Network reality: Multi-vendor, multi-technology, heterogeneous IT infrastructures

Tufin Orchestration Suite™: Your Toolbox for NERC CIP V6 Compliance



The Tufin Orchestration Suite™ (TOS) addresses these challenges by managing security policies and enforcing compliance across BES enterprise networks. Amid changes to the network, the TOS provides application-driven connectivity to ensure critical application accessibility for business continuity.

Tufin Orchestration Suite enables NERC CIP V6 compliance by providing enterprises responsible for BES networks with solutions to:

- Manage and visualize network Cyber Assets and Cyber Systems through a single pane of glass across the physical and hybrid network, and the cloud
- Control and ensure secure application connectivity across the entire network
- Maintain application-driven network security change automation based on risk assessment
- Reduce the attack surface and mitigate threats of Transient Assets through effective management of network segmentation
- Provide audit-ready evidence on-demand with an automatic audit trail
- Enforce your security policy inclusive of NERC CIP and other regulatory requirements

From \ To	Control Center	Corporate	DMZ	EACMS	Internet	PACS	Substation
Control Center		C	C	C	C	C	C
Corporate	C		C	C	C	C	C
DMZ	C	C		C	C	C	C
EACMS	C	C	C		C	C	C
Internet	C	C	C	C		C	C
PACS	C	C	C	C	C		C
Substation	H	C	C	C	C	C	

Tufin's Unified Security Policy matrix provides a single pane of glass for managing NERC CIP V6 policies as well as other enterprise network policies

Tufin at a Glance

Offices: North America, Europe and Asia-Pacific

Customers: 2000+

Leading Verticals: Finance, telecom, energy and utilities, healthcare, retail, education, government, manufacturing, transportation and auditors

Channel Partners: More than 240 worldwide

Technology Partners & Supported Platforms: Amazon Web Services, BMC, Blue Coat, Check Point, Cisco, F5 Networks, Fortinet, Intel Security, Juniper Networks, Microsoft Azure, Openstack, Palo Alto Networks, VMware and more

[1] https://info.publicintelligence.net/INL-CyberThreatsElectricSector.pdf

tufin
www.tufin.com

SB-03-18