# COMPLIANCE AND SECURITY FOR UTILITIES

## Preparedness and Critical Infrastructure Protection

## THE CHALLENGE

### Meet NERC requirements and prevent catastrophic infrastructure events.

IT and security professionals in the utilities industry know just how challenging it is to meet the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements. Established to ensure the bulk electric system (BES) is protected from unwanted and destructive effects caused by cyberterrorism and other cyberattacks, NERC CIP policies are constantly changing on everything from security management controls to physical security of cyber systems, and even configuration change management and vulnerability assessments. Utilities require flexibility to adapt and change rapidly to make sure they are compliant or they can be subject to fines or sanctions.

A 2018 analyst firm survey[1] showed that regulatory changes and scrutiny was the top concern for energy and utility organizations. But security and compliance teams often have limited visibility into where rules are hidden, how vulnerabilities can be accessed and how risks can be mitigated.

Specific challenges facing utilities include:

- Overly permissive rules giving unknown access
- Frequent surges and changes to systems
- Added risk from unresolved vulnerabilities, random patching
- Changes cannot keep pace with NERC CIP requirements

## THE SOLUTION

### Complete visibility and automation for utilities.

FireMon brings utility networks under control with traffic flow analysis and rule reporting so you can identify where policy can lead to exposures. The system flags overly permissive rules for cleanup, simulates attacks to show how vulnerabilities can be accessed and enables security orchestration across utility networks for instant remediation.

FireMon is the only solution that offers real-time monitoring and continuous compliance checks, notifying you when changes happen and need enforcement, all from a single pane of glass.

[1]Energy and Utilities Industry Group. Executive Perspectives on Top Risks for 2018: Key Issues Being Discussed in the Boardroom and C-Suite. Protiviti.

## WHY FIREMON?

**CONTINUOUS COMPLIANCE**

Avoid lapses in compliance with sub-second checks across 350+ controls.

**ATTACK SIMULATION**

Combining vulnerabilities with network policy shows the pricise path an attacker can take through the network.

**ADAPTIVE CONTROLS**

Critical infrastructure can change in the blink of an eye, including new inputs that demand new security rules. FireMon's adaptive controls respond to those changes, instantly pushing updated rules to the right enforcement points to fortify the network.

**REAL-TIME MONITORING**

Your networks become self-aware with real-time monitoring and rule optimization. As new network federations come in and go out, active data capture keeps an eye on all these interconnected parts, removing risk with perfect visibility.

**DATA RETENTION AND AUDITING**

NERC CIP requires that utility organizations retain specific evidence for a period of time to demonstrate compliance. FireMon delivers your complete compliance and change history at your fingertips with customizable search and reporting.

FIREMON

FIREMON FOCUS

SECURITY MANAGER

FireMon's device and policy management solution manages firewall policies.

## SOLUTION OVERVIEW

FireMon identifies all the connections within your networks, discovering overly permissive, outdated or hidden rules. Total visibility gives you the confidence that utility controls and systems are protected from unauthorized access.

Only FireMon hardens security for utility networks, translating security intent and automating policy changes for any fluctuations in the operating environment.

### ACCESS PATH ANALYSIS

Opens the door to all the connections hiding in complex environments, removing backdoors to the network.

### RISK ANALYSIS

Simulate attacks to uncover exposures, model patching options and score risks to prioritize remediation.

### AUTOMATED RULE PUSH

Commands security in your environment with sub-second changes, adapting to the dynamics as the network shifts.

### REAL-TIME MONITORING

Gives clear direction on what is happening the moment it is happening, alerting you to issues in the network.

### AUTOMATED DECOMMISSIONING

Removes expired and unnecessary rules instantly, so integrated federations are always protected.


## WHO IS FIREMON?

The FireMon platform delivers continuous security for hybrid enterprises through a powerful fusion of vulnerability management, compliance and orchestration. Since creating the first-ever network security policy management solution, FireMon has continued to deliver visibility into and control over complex network security infrastructures, policies and risk postures for more than 1,700 customers around the world. For more information, visit www.firemon.com.

FIREMON